MASTER'S THESIS

Security Information and Event Management for Small and Medium-Sized Enterprises

Alan Mercer

2013

Master (120 credits)
Master of Science in Information Security

Luleå University of Technology
Department of Computer science, Electrical and Space engineering

ACKNOWLEDGEMENTS

This work is dedicated to the following people

Andy Riddett

My manager and supporter throughout the last two years; without his permission, sponsorship and guidance my success on this Masters programme would not have been possible.

My lecturers over the last two years

Dan Harnesk, Devinder Thapa, Jörgen Nilsson, Lars Furberg, Tero Päivärinta, Todd Booth

From the very first lecture on Systems Thinking you guys have stretched & challenged this middle-aged brain to make me a better information security professional (and possibly a better human being!)

My thesis supervisor

Maung Sein

For his expert guidance and words of encouragement throughout this thesis work.

My friend and student partner

Esi Man Nunoo

Who I thank for the friendship and help she has given me and I completely admire the effort she has made to be such a success throughout this Masters programme.

And finally, most importantly, my wife and daughter

Sara Hassen
Sahai Margot Mercer

I owe you two years of hugs, kisses and my totally undivided attention.

ABSTRACT

Purpose
This research project sets out to identify the security event management problems perceived in the SME context, prioritise these problems and then seek to solve them through the design and implementation of a prototype Security Information and Event Management (SIEM) system.

Design/Methodology/Approach
Action Design Research (ADR) is the research methodology used in this research project. ADR combines Action Research (AR) and Design Science (DS) research to solve a problem situation in a specific organisational setting through intervention and evaluation as well as the construction and evaluation of a novel IT artefact. A prototype SIEM was successfully designed and implemented in the case organisation over the course of a ten week intervention.

Findings
A number of findings emerged related to the testing of Design Principles (DPs) extracted from earlier SIEM research, the testing of ADR in the context of an SME as well as the presentation of nine new DPs for SIEM design and implementation in similar future projects.

Practical Implications
Apart from a working prototype SIEM in the SME context one output from the research project is a planning and implementation checklist for practitioners for future SIEM design and implementation projects, generalizable to all contexts and not just that of the SME.

Originality/Value
This research provides a short state-of-the-art summary of current SIEM research, validates two DPs extracted from earlier SIEM research, proposes nine new DPs relevant to future SIEM design and implementation and tests the effectiveness of ADR in the context of an SME research project.

Keywords
Security Information Event Management (SIEM), Small and Medium Enterprise (SME), Action Design Research (ADR), Design Principles (DP)

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

ADR	Action Design Research
AR	Action Research
BIE	Building, Intervention & Evaluation
BST	British Summer Time
DB	Database
DC	Domain Controller (Microsoft Windows Operating System)
DNS	Domain Name System
DP	Design Principles
DR	Design Research
DS	Data Source (in the context of this research project)
EICAR	European Institute for Computer Antivirus Research
ePO	e-Policy Orchestrator (McAfee)
EPS	Events Per Second
G	Goals (of the research project)
HIDS	Host-based Intrusion Detection System
HP SIM	Hewlett-Packard Systems Insight Manager
IAM	Identity and Access Management
IDS	Intrusion Detection System
IIS	Internet Information Server (Microsoft web services)
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
KPI	Key Performance Indicator
LCE	Log Correlation Engine (Tenable Security)
MASSIF	Management of Security information and events in Service Infrastructures
NIC	Network Interface Card
NIST	National Institute of Standards and Technology (USA)
NTOP	Network Top (Network tool)
OCS NG	Open Computer and Software Inventory Next Generation (Inventory tool)
OPSEC	Open Platform for Security (Check Point)
OSS	Open Source Software
OSSEC	Open Source Security (HIDS software)
OSSIM	Open Source Security Information Management (Alien Vault SIEM)
PCI	Payment Card Industry
PCIe	Peripheral Component Interconnect Express (Computer Expansion bus)
PP	Perceived Problem (in the context of this research project)
PWC	Price Waterhouse Coopers
R	Reflection (in the context of this research project)
SAN	Storage Area Network
SC	Selection Criteria (in the context of this research project)
SCADA	Supervisory Control and Data Acquisition
SEM	Security Event Management
SIM	Security Information Management
SIEM	Security Information & Event Management
SME	Small & Medium Enterprise
SOC	Security Operations Centre
SPAN	Switched Port Analyser (Cisco)
UCT	Coordinated Universal Time

VA	Vulnerability Assessment
VLAN	Virtual Local Area Network
WSN	Wireless Sensor Network
WSUS	Windows Server Update Services

1. INTRODUCTION

This chapter introduces the problem of security event management and describes a common solution to the problem – a Security Information Event Management (SIEM) system. Next the challenges of small and medium enterprises (SME) and the lack of research into SIEM systems in the SME context are discussed. Finally the objective of this research work and the structure of this thesis paper are set out.

1.1 Problem Description

As security breaches increase year-on-year (PWC, 2013), mostly discovered months after the event (Verizon, 2013) one of the key challenges facing Information Security practitioners in the field today is that of timely collecting, collating and analysing the security events generated from a wide source of network systems, security mechanisms, systems and applications deployed across a modern business.

Through this event collection, analysis and intelligence generation, security teams can identify vulnerabilities in their infrastructure, as well as enumerate, alert and report on attempts to exploit these vulnerabilities, through externally sourced attacks via shared networks, like the Internet, or from internal sources, such as staff with malicious intent.

1.2 Security Information & Event Management (SIEM) Systems

Security Information and Event Management (SIEM) solutions are systems capable of analysing security events in real time as well as offering long-term log storage, historical reporting and trend analysis. They act as incident alerting mechanisms and correlate vulnerability and threat data to offer insight into risk prediction (and prioritization of these risks) as well as log auditing and reporting for compliance purposes, such as Payment Card Industry (PCI) regulations.

SIEMs are capable of giving the information security function a holistic view of their exposure to security threats through the aggregation of log data from multiple sources, such as firewalls, switches, load balancers, web server logs and proxy servers; correlation of these logs to extract meaning and intelligence from this mass of data; alerting when certain event conditions are met; and one overall dashboard that gives visibility to events that previously might have required management of multiple dashboards and reporting tools.

The SIEM is a combination of log/event storage and subsequent event analysis which is emerged from SEM and SIM technology in the middle of the last decade (2005 onwards) – SEM or Security Event Management is the consolidation and storage of multiple log sources and security events, whereas SIM or Security Information Management is the analysis and longer-term trend analysis of these logs. SIEM adoption has grown rapidly over the previous five years, largely driven by the demands of event logging for PCI compliance.

SIEMs are supplied as applications, virtual machines or hardware devices by large commercial vendors such as HP, McAfee and Symantec or as Open Source Software (OSS) applications, namely Alien Vault's Open Source Security Information Manager (OSSIM) and Splunk Inc.'s Splunk.

These SIEMs are implemented in a variety of contexts – from large scale enterprises with multiple security domains to administer to industrial control systems for critical infrastructure – however one context of particular interest in that of the small and medium-sized enterprise (SMEs).

1.3 Small & Medium Sized Enterprises

SMEs have similar challenges to larger business with regards to this event collection, correlation and analysis, yet as Welsh and White (1981) point out, through a chronic lack of resources SMEs are weak in terms of available finances, detailed planning, operational control, staff training and deployed information systems. The IT and IT security functions may be very small and understaffed, with technical security responsibilities may fall largely to operationally focused staff, whose technical knowledge and skill set may be lacking.

SMEs also differ from larger enterprises in other ways. Projects are run with less planning and project management (Murphy & Ledwith, 2007), a lack of rigorous software procurement process affect technology decisions to 'build or buy' (Daneshgar et al., 2013) and technology implementations are significantly influenced by CEO decision making (Ghobakhloo et al., 2011). What works for a large, mature business may be impractical in the SME context.

Granted many SMEs may choose the cloud managed services SIEM option that has become popular through low upfront costs and ease of implementation (Salleh et al. 2012) , however not every SME wishes to trust the security monitoring of their critical systems to a third party; driving the SME towards the in-house, self-implemented SIEM.

As Conradi (2007, p. 366) points out, organisations, large or small, in the UK must comply to European Data Protection legislation which requires "appropriate technical and organizational measure to be in place" and SMEs working in Financial Services have to "take reasonable care to establish and maintain systems and controls appropriate to the business", so many contracts the SMEs seek to win now demand suppliers comply with security standards such as ISO 27001 (Cowan, 2011); and these standards – including the PCI Data Security Standard (PCI, 2013) – which is required as part of processing credit card transactions - set out requirements concerning the logging of security events.

According to Ramdani and Kawalek (2007, p. 410) almost 60% of UK employees work for SMEs and over 50% of business turnover in the UK is generated by SMEs. Additionally SMEs are considered softer targets for criminals with the annual PriceWaterhouseCoopers (PWC, 2013, p. 2) Information Security breaches survey of 2013 reporting that 87% of SMEs experienced a security breach in 2012, the worst security breach costing on average £35k – £65k. The report also highlights weaknesses in the way the SME implements information risk management, incident management and monitoring.

So SMEs form a large percentage of UK business, suffer from expensive security breaches and have similar challenges and requirements regarding security event consolidation and analysis (to detect and correct these breaches) as larger businesses; however they typically have fewer human and technical resources and develop, implement and maintain systems, unlike larger enterprises.

1.4 Identification of the Knowledge Gap

Academic research is taking place around the design and development of SIEMs, more so in the last few years. Much of this research is focused one of four areas below, which are covered in greater detail in the next chapter's literature review.

(1) The design and implementation of SIEMs in the context of large scale deployments and certain industry types, particularly critical systems infrastructure (dams, control systems and power stations).

(2) The application of different techniques for deeper analysis and insight into the collected data, typically techniques taken from alternative fields such as Business Intelligence solutions or Data Mining tools.

(3) The design and implementation of SIEMs across heterogeneous systems and application networks, distributed computing environments and even linking of physical security systems and information technology systems into the same SIEM.

(4) Novel SIEM design, such as the linking of SIEM designs and deployments to security models and security standards for compliance purposes e.g. compliance with ISO 27000 standards or SIEMs specifically focused on digital forensics.

There is no previous SIEM-related research in the context of the Small and Medium-sized Enterprise (SME), so here is the knowledge gap.

1.5 Purpose / Objectives of this Research

The purpose of this Master's Thesis is to understand the event management problems facing the SME, prioritize these problems and attempt to solve them through the design and implementation of a SIEM prototype in this SME context. This thesis would build on earlier work in the field by taking applicable parts of existing SIEM design forward into a SIEM design that will work in the context of an SME.

The research method of Action Design Research, where the IT artefact emerges from a combination of informed design, implementation in the real-world context and iterative analysis will be used to design and implement the artefact. New Design Propositions related to the design and build of a SIEM in the SME context are expected to emerge from this research along with practical contributions relevant to information security practitioners and theoretical contributions relevant to academics.

Scope & Limitations
This research work was carried out over a ten week period in a UK-based technology-focused SME, working in the financial services sector. The project was signed off by the IT Director to involve the IT Operations team on a 'best effort' basis, so important operational concerns took priority at all time over the project work.

The objective of the SIEM prototype evaluation was to sufficiently inform any decision to take the project further into a next phase with a wider scope of data source collection and move from a prototype SIEM to live implementation within the SME; therefore the research documented in this thesis was limited to this initial prototype build and evaluation only.

1.6 Structure of this Thesis

This chapter introduced the problem of security event management and described a common solution to the problem – a Security Information Event Management (SIEM) system. The challenges of small and medium enterprises (SME) and the lack of research into SIEM systems in the SME context were discussed, along with the objective of this research project.

In the next chapter the method of reviewing the literature of previous SIEM research is set out, followed by a summary of the state-of-the-art of SIEM research today. SIEM research themes are proposed and a research gap relating to SIEM research in the SME context is identified.

The following chapter describes Action Design Research (ADR) and a justification is made to use ADR for this SIEM research in an SME context.

The results chapter of the thesis introduces the case organization (LTO Limited) along with the project set up, roles and timings of the ADR encounters. Outcomes of the four phases of ADR are presented, including the four sub-phases of the Building, Implementation and Evaluation (BIE) phase of ADR. The reflections of the research project team are set out and then distilled into nine proposed Design Principles for future SIEM design, along with a high level SIEM Planning and Implementation Checklist for practitioners.

This two concluding chapters of this thesis discuss the outcomes of the SIEM prototype build, linking the proposed Design Propositions to academic theories and commentary on the usefulness of ADR as a research methodology in the context of the SME research project. The outcomes of the research are considered in the context of IT and Open Source Software adoption in SMEs. Finally the research project’s implications for both academic theory and practitioner are summarized and end with a brief discussion of the limitations of the research and suggestions for future SIEM and SME related research.

2. THEORETICAL BACKGROUND

In this section the method of reviewing the literature of previous SIEM research is set out, followed by a summary of the state-of-the-art of SIEM research today. SIEM research themes are proposed and a research gap relating to SIEM research in the SME context is identified.

2.1 Literature Review Method

The process this literature review follows the guidelines set out by Okoli and Schabram (2010), which recommends an eight-step literature review process that is academically rigorous, comprehensive and reproducible.

The search for literature started with a broad scope – to search for any articles or academic papers concerning SIEMs. Tools such as the Lulea University Library, Google Scholar, Scopus and ProQuest were employed. This scope was then narrowed to focus on SIEM research related to the design and implementation of an SIEM in the context of an SME.

Primary sources, or first-hand reports of research, found in peer-reviewed academic journal articles or conference papers were favoured, though this paper ultimately cites a number of secondary (e.g. review papers) and tertiary sources (e.g. books) of literature relevant to SIEM research.

Once potential articles were identified, a brief search of the sources the article cited – or backwards search – was conducted, followed by a Google Scholar 'forwards search' to identify the articles or papers citing the initial article found. Using this method, academic journal articles were identified for further screening. Once it became clear that no new articles were easily identifiable, the search stopped and the review moved forwards to the 'screening for inclusion' stage.

Thirty-six papers went forward for screening for inclusion, however only twenty-four were taken to quality appraisal, based upon their application to the design and implementation of SIEMs in general, or SIEMs in an SME context. Based upon the year of the study (more recent was better), methodology of research (design science), testing of the design by implementation or prototype and generalizability of findings, four more papers were discarded; leaving twenty papers as the targets of data collection.

The research studies were then re-visited and a data collection form was completed for each paper. This collected the purpose and contribution of the research (was it clear?), why it was important, the outcome, the context, any future suggested research and any useful comments (based on observations or interesting findings). The collected data was aggregated, analysed and the report that follows was prepared.

2.2 Literature Review

This relative novelty of SIEM technology is borne out by the dates of the surrounding research studies. Of the 24 studies reviewed, ten were written in 2012, seven in 2011, three each in 2010 and 2009 and one in 2008.

Much of this research is focused into one of four specific SIEM-related research themes.

(1) The design and implementation of SIEMs in the context of large scale deployments and certain industry types, particularly critical systems infrastructure.

(2) The application of different techniques for deeper analysis and insight into the collected data, typically techniques taken from alternative fields such as Business Intelligence solutions or data mining tools.

(3) The design and implementation of SIEMs across heterogeneous systems and application networks, distributed computing environments and even linking of physical security systems and information technology systems into the same SIEM.

(4) SIEM designs with novel features that may be generically applicable to all SIEMs, such as automation of security controls related to the ISO 27000 or NIST series of security standards; or niche SIEM designs such as a SIEM design in the context of digital forensics.

Taking each theme in greater detail:

Theme 1 - Large Scale SIEM and/or Critical Infrastructure Environments
Research in the first research category - around the design of SIEMs in large scale and/or critical infrastructure environments includes work by Coppolino et al. (2011) who extend a commercial SIEM framework to the monitoring, control and security devices of a dam infrastructure; Romano et al. (2012) takes this further to include wireless sensor network technologies in Supervisory Control and Data Acquisition (SCADA) systems.

Theme 2 – SIEM Data Analysis Techniques
The application of different data analysis techniques to extract additional information from typical SIEM event stores in second area of SIEM research is covered by Gabriel et al. (2009) who apply data mining techniques to SIEM logs to detect hidden patterns of malware activity whilst Hadziosmanovic et al. (2012) propose a semi-automated log-mining design for SCADA logs.

Theme 3 – SIEMs in Heterogeneous/Distributed Computing Environments
As far as research into SIEMs across heterogeneous and distributed computing environment is concerned Kufel et al. (2013) propose several possible approaches for SIEM implementation across email, finance, HR and portal systems; and Sohn et al. (2012) suggests an SIEM structure that integrates physical and IT security events for a converged view of security-related activity across an organization.

Theme 4 – Novel SIEM designs
The final category of novel SIEM design ranges from the use of SIEMs to meet the compliance demands of security standards such as ISO 27001; Metzger et al. (2011) proposing a SIEM to support ISO 27001-compliant incident management and Montesino et al. (2012) describes a SIEM framework that permits the automation of ISO 27001 security controls for reduced complexity and improved efficiency.

It is interesting to note that six of the twenty four (25%) papers considered in this literature review were sponsored by the European Commission Project – MASSIF (or Management of Security Information and Events in Service Infrastructures) which seeks to develop a new generation of SIEMs applicable to Olympic Games security, mobile-phone money transfer systems, the challenges of SIEM in distributed computing environments and SIEMs for critical infrastructure, namely a Dam. This project is clearly supporting solid SIEM-related research, albeit across these four specific contexts.

Design Research is the preferred research method of these earlier studies, with designs validated thorough prototyping and experimental system tests. Apart from the design by Metzger et al. (2011)

which has been applied in a real-world scenario very successfully for one year the researched designs have not been implemented in their intended contexts and no learning from the implementation, possibly warranting a re-design, have been recorded. Even Metzger gives little details of the challenges or knowledge gained from implementation of the design.

Many of the papers do not ground their design science in any natural science theory and only the Romano et al. (2012, p. 224) and Coppolino et al. (2012, p. 6) offer any solid design principles “SIEMs should limit consumption of shared resources, such as network or central server processing” and “When physical access to the sensoring devices cannot be inhibited, and effective security solution must address detection of manipulations” respectively. Whilst it may be possible to extract further design principles from the body of the research works, the emergence of Design Principles and design theory do not seem central to the research.

There are no specific research works addressing the design of a SIEM in the context of an SME. Some earlier generic SIEM Design Principles may inform a designer of SIEM in the SME context, but this specific area appears completely devoid of research.

3. RESEARCH METHODOLOGY

In this chapter the Action Design Research (ADR) method is summarized and a justification is made to use ADR for this SIEM research in an SME context.

3.1 Research Method & Process

The research method that this plan proposes is Action Design Research (ADR), a combination of Design Science Research (DR) and Action Research (AR) which Sein et al. (2011, p. 40) describe as 'a research method for generating prescriptive design knowledge through building and evaluating ensemble IT artefacts in an organizational setting'.

Design Science Research seeks to develop prescriptive design knowledge (referred to as design principles) through building and evaluating technically novel IT artefacts to solve a class of problems - however the artefact is rarely built and evaluated in an organizational setting. The artefact itself is central to the research; any organizational impact is peripheral.

On the other hand, Action Research focusses on practical action through research to solve a problem in the organizational context; the practical action should benefit the organization as well as inform theory. Unlike DR, where the artefact is central, in AR the organizational impact is central (and the artefact peripheral).

As a combination of both these research approaches ADR seeks to solve a problem situation in a specific organizational setting (through intervention and evaluation) *as well as* the construction and evaluation of the artefact developed to solve this organization-specific problem.

Additionally, ADR posits that the ensemble artefact emerges as a result of this interaction within the organization setting; as it is developed iteratively together between the researcher and the case organization. It should be possible to develop the learning from the research into generalized solution concepts for similar classes of problem.

The artefact under construction and evaluation is a SIEM to solve the problem of collecting and analysing security events from multiple system and application sources in the context of an SME. The 'emergent ensemble artefact' will be shaped by the design and ultimate use of the SIEM.

The learning from the research should inform not only future SIEM design and implementation in the SME context, but also should be abstracted to general SIEM design and implementation in wider contexts. In addition it is possible that additional learning from the research may be abstracted again to the implementation of information technology in the SME context.

To further clarify through reference to Iivari (2013) two strategies for Design Science Research are set out. This proposal seeks to follow Strategy Two, defined as "Constructing a real system implementation as a specific solution to a problem encountered by a client, distilling lessons from the above construction that is packaged into a new, innovative IT meta-artefact as a general solution concept". The meta-artefacts being design principles for future SIEM design. The research dimensions of this strategy are set out in Table 3.1 below.

		Strategy 2	LTO Limited Research Proposal
Definitional Characterisation		Constructing a real system implementation as a specific solution to a problem encountered by a client, distilling lessons from the above construction that is packaged into a new, innovative IT meta-artefact as a general solution concept	
Context	1. Researcher-client Relationship	Client involvement inevitable	LTO Limited, a UK technology services SME working in the Financial services arena
	2. Priority of problem	1. A specific problem encountered by a Client 2. The general problem (the DSR problem) to be figured out later during the DSR project	1. To address the problem of security event collection, collation, analysis and alerting in the SME through the design and implementation of an SIEM. Test existing design principles and new design principles will be developed.
	3. Typical uncertainty of a DSR project	1. Uncertainty about the specific solution to the specific problem encountered by the client. 2. Uncertainty about the possible DSR contribution	1. Uncertainty about the specific SIEM solution. 2. Uncertainty about the DSR contribution – would earlier Design Principles apply, would new ones emerge.
Outcomes	4. Artifacts Built	1. A real system implementation as a specific solution to a problem encountered in practice 2. Conceptual IT meta-artefact as a DSR Contribution 3. Possibly a real system implementation (instantiation) of the conceptual IT meta-artefact	1. A real system implementation of the SIEM in LTO Limited. 2. Design principles verified/extended from earlier relevant research and new design principles identified.
	5. Primary role of the real system implementation	1. The real system implemented primarily a source of inspiration 2. Instantiation as a proof of concept and possibly used in the evaluation	1. The real system SIEM and design principles mutually inform each other. 2. The real system SIEM will serve as an instantiation of the design principles.
	6. Nature of the target IT artifact	Emergent system	The artifact will emerge during reflection & learning as the design is shaped through ongoing use.
	7. Typical nature of the IT meta-artifact	New, innovative design principles	Verification and extension of previously identified design principles as well as proposed new SIEM design principles.
	8. Innovativeness	Mixed tendencies + if an interdisciplinary research team, it may foster creativity + practical problems may challenge existing solutions, knowledge and wisdoms - easily focused on client's current problems - clients may be reluctant to experiment with the cutting-edge technology	+ Anticipated challenge to and enhancement of existing design principles - Research team not interdisciplinary

	9. Practical relevance	A priori better equipped to address immediate practical problems	A SIEM system will be operational within the company
Process	10. Major process driver	Experiences from the process of addressing the specific solution to a problem encountered in practice.	Experiences from developing the prototype SIEM in LTO Limited.
	11. Research Methods	Action Research or Action Design Research (in the intervention) Constructive (when constructing the general solution concept or IT meta-artefact) Other empirical (if separate evaluation) - field experiment - field study - case study - action research	ADR
	12. Generalization	1. Identify various problems encountered while constructing a real system implementation as a specific solution to a problem encountered by a client 2. Generalize these specific problems into a general class of problems. 3. Identify lessons from a) the real system implementation as a specific solution to the client's problem and/or b) from the process of developing that specific solution. 4. Generalize these lessons into IT meta-artefact as a general solution concept (e.g. design principles) 5. Associate the general solution concept with a class of problems identified.	1. Specific problems encountered during construction generalized into general class of problems relating to security event management systems in (a) SME context (b) general contexts 2. Specific lessons learned during the implementation and/or development generalized into design principles in (a) SME context (b) general context, related to SIEM design and potentially IT and OSS adoption in the SME context.
Resources	13. Access to a client	Necessary, but may be challenging	Good access to LTO Limited's IT Operations and support of the IT Director
	14. Expertise Needed	Often multidisciplinary or interdisciplinary	Disciplinary (Information Systems only)
	1. Research Team	The core research team is usually 3-10 members. The real system implementation to address the client's specific problem usually requires additional members, but all these members do not necessarily have a research interest in the project.	One researcher. One/Two Technology Services engineers on team Up to Eight Technology Services engineers and two IT Managers as stakeholders.
	16. Time & cost	Usually requires intensive involvement in the project over a longer period of time. Overall, time-consuming and expensive	2/3 months No dedicated project budget but limited security budget available. Virtual machines, hardware and software licences available already.

Table 3.1 - Design Science "Strategy Two" Dimensions

3.2 Summary of the Action Design Research Process

The project will follow the four stages of Action Design Research – problem formulation, building, intervention and evaluation, with reflection and evaluation across these activities. The final stage is the formalization of learning.

ADR Phase 1 – Problem formulation
During phase one of ADR the research opportunity is conceptualized, the organizational commitment is secured and roles and responsibilities for the work is defined. Contributing existing research and prior technological advances are identified and the stakeholders involved in the research effort set out the perceived problem (and stated goals) that the research will address; which should be an instance of a class of similar problems. The initial IT artefacts to design and evaluate is defined in this phase.

The principles of the problem formulation stage of ADR are:

(a) Praxis-inspired research – the research must have a practical application in the field.

(b) Theory-ingrained artefacts – artefacts created by ADR are carriers of theoretical traces i.e. there is an underlying theory that structures the problem and guides the design.

ADR Phase 2 – Building, Intervention and Evaluation (BIE)
Phase 2 of the ADR involves an iterative process of research in to the artefact design and implementation in partnership with the case organization. The initial knowledge-creation target is discovered, artefact feasibility studies are carried out, cycles of building, and intervention and evaluation are carried out until no further cycles are required.

The principles of the BIE phase of ADR are:

(a) Reciprocal shaping – the IT artefact and the client/researcher interaction with it, in the organizational context influence the design and implementation of the artefact.

(b) Mutually influential roles – the designer and the practitioner listen to each other and learn from the shared design and implementation experience.

(c) Authentic and concurrent evaluation – evaluation, both formal and informal, occurs by all parties during the course of the building and implementation of the artefact.

ADR Phase 3 – Reflection & Learning
Reflection on the design and redesign occurs throughout the course of the project as the results of the intervention are evaluated against the stated goals of the research. Additionally the adherence to the principles of each ADR phase form part of the reflection.

The principle that governs phase 3 of ADR is that of guided emergence, whereby the artefact emerges through the preliminary design and is refined by on-going interactions (and use of the artefact) among the participants; commonly with different perspectives on the artefact; such as an end-user, IT system administrator and researcher.

ADR Stage 4 – Formalization of Learning
The specific outcomes of the research are articulated and presented to practitioners and should be abstracted into solutions for a class of practical problems, with a set of design principles that emerge from the research.

4. RESULTS

In this section of the thesis the case organization (LTO Limited) is introduced, the project set up, roles and timings of the ADR encounters are documented and then outcomes of the four phases of ADR are presented, including the four sub-phases of the Building, Implementation and Evaluation (BIE) phase of ADR. The reflections of the research project team are set out and then distilled into nine proposed Design Principles for future SIEM design, along with a high level SIEM Planning and Implementation Checklist for practitioners, consolidated from previous practitioner literature and the results of this research project.

4.1 Design in the Case Organisation

The Company – LTO Limited
The case organisation is a leading technology organization for UK financial intermediaries and provides access to online (Internet-based) quote services as well as online applications for a large variety of financial products (life insurance, health insurance, annuities, pensions and bonds).

The operation of LTO Limited is based on the use of e-commerce services between a variety of partners, from single end-user Financial Advisers, groups of Financial Advisers working for one large Distributor organisation, software developers who have integrated the web services of the company into their software products and the large finance and insurance companies who provide the financial products that are quoted and applied for through the company.

Employing 85 staff in one head office, over 50% of these are technical staff and either application developers, testers or operational support focused. The company's internet-facing production infrastructure is hosted approximately 50 miles away in a traditional hosting centre, with a geographically and organisationally separate backup disaster recovery site approximately 15 miles from the head office.

Within the corporate information technology infrastructure there are a number of systems generating security-related events - load balancers, firewalls, Windows servers, web servers, network switches, anti-virus agents, network-based intrusion-prevention systems and vulnerability scanners – which means a number of different dashboards, consoles and alerting systems for the operational and security staff to monitor. With only one dedicated security resource and eleven IT support staff this becomes a challenge.

4.2 Set-up of the Project

Having acknowledged the on-going problem of security event log consolidation, correlation, alerting and reporting, the case organisation initiated a ten week long joint IT Security/IT Operations SIEM feasibility project. The support of the IT Director and IT Operations Manager was key to permitting resources to be allocated to this work; however given the busy nature of the SME IT staff, work on the project was not given the highest priority and it was understood that troubleshooting problems and other previously agreed, business-initiated projects would take resource ahead of the SIEM work.

The initial goal of the project was to understand and prioritise the specific security event log collection problems within the organisation's infrastructure. The SIEM features and security event data sources relevant to addressing the prioritised problems were agreed. Specific target systems that will provide these data sources for security event log collection were then identified. A selection of both commercial and Open Source SIEM solutions were considered at the base SIEM solution before the implementation of a prototype SIEM was started.

The anticipated outcome of the first phase of the SIEM feasibility project was the implementation of a prototype SIEM which would be evaluated against a pre-agreed set of criteria. This evaluation would influence the decision to move to the next phase of the project work, which would involve a wider scope to the type and number of data sources (and therefore target systems) measured, as well as deeper and more formal involvement by the IT Operations team. This additional phase of project work would be beyond the scope of this ADR work.

Roles & Responsibilities
It was agreed that the project sponsor would be the IT Director, with the IT Security Manager as the 'researcher' working in collaboration with the IT Operations team. The IT Operations Team was divided into those who would have a closer involvement with the implementation and those who would have peripheral involvement. All of the SIEM stakeholders were involved in agreeing the perceived problems and their priority and most (all but the IT Director) were involved in selecting the prioritised set of data sources, target systems and evaluation criteria for SIEM selection.

The table below sets out the roles and responsibilities agreed for the project in the initial project kick-off meeting.

Role	Responsibility	Fulfilled by
Project Sponsor	Sign-off of goals, high level project steering.	IT Director
ADR Team - Researcher	Work with practitioners on the project to design and implement the SIEM artefact	IT Security Manager
ADR Team - Practitioners	Work with the researcher to design and implement the SIEM artefact	3 x IT Operations Team Members
ADR Team - End Users	Input into the goals of the project and prioritisation, but not deeply involved with either the general project or the implementation work.	4 x IT Operations Team Members
ADR - Independent Observer	Deeper understanding of the project work, involvement with goal setting and input into surveys but not involved in implementation. Provider of peer feedback to the researcher.	IT Operations Manager

Table 4.1 - Project Roles & Responsibilities

Timings of Encounters and Reporting Mechanisms of the Project
At least one weekly project meeting was held during the ten weeks that the project ran, though some weeks multiple meetings were held. These formal meetings were to report progress on the SIEM project work, update participants on any allocated actions and acted as a forum to debate and reach decisions.

Meeting notes were taken, along with documented key decisions. These notes were turned into formal meeting minutes and distributed to the project team. Any pertinent reflections from project work that was carried out in between meetings, as well as general reflections on the operation of the project work were highlighted and documented in these minutes too.

Outside of formal project meetings, informal one-to-ones or small group gatherings were carried out with project members and any reflections or decisions were recorded manually and added to the meeting minutes of the next formal project meeting.

In addition five online surveys were carried out, using the Survey Monkey tool (http://www.surveymonkey.com/). Given the busy nature of the IT Operations team, project participants could not always attend the update meetings so this mechanism was a convenient way of gathering the views of the entire project group. The purpose and target audience of the surveys is listed in the table below.

No.	Survey	Target Audience
1	Perceived organisational security event management problems & their ranking by importance.	All of the ADR team
2	Potential security event data sources & their ranking by importance.	All of the ADR team
3	Evaluation criteria for selecting the SIEM base software, ranked by perceived importance.	All of the ADR Team
4	Evaluation of the SIEM prototype against the agreed criteria for prototype success. Opportunity to feedback on overall project successes, failures and whether the SIEM work should continue past the prototype stage.	All of the ADR Team
5	Evaluation of the researcher's reflections and proposed Design Principles (DPs).	ADR Practitioners

Table 4.2 - Online surveys run as part of the project

Resources available to the project

The hardware and software resources available to the project were agreed during the project set-up. This consisted of a spare HP G5 rack mounted server with an external storage array and 8GB of memory. The server was equipped with a 4-port network interface card to permit the monitoring of multiple networks.

Project Phases

After the planning and project kick-off meeting the SIEM feasibility project was carried out in six discrete phases, as set out in the table below.

No.	Phase	Duration
1	ADR Phase 1 – Problem Formulation	2 weeks
2(a)	ADR Phase 2 – BIE – Phase 1: SIEM Data Sources	2 weeks
2(b)	ADR Phase 2 – BIE – Phase 2: Base SIEM Selection	1 week
2(c)	ADR Phase 2 – BIE – Phase 3: SIEM Prototype Implementation	3 weeks
2(d)	ADR Phase 2 – BIE – Phase 4: SIEM Prototype Evaluation	1 week
Note: ADR Phase 3 (Reflections) occur throughout the project, so this is not listed as a discrete phase of work.		
4	ADR Phase 4 – Formalisation of Learning	1 week

Table 4.3 - Overall Phases of the ADR project

The types of encounters with different project stakeholders and the data collection methods used are set out in the table below.

Group	Formal Encounters	Type of Encounter / Data Collection Methods
ADR Team	5	Kick-Off meeting, Brainstorm session of perceived problems & potential data sources, online surveys
ADR Researchers & Practitioners	9	Kick-Off meeting, Brainstorm session of perceived problems & potential data sources, online surveys & weekly progress report meetings
Project Sponsor & Researcher	2	Project Initiation Meeting, Goals agreement Meeting. The Sponsor was also copied all meeting minutes.

Table 4.4 - Encounters with Project Stakeholders

Numerous informal encounters took place over the course of the project; these were face-to-face meetings at team member desks or server rooms, e-mail exchanges and via a dedicated SharePoint site set up for the project team.

The project timeline, highlighting key project events, decisions and reflections is set out in Figure 4.1 overleaf.

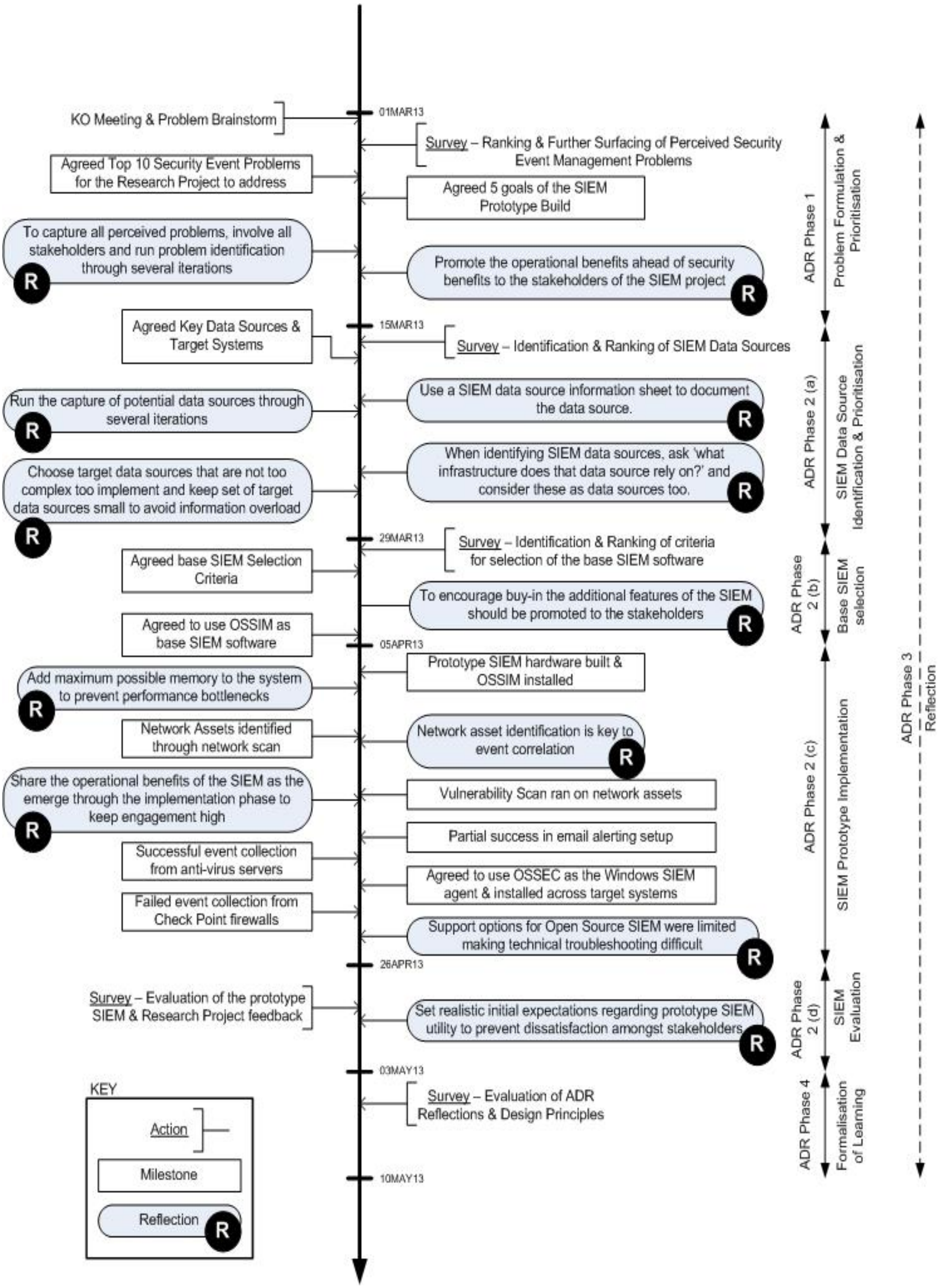

Figure 4.1 - SIEM Research Project Timeline

4.3 ADR Stage 1 – Problem Formulation

Duration	2 weeks
Participants	Researcher, Practitioners & End Users
Purpose	Identification and prioritisation of perceived problems relating to event collection

After project set-up and kick off of the project entered the first phase of ADR, which is problem formulation. This involved the articulation and prioritization of the specific problems perceived by project participants concerning security event collection, correlation, alerting and reporting.

Perceived Problems
Whilst previous research, practitioner literature and security standards establish the technological problem of collecting security event (or events of potential security interest) from a disparate set of systems, normalizing and correlating these logs and applying some intelligent analysis to trigger alerts (and event storage for historical reporting), this generic problem can be sub-divided into more specific sub-problems. Different sized organisations, will have different systems deployed, different resources available – both human and financial – to tackle the problems and different priorities relating to these problems.

The first requirement from the research team was to collect and document as many of these perceived problems, before ranking them into relative importance. This ranked set of problems permitted the team to agree on the data sources, target systems and scope of the project work as well as agree the goals and ultimate evaluation criteria of the project.

The identification of problems to address started in a section of the initial kick off meeting set aside to "brainstorm" these problems in the context of LTO Ltd. This identified 15 problems, which are set out in the table below.

No.	Perceived Problem	Identified by
PP-01	No real time security event log reporting or alerting	Brainstorming Session
PP-02	DC events are not collated.	Brainstorming Session
PP-03	No resources to monitor security events	Brainstorming Session
PP-04	Security events are not linked to give insight into undocumented service behaviour.	Brainstorming Session
PP-05	Server logs are configured with default settings.	Brainstorming Session
PP-06	Logging is disabled due to the volume of data generated which is not collated or analysed.	Brainstorming Session
PP-07	Logging fills server disk space quickly and can impact server availability so it is disabled.	Brainstorming Session
PP-08	Key data file access (and therefore potential data loss is not monitored)	Brainstorming Session
PP-09	Logging formats are incompatible so monitoring mechanisms cannot interoperate	Brainstorming Session
PP-10	There is a lack of change auditing for key files (such as configuration files) which hampers accurate change control.	Brainstorming Session
PP-11	No ability to see patterns of events across multiple systems.	Brainstorming Session

PP-12	No resource available for configuration of highly comprehensive event monitoring & alerting system.	Brainstorming Session
PP-13	No visibility of accidental or malicious changes to systems.	Brainstorming Session
PP-14	There is no automated asset tracking mechanism to check when systems – whether authorised or not - join the network	Brainstorming Session
PP-15	No joined up, correlated overall view of vulnerability across the systems managed by IT.	Brainstorming Session

Table 4.5 - IT Team perceived problems

After the minutes of the meeting were circulated and a short period of reflection, a further five problems were surfaced at the second project progress meeting, set out in Table 4.6 below.

No.	Perceived Problem	Identified by
PP-16	No centralised dashboard displaying security events and alerts from multiple sources	Reflection/Raised at Progress Meeting
PP-17	No log data retention rules; data is kept either until overwritten or for ever.	Reflection/Raised at Progress Meeting
PP-18	No documentation on what security logs and alerts are available.	Reflection/Raised at Progress Meeting
PP-19	No policy on what security logs and data should be enabled; how they should be collected and for how long they should be kept.	Reflection/Raised at Progress Meeting
PP-20	No monitoring of network traffic to understand which systems are generating unusual traffic patterns.	Reflection/Raised at Progress Meeting

Table 4.6 - Additional perceived problems surfaced on reflection

Project Goals

To prioritize these problems a Survey Monkey survey was commissioned and all project participants were invited to take part. The survey asked participants to rate the perceived problem as a key problem, an important problem but not key, or not important. If any perceived problems had been missed by earlier work, these could be proposed as part of the survey.

The top ten perceived problems in ranked order can be found in the table below.

Problem No.	Agreed Key Problems	Survey Response (% agreed key)	Way to address
PP-15	No joined up, correlated overall view of vulnerability across the systems managed by IT.	85.7%	Ensure vulnerability assessment (VA) tools are in scope of data collection
PP-01	No real time security event log reporting or alerting.	71.4%	Dashboard with alerting & reporting functions
PP-02	DC events are not collated.	71.4%	Domain controller (DC) events will be collected
PP-03	No resources to monitor security events.	71.4%	Dashboard with (automated) alerting & reporting functions
PP-04	Security events are not linked to give insight into undocumented service behaviour.	71.4%	Event correlation engine in the selected SIEM will address this

PP-16	No centralised dashboard displaying security events and alerts from multiple sources.	71.4%	The Dashboard element will address this
PP-11	No ability to see patterns of events across multiple systems.	71.4%	Event correlation engine in the selected SIEM will address this
PP-12	No resource available for configuration of highly comprehensive event monitoring & alerting system.	71.4%	This research work will in part address this
PP-13	No visibility of accidental or malicious changes to systems.	57.1%	HIDS element of the selected SIEM or specific Windows file auditing events
PP-10	There is a lack of change auditing for key files (such as configuration files) which hampers accurate change control.	42.9%	HIDS element of the selected SIEM or specific Windows file auditing events

Table 4.7 - Top 10 perceived problems in ranked order

It was agreed by the project team that that targeting the top ten problems would be the goal of the SIEM feasibility project, so these top 10 problems were distilled into five goals as set out in the table below. Note that PP-12 will be addressed through the successful completion of this research work.

No.	Prototype SIEM Project Goals (Evaluation Criteria) – linked to Perceived Problem (PP)
G-1	SIEM must show a correlated view of security vulnerabilities across IT managed systems (PP-15).
G-2	SIEM must provide a dashboard to display security events, log reporting and alerting, including events generated by DCs (PP-01, PP-02, PP-16).
G-3	SIEM must offer automated means to save the time and resources spend on manual monitoring of security events (PP-03).
G-4	SIEM must link events and show patterns across multiple systems (PP-04, PP-11).
G-5	SIEM must give visibility of changes to key system files and visibility of accidental or malicious system changes (PP-10, PP-13).

Table 4.8 - ADR SIEM project goals

Definition of the initial artefact

From these project goals it was possible to derive the selection criteria for the base SIEM system software, to be applied in the BIE Phase of the ADR project.

No.	Base SIEM software selection criteria
SC-1	The SIEM must have a correlation engine to link and analyse events from multiple systems
SC-2	The SIEM requires a dashboard with configurable automated alerting and reporting functions
SC-3	The SIEM must have the ability to collect, parse and correlate Windows Domain Controller events
SC-4	The SIEM must have the ability to incorporate vulnerability assessment tools and/or parse VA data
SC-5	The SIEM must have a Host-based IDS component or the ability to parse Windows file auditing events

Table 4.9 - Base SIEM software selection criteria

Theoretical Basis

As the literature review set out, previous research in the field of SIEM design is limited; and none of what exists was carried out in the context of the SME. Only two papers, Coppolino et al. (2012) and Romano et al. (2012) set out any SIEM-related design principles from their work.

Author	Research Paper	Previous DPs
Coppolino et al. (2012)	A Trusted Information Agent for Security Information and Event Management	3
Romano et al. (2012)	Protecting the WSN Zones of a Critical Infrastructure via Enhanced SIEM Technology	6

Table 4.10 - Previous SIEM research with potential DPs relating to SIEM design

These previous DPs were either tested as part of the SIEM prototype build, or explicit reasons were given why they were disregarded. The results of this DP testing are discussed later and summarized in the Appendix (Table 8.1).

4.4 ADR Stage 2 - Building, Intervention & Evaluation (BIE)

Duration	7 weeks for all 4 phases
Participants	Varied – see sections on each phase of BIE
Purpose	To build the artefact as part of the problem solving intervention & evaluate it

This stage of the ADR seeks to produce the innovative artefact. The BIE stage for this SIEM project was broken into four discrete BIE phases as set out below.

No.	BIE Phase	BIE Phase Purpose
1	SIEM Data Sources	To decide which event data to collect and from where
2	Base SIEM Selection	To decide the base software for SIEM prototype implementation
3	SIEM Prototype Implementation	The implementation of the prototype SIEM
4	SIEM Prototype Evaluation	To determine if the prototype SIEM met the original design goals

Table 4.11 - Sub-phases of BIE

ADR BIE and SMEs

One of the questions surrounding the use of ADR in the context of the SME is which form of BIE the research process followed – IT or Organisation-dominant BIE.

IT-Dominant BIE

This form of BIE is followed when the technology does not yet exist within the organisation. In this case the practitioners and researchers first develop the alpha version of the technology before the beta version of the artefact is presented to the End-Users to evaluate.

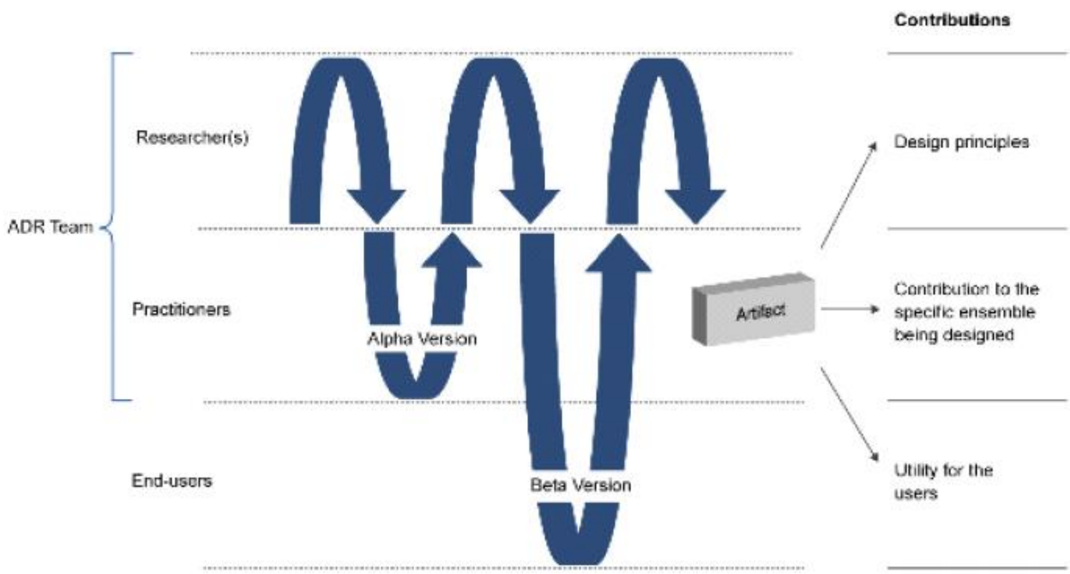

Figure 4.2 – IT-Dominant BIE - from Sein et al. (2011, p. 42)

Organisation-Dominant BIE
If the technology already exists then the End-Users can be involved with the Practitioners and Researchers during both the Alpha and Beta builds and evaluations of the artefact.

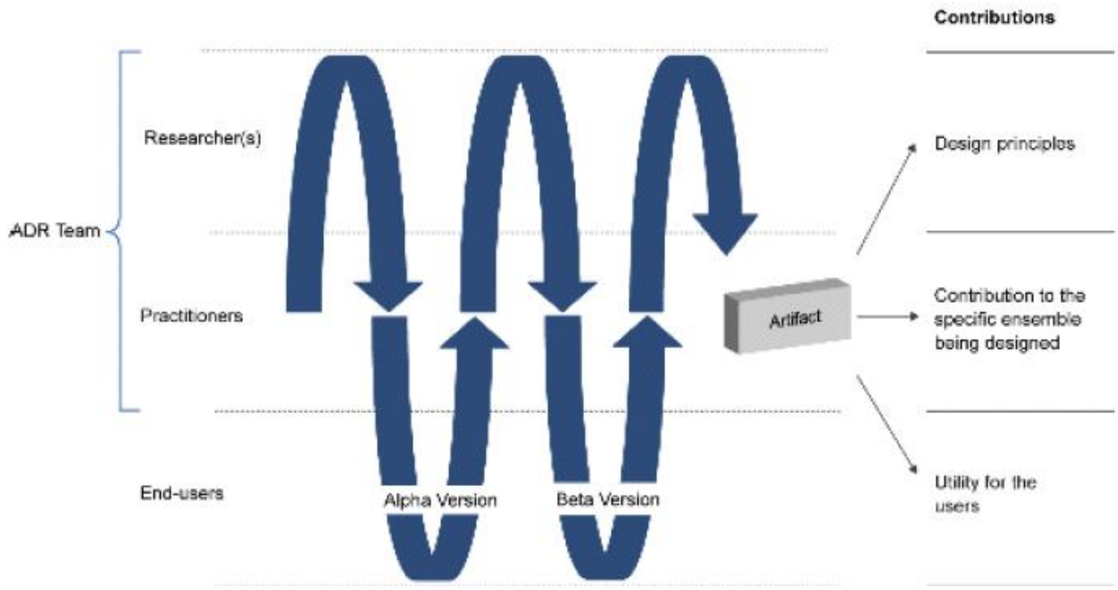

Figure 4.3 - Organisation-dominant BIE - from Sein at al. (2011, p. 43)

A challenge arises over which form of BIE to follow when the Practitioners and the Researchers are also the 'End-Users' of the artefact. This is the case at LTO Limited as the ADR Team consists of both the IT Operations Team and the single Information Security resource – future end-users of the SIEM. Given that SIEM technology did not yet exist in the company, an IT-Dominant BIE form was the most appropriate choice. To delimit the project group into the ADR teams of Researcher, Practitioner and End-User the project team was deliberately broken into the roles set in the Table 4.1.

An additional role of "impartial observer" was created, where the IT Operations Manager, who was familiar with the goals of the work, yet less involved in the daily project operation to see if any additional or interesting insight was generated.

4.4.1 ADR Stage 2 - BIE Phase 1 – SIEM Data Sources

Duration	2 weeks
Participants	Researcher, Practitioners & End Users
Purpose	To decide which event data to collect and from where

Whilst the project team now knew that the SIEM must be able to collect, parse and correlate events from multiple systems (particularly Windows domain controller events), incorporate VA and HIDS features and present alerting and reporting functions via a dashboard, this phase set out to identify the specific data sources that would be within the scope of the prototype SIEM build.

Once the generic data sources were identified and prioritised, this allowed the actual target systems, based upon the agreed scope, to be recorded and therefore candidates for event collection by the SIEM, either through agent installation (event push) or agentless event collection (event pull).

The data collection identification effort followed a similar approach as the one used to identify and prioritise the initial problems the SIEM research will seek to solve i.e. a brainstorming session, followed by reflection, progress meetings and online survey.

Twelve potential data sources were identified during brainstorming (see Table 4.2), which expanded to fourteen after reflection and a follow-up meeting. Four more new potential data sources were identified as a result of the survey. These data sources were prioritised by the project participants into

(a) Key data sources
(b) Important data sources (but not key)
(c) Data not worth collecting.

This was carried out in the survey and in a follow-up meeting, which resulted in a set of prioritised data sources which would form the scope of the prototype build. These data sources are set out in the table below.

No.	Potential Data Source	Survey Response (% agreed key)	Identification Method
DS-01	Windows Domain Controllers (DC)	100%	Brainstorming Session
DS-02	Firewalls	85.7%	Brainstorming Session
DS-03	Bloxx Proxy	28.6%	Brainstorming Session
DS-04	Windows Servers	71.4%	Brainstorming Session
DS-05	HP SIM	28.6%	Brainstorming Session
DS-06	McAfee anti-virus	85.7%	Brainstorming Session
DS-07	Safend endpoint protection	42.9%	Brainstorming Session
DS-08	Check Point IPS	85.7%	Brainstorming Session
DS-09	Desktop Central	42.9%	Brainstorming Session
DS-10	WSUS	50%	Brainstorming Session
DS-11	Nessus	71.4%	Brainstorming Session
DS-12	Cisco switches	42.9%	Brainstorming Session
DS-13	Cisco switch – network traffic information	42.9%	Reflection/Raised at Progress Meeting
DS-14	IIS Web Server logs	71.4%	Reflection/Raised at Progress Meeting
DS-15	VMWare / Virtual Infrastructure logs	Not key for prototype build*	Survey
DS-16	Storage Area Network (SAN) logs	Not key for prototype build*	Survey
DS-17	F5 load balancer logs	Not key for prototype build*	Survey
DS-18	Public-facing DNS servers	Moved into scope by IT Operations Manager*	Survey

Table 4.12 - SIEM data sources

*Discussed post survey in the Progress Meeting

Note that some typical data sources – such as the email systems - were not considered as they have been outsourced so the security event logs were not available for the SIEM prototype build.

Target Systems

It was then important to agree which systems, within the scope of the data source collection, would become targets for event collection by the SIEM. To clarify, one of the project goals was deliver a SIEM which could correlate and link events from multiple systems. An identified source of data was event logs on Windows Servers; and key target systems were the actual Windows Server system names within the network.

Target System Prioritisation

To understand the criticality of the target system the four factors were considered

1. Is the system critical for the company's business operations?
2. Is the system critical for day-to-day IT operational or development tasks?
3. Does the system support a critical system?
4. Does the system contain a key company Information Asset or otherwise sensitive data?

After discussion at a project update meeting the project team identified target systems for each data source. These were then prioritised based upon the need to have a sufficiently wide scope to assess the SIEM prototype verses and the limited time available to complete the project.

The project team understood that some data sources and therefore target systems would not be in scope of the prototype build, but could move into scope in later stages of the ultimate post-prototype (and non-ADR) project work. Similarly it was agreed that if it became clear during the implementation phase that a certain data source or target system was excessively complex or time consuming to implement, it could be taken out of scope of the prototype build. The table of selected target systems in scope for the SIEM prototype build is below.

No.	Potential Data Source	Target System	Reason
DS-01	Windows Domain Controllers (DC)	Main Office Domain Controllers (6 systems)	Domain related security events stored here
DS-02	Firewalls	Firewall Management Server	Stores firewall logs
DS-04	Windows Servers	Finance Software Server Office File Server Office SharePoint Server Office Back-end App Database Server	These systems are containers for important corporate Information Assets (finance data, HR data, business data, and customer data).
DS-06	McAfee anti-virus	ePO management server	Stores anti-malware logs
DS-08	Check Point IPS	Firewall Management Server	Stores IPS logs
DS-14	IIS Web Server logs	Office Share Point Server	Corporate information assets stored in Share Point collaboration software.
DS-18	Public-facing DNS servers	The two Domain Controllers at the Primary and Secondary Hosting centres	Access to the company's external Internet-facing services relies on DNS.

Table 4.13 - Target systems for the prototype SIEM

SIEM Data Source Information Sheet

To help document the decisions made concerning each data source and the associated target systems, a SIEM Data Source Information Sheet (see Table 4.15 below) was designed and populated for the key data sources of the prototype build. During the course of a progress meeting, the high level decisions relating to each data source were discussed, agreed and documented on the sheet. The table below sets out the elements of the data source information sheet.

Data Source Collection – Elements of the Information Sheet	
Data Source Name	Source data type
Reason for data collection	Alert on which events
Target Systems	Action taken on alert
Frequency of data collection	Report type & Frequency
Data Collected through Push (Agent)/Pull (Agentless)	Notes

Table 4.14 - Data Source collection worksheet elements

Once the key data sources and target systems had been agreed, the project team met to agree the scope of the prototype build work and an opportunity was given to revisit any earlier decisions. The project sponsor (the IT Director) was also given the opportunity to ratify the scope of the prototype SIEM build work.

	Description	**Proposed Implementation**
Data Source	Windows Event Logs	The Open Source OSSEC agent will be used to collect, decode, analyse and forward events to the prototype SIEM.
Reason for data collection	Multiple failed user logins indicating an attempt to brute force a system password.	A rule will be created on the prototype SIEM to alert relevant staff if a brute force attack against a system password is detected.
Target Systems (Domain & Systems)	Company HQ Windows domain - Finance application server - HQ fileserver - Application backend DB server - HQ Intranet Server	<u>Company.local domain</u> FINANCE01 (192.168.1.2) FILESERVER01 (192.168.1.3) SQLDB01 (192.168.1.4) WEBSVR01 (192.168.1.5)
Frequency of collection	Real time	Event log data will be sent in real time from the OSSEC agent to the prototype SIEM.
Data Collected through Push (Agent) or Pull (Agentless)	Push from data source	The OSSEC agent will push events to the prototype SIEM over a UDP 1514 network connection, encrypted using zlib through pre-shared Blowfish keys.
Source data type	(Varies by implementation)	The source data will be OSSEC agent logs in ***eventlog*** format (note the alternative SNARE agent forwards logs via syslog).
Alert on which events	Multiple failed user logins	A policy rule will be created within the prototype SIEM to alert on multiple failed logins within a short timeframe.
Action taken on alert	Email Administrators	A policy action within the prototype SIEM will be configured to email the IT Team members when the policy rule above is matched.
Report type & Frequency	Weekly, by email	The prototype SIEM will be configured to generate a weekly report and email the report to IT Team members.
Notes	The OSSEC agent also includes file integrity monitoring and rootkit detection capabilities. It can also be configured to pre-filter certain unimportant events at the agent side to reduce the processing load on the prototype SIEM as well as network traffic.	

Table 4.15 - Sample SIEM Data Source information sheet

4.4.2 ADR Stage 2 - BIE Phase 2 – Base SIEM Selection

Duration	1 week
Participants	Researcher, Practitioners & End Users
Purpose	To decide the base software to use for SIEM prototype implementation

At this stage of the project work, the overall project goals had been agreed, the key data sources and target systems had been identified and the evaluation criteria for the prototype made clear to judge the success or failure of the prototype. The selection of the base SIEM system software was the focus of the second phase of BIE.

In-house developed or off-the-shelf SIEM
With limited access to software development resource, none of which had been allocated to the SIEM feasibility project, the only choice for the project was to implement a third-party developed SIEM and customise it to meet the requirements of the research project.

Open Source or Commercial SIEM
A number of competing SIEM solutions exist, mostly commercially developed, but also two notable Open Source SIEMs were considered options for the project.

After researching the options available through academic literature (Karlzen, 2009), practitioner sources (Gartner, 2012) and vendor web site review (see Table 4.16), six alternative SIEM solutions were shortlisted.

No.	SIEM Vendor	SIEM Name	Licence Model	Link to Vendor Site
1.	Alien Vault	OSSIM	Open Source	http://communities.alienvault.com/
2.	HP	ArcSight Express	Commercial	http://www8.hp.com/us/en/software-solutions/software.html?compURI=1340562
3.	McAfee	Enterprise Security Manager	Commercial	http://www.mcafee.com/uk/products/enterprise-security-manager.aspx
4.	Solar Winds	Log & Event Manager	Commercial	http://www.solarwinds.com/log-event-manager.aspx
5.	Splunk	Splunk for Enterprise Security	Open Source / Commercial (based on data volumes)	http://www.splunk.com/view/enterprise-security-app/SP-CAAAE8Z
6.	Tenable	Security Centre & LCE	Commercial	http://www.tenable.com/products/securitycenter

Table 4.16 - Base SIEM software options for the prototype SIEM build

The set of criteria for the selected SIEM were divided into two parts. Firstly those features or abilities that are essential for the SIEM feasibility project that emerged from the problem identification and prioritisation effort, summarised as selection criteria in Table 4.17. Secondly an opportunity was given to the entire set of project stakeholders to set out their perceived importance of SIEM features in an online survey. Sixteen features were offered for project members to rank.

These selection criteria are shown in the table below.

No.	Selection Criteria for base SIEM	Perceived ADR Team Ranking (1-5, 5 most important)
Criteria Emerging from Perceived Problem Identification		
SC-01	Correlation Engine required	Not part of the survey
SC-02	Dashboard with configurable alerting & Reporting	Not part of the survey
SC-03	Parse MS Windows Server DC events	Not part of the survey
SC-04	Incorporate VA tools (Nessus)	Not part of the survey
SC-05	IDS component or Windows file audit parsing	Not part of the survey
SC-06	Parse MS Windows Server events	Not part of the survey
Criteria Ranked as part of the ADR Team Survey		
SC-07	Ability to integrate with existing infrastructure	3.63
SC-08	The ability to use the SIEM dashboard to display security metrics e.g. viruses detected, firewall blocks etc. all in one place	3.38
SC-09	Easy to customise	3.38
SC-10	The number/type of devices the SIEM can collect, parse and analyse logs from	3.38
SC-11	The ability to edit sources, targets and events for severity/importance to avoid being swamped with events	3.38
SC-12	Cost to purchase and implement	3.25
SC-13	Scalability to cover multiple sites	3.25
SC-14	(Free) built-in sensors such as HIDS, VA, network monitoring, asset discovery tools (so multiple 3rd party tools not required	3.13
SC-15	The people resources needed for training and support	3.13
SC-16	Useful out of the box rules, alerts, reports (to save time)	3.00
SC-17	Number of Events that can be handled per second	2.86
SC-18	The ability to report on compliance and acceptable use	2.50
SC-19	Data retention & archiving mechanisms	2.38
SC-20	SIEM delivery mechanism – is it software, hardware device, VM, cloud, managed service	2.13
SC-21	Equipment required to host SIEM (if relevant)	2.13
SC-22	A built-in ticketing system to deal with alerts/anomalies etc.	2.00

Table 4.17 - Selection criteria for the base SIEM software

Base SIEM Software Evaluation
All six of the potential SIEM applications support the core evaluation criteria, though a difference in the way vulnerability assessment tools integrated with the product was noted. Alien Vault OSSIM and Tenable Security Centre include built-in VA tools, whereas the other four SIEMs only offer the ability to parse VA reports from VA tools.

Given there was no financial budget available for the SIEM feasibility project; and given the IT budget of the company, SIEM solutions with a cost in excess of £20k were considered too high for the company. These products are not targeting the SME end of the SIEM market. Therefore McAfee Enterprise Security Manager, HP ArcSight and Tenable Security Centre/LCE were all dismissed from the evaluation due to cost considerations. Even if a 30 day evaluation of the product had provided the basis of a successful SIEM prototype, the full product would have been beyond the financial means of the SME.

Solar Winds Log & Event Manager does target the SME end of the market, however a 30 node licence is in the region of £3k. It was anticipated that 30 nodes would be insufficient to cover the infrastructure that would be required if a future SIEM was placed into production. In addition, the Alien Vault OSSIM is provided with a number of features and bundled Open Source tools that meet the evaluation criteria set out by the project team (HIDS, VA, network monitoring and asset discovery tools); whereas the Solar Winds product did not. Splunk was also dismissed from the evaluation as although the licencing model starts off free, as processed event log data volumes rise, a threshold is likely to be reached where an expensive commercial licence is required.

The project team agreed that Alien Vault OSSIM was the preferred candidate for the SIEM prototype build as it was free, yet has a commercial option for larger deployments and deployments that require formal data retention and archiving mechanisms.

The Open Source version is limited by the number of sites that can be added to the SIEM architecture as well as providing only a limited number of correlation rules and pre-defined reports. However, for the purposes of this prototype SIEM build and feasibility study, only one site was in focus. Even with a limited rule set and reporting options, the OSSIM should provide the project team with an introduction to SIEM systems, permit the build of a prototype SIEM as well as a pathway to move to a more fully featured, scalable commercial product, should the need arise.

4.4.3 ADR Stage 2 - BIE Phase 3 – SIEM Prototype Implementation

Duration	3 weeks
Participants	Researcher & Practitioners
Purpose	The implementation of the prototype SIEM

With Alien Vault OSSIM as the base SIEM solution, the project team started to implement the customised version of the SIEM for LTO Limited. A total of ten steps were taken to build the prototype over the 3 week period. Whilst reflections related to the BIE of the prototype SIEM are presented in more detail later in this report, observations of note are recorded below.

Troubleshooting Challenges
To help facilitate the build and troubleshoot any technical problems encountered the Alien Vault support forums relating to OSSIM were used as an information resource, though it was noted that the vendor was engaging in a documentation refresh exercise and the support forums and

documentation web site moved during the course of this project. Unfortunately it meant sometimes documents were referenced but not available and made troubleshooting challenging.

Google searches were used to seek solutions to problems, however these often returned articles and forum posts that were either concerning older versions of the product or either partially resolved or completely unanswered. Given that OSSIM is Open Source, support was based upon volunteers and peer users posting answers on support forums. Alien Vault do supply some useful “how-to” and “introduction to” documents and videos; however these sometimes referred to older versions of OSSIM or the Alien Vault commercial product. Although the commercial product is an extension of OSSIM, it has some significant differences that limited the usefulness of some of the provided documentation.

A newer version of OSSIM was released during the course of the implementation phase – which again delayed troubleshooting, as support documents had not caught up with the new version and newer major releases suffer from bugs that are then fixed quickly in subsequent minor releases.

Step 1 – Source and preparation of the hardware
The rack-mounted HP G5 server was allocated to the project with 8GB of memory, 4 x 72GB disks in the internal disk array and an external HP E200i storage system. A four-port PCI-e NIC was sourced to add to the built-in two port Ethernet NIC on board the server. The extra NICs were for future network monitoring of different VLANs using a SPAN port of the core network switches. The firmware of the disk controllers and hard disks was upgraded to the latest available from the HP support web site.

Step 2 – Installation of the Alien Vault OSSIM software
The software was downloaded from the vendor web site and a bootable DVD created to install the product onto the HP server. The OSSIM software was installed as per the installation guide. Features such as Wireless Intrusion Detection were disabled if they were not within scope of the prototype build.

Step 3 – Installation of SIEM agents on test work stations prior to installation on live systems
The three Microsoft Windows server agents that come customised for OSSIM to use are OSSEC, SNARE and OCS NG.

Agent Name	Description	Link to Vendor Site
OSSEC	Host-based IDS, file integrity monitoring & event log alerting for Windows	http://www.ossec.net/
SNARE	Full Windows event log control and redirection to SIEM via Syslog	http://www.intersectalliance.com/projects/SnareWindows/
OCS NG	Windows Inventory agent which details CPU, RAM and software installed	http://www.ocsinventory-ng.org/fr/

Table 4.18 - OSSIM pre-configured event collection agents

These agents were installed on two low risk desktop systems to test their use with OSSIM without risking a software conflict on one of the key target systems.

Each agent was evaluated for the quality of data passed to the OSSIM and any potential to destabilise the system the agent was installed on.

SIEM Agents (OSSEC, SNARE & OCS NG)
The OSSEC agent performed well and immediately began sending useful events to the SIEM server. It was not possible to configure the SNARE agent to connect to the prototype SIEM and given it

replicates some of the features of the OSSEC agent; it was dismissed as a potential event collection agent.

The OCS NG inventory agent worked well and passed regular inventory information to the OSSIM server, however this information was displayed in a separate dashboard that was not linked to the asset database of the SIEM. Therefore it was not possible to link, for example, inbound network attacks seeking to exploit software vulnerability with the installed software on the target system that OCS had collected. This reduced the usefulness of the OCS NG inventory agent as LTO Limited already had a system inventory tool called Desktop Central installed. The project team agreed to move forward with the OSSEC agent as the default agent for event collection for Windows systems.

Step 4 – Network asset scan of the local network with the built-in Nmap scanning tool
The network ranges that were in scope for event collection by the SIEM prototype build were configured and the built-in Open Source Nmap network scanning tool was run against the selected networks to identify alive systems on the network, name them using DNS lookups and attempt to identify the operating system.

At the point of starting the Nmap scan, even on the least aggressive and less comprehensive service checks, the entire SIEM system ceased to be responsive. The reported memory in use jumped to 100% and remained ‘flat-lined’ during the course of the scan. These scans took so long to complete – one was cancelled after 18 hours through a manual reboot of the SIEM server – that project members began to question the choice of Alien Vault OSSIM as the base SIEM software for the project.

The solution to this problem was to upgrade the server hardware from 8GB to 20GB and from this point on the SIEM server and dashboard were sufficiently responsive, even during these network scans.

Step 5 – Vulnerability scan of the local network with the built-in Nessus VA tool
Alien Vault OSSIM includes both Nessus and Open VAS vulnerability scanning tools. Given the company already had experience with Nessus, a test scan was completed against the subset of network systems that were event collection targets for the prototype build. The scan completed successfully and gave immediate value by identifying vulnerabilities in the HP SIM server and company Share Point server.

Step 6 – Installation of the OSSEC agent on a low-risk subset of target systems
Once step 3 confirmed that the OSSEC agent was unlikely to destabilise one of the target Windows server systems, a subset of the lower-risk target systems were identified and the OSSEC agent was installed on them and monitored for five days for any system instability.

The approach to agent installation here was where there were two servers, such as two domain controllers, one of the servers had an OSSEC agent installed and the other was run without an agent to avoid the risk of agent install taking both systems off-line.

Step 7 – Configuration of the email relay mechanism and set up of real-time alerting
The ability to automatically alert security and operations teams when certain important events occur is a key feature of any SIEM system. To show value it was important to enable this aspect of the prototype SIEM.

Unfortunately the configuration of the service was not straightforward. The management dashboard required mail server credentials to be entered, but the company mail server relied on anonymous internal emailing for infrastructure system mail relaying. After troubleshooting at the network level using telnet to the SMTP server, followed by troubleshooting of the Postfix mailer system built into the SIEM it became apparent that the fault lay with the SIEM software, rather than the mail subsystem, the network or the mail relay server.

Eventually it became possible to trigger an alert using a test rule to send an alert on network login, however other features of the mailing facility, such as emailing historical event collection reports to project participants, were still not operational, even by the time the prototype build completed.

Step 8 – Configuration of the OSSIM to collect malware events from the McAfee ePO server
With the help of the database administration team it was possible to configure the OSSIM server to collect the malware-related events directly from the ePO server on the network and feed these into the correlation engine of the SIEM.

This immediately triggered some alerts that highlighted a misconfiguration in agent policy that still caused a "block" alert to be sent for a protection mechanism that had been disabled. In addition, when the SIEM event collection from ePO was tested with the EICAR anti-virus test string, it was noted that inbound "virus alert" email to the security manager's inbox were being blocked as 'junk mail'.

One issue with the McAfee ePO log monitoring was that the logs all appear in the dashboard as UCT time, not local time. This meant it was not easy to link system events manually (in BST) with the times on the McAfee event log (in UCT) as they were one hour apart. This does not impact automatic event correlation by the SIEM, but is a consideration when manually analysing the logs.

Step 9 – Importing of Check Point firewall logs from the firewall management server
This step became one of the most time consuming parts of the three week implementation phase. Numerous sources of information were reviewed for information to assist; the Check Point OPSEC tools were installed on the SIEM and the Check Point firewall management server was configured as per the guide on the support forum, however after days of configuration checking and alterations based on advice in forum posts, it was not possible to extract the firewall and IDS logs.

Firewalls are a key data source for SIEM event correlation, both with regards to inbound attack recording/blocking, to logging of outbound access to web sites that might be a cause of malware infection. Enabling this data source would be a priority in any later stages of a post-prototype SIEM implementation.

Step 10 – Installation of OSSEC agent on the remaining target systems
Once the OSSEC agent had run successfully for a week on low-risk workstations and then on a subset of key target servers for another week, it was safe enough to install the agents on the remainder of the key target servers to permit the event log collection of all the Windows server target systems that were required as part of the SIEM prototype evaluation.

4.4.4 ADR Stage 2 - BIE Phase 4 – SIEM Prototype Evaluation

Duration	1 week
Participants	Researcher, Practitioners & End Users
Purpose	To determine if the prototype SIEM met the original design goals

Once the prototype SIEM was built, all of the ADR Team (including 'End-Users' or those IT

Operations staff who had not been involved heavily with the implementation work) were asked to take an online survey whilst running through a set of instructions based upon whether the SIEM prototype was capable of solving the 10 key problems distilled into five project goals earlier in the project.

The questions and activities carried out by the ADR Team are recorded below. Participants were also given the opportunity to offer comments on why they scored each question as they did. Each question in the survey required the participant to login to the SIEM and navigate around the dashboard.

Questions relating to the Project Goals/Perceived Problems the SIEM should solve

Q1. Problem - "No correlated view of vulnerability across IT Managed Systems" (PP-15)
The ADR team were asked to navigate to the display relevant to discovered vulnerabilities, find a specific system, drill into the report and use the event filters to find a specific vulnerability with that system. The participants were then asked to review the ticket that had been raised automatically by the vulnerability scan.

The participants were asked “does this prototype SIEM show the potential to give a joined-up and correlated view of security vulnerability across IT managed systems?” and the survey responses were summarised below.

Participant View (PP-15)	Strong Yes	Yes but needs tuning	No
% of responses	43%	57%	0%

Participant Commentary:
- One participant expressed concern that the IT team will have little time to fix the vulnerabilities that the vulnerability scanner surfaces.
- Concern that the reporting of these vulnerabilities as displayed by the SIEM might give a flawed view of IT Operations and lead management to think they were not doing a good job. Some context would be needed to be added to the report, such as why some software was still running on older versions.
- The SIEM should provide the ability to ignore some warning messages if the vulnerabilities are known and already accepted.

Q2. Problems - "No real time security event log reporting or alerting or DC event collection and no centralised dashboard to see these events" (PP-01, PP-02, and PP-16)
The ADR team were asked to navigate to the display showing security events arriving into the SIEM in real time as well as historical events. The participants were also asked to drill down into the specific Windows Logon Failure security events generated by the DCs and identify the user account for the failed logon. It was acknowledged that the email alerting mechanism was not yet functional, however the survey participants were shown how the event could trigger an email alert.

The participants were asked “does this prototype SIEM show the potential to provide real-time security event reporting and alerting, DC event collection and a centralised dashboard to see these events?” and the survey responses were summarised below.

Participant View (PP-01, PP-02, PP-16)	Strong Yes	Yes but needs tuning	No
% of responses	43%	57%	0%

Participant Commentary:
- Shows promise but would like alerting for failed logins to be functional

Q3. Problem - "No people resources to monitor security events" (PP-03)
The ADR team were asked to navigate to the display showing Alarms, Tickets and Reports. After reviewing each display the participants generated a historical report of SIEM events and downloaded the PDF. It was again acknowledged that the email alerting mechanism was not yet functional, however the survey participants were shown how to configure automated reports.

The participants were asked "does this prototype SIEM show the potential to automatically trigger alerts for important security events and provide automated reports of historical events, saving the time of manual security event monitoring?" and the survey responses were summarised below.

Participant View (PP-03)	Strong Yes	Yes but needs tuning	No
% of responses	14%	72%	14%

Participant Commentary:
- Concern over time to maintain the SIEM and action the alerts that have been triggered
- The SIEM needs a formal support contract in place rather than the peer forum support from Open Source software, otherwise time is spent troubleshooting unnecessarily.

Q4. Problem - "Security Events are not linked and no ability to see patterns of events across multiple systems" (PP-04, PP-11)
The ADR team were asked to navigate to the display showing cross correlation reports that linked a SNORT detected IDS event with a Nessus vulnerability found to trigger an alarm. The participants were shown how multiple rules could be written to trigger alarms when a sequence of activities are detected, such as a user logon to a key file server and then a registry change taking place.

The participants were asked "does this prototype SIEM show the potential to link security events so patterns of events and activity across multiple systems become visible?" and the survey responses were summarised below.

Participant View (PP-04, PP-11)	Strong Yes	Yes but needs tuning	No
% of responses	57%	43%	0

Participant Commentary:
- Concern that the utility here is governed by the rules manually set up by IT Operations and therefore the time that would be needed to set these correlation rules up.

Q5.Problems - "No change auditing for key system files and visibility of accidental or malicious system changes" (PP-10, PP-13)
The ADR team were asked to navigate to the display showing the configuration related to host-based IDS agents and events generated relating to registry changes and changes to key system files. The participants were also shown the key files monitored by default on the installed OSSEC agents and how additional files could be added to this list.

The participants were asked "does this prototype SIEM show the potential to audit and alert on changes made accidentally or maliciously to the system registry and key system files?" and the survey responses were summarised below.

Participant View (PP-10, PP-13)	Strong Yes	Yes but needs tuning	No
% of responses	43%	43%	14%

Participant Commentary:
- Concern over the time to set up the files to be monitored on each of the OSSEC HIDS agent

Additional Questions

The participants were then asked for their views on continuing the project beyond the initial prototype build.

Q6. Should the SIEM project should continue beyond the prototype build?

Participant View	Strong Yes	Yes	No
% of responses	14%	72%	14%

The participants were also asked how they felt about building the SIEM as part of a research project using ADR.

Q7. Do you feel the additional rigor, documentation and discipline of the ADR process resulted in a better outcome for the SIEM design and implementation?

Participant View	Strong Yes	Yes	No difference	Worse outcome
% of responses	100%	--	--	--
Participant Commentary: The additional rigor helped maintain focus Running the project in this way legitimised the effort put in				

The participants were finally asked for their views on what they liked about the SIEM prototype, what they disliked, what must be working in the next phase if the project moves forward and any other observations about the prototype SIEM.

	Participant Commentary
Like	The interface is fast, clean and easy to read The dashboard displays are layered well The dashboard looks professional and clutter-free The graphs are slick The built-in SNORT IDS and OSSEC HIDS
Dislike	The dashboard is too busy and not very intuitive Too many alerts are displayed and the filtering is not easy Finding the right information quickly is not easy – it takes too long to drill down into the interface The dashboard is not as straight-forward to use as expected.
Next phase must include	Email alerting must work Firewall log collection Log collecting from the virtual infrastructure The Internet-facing systems must be data sources Remote sensors needed at the production and DR hosting facilities Intrusion-prevention logs Alerts on file-access denied security events Alerts on specific Windows security events
General Observations	Concerns that the SIEM will be 'another tool where only a small fraction of the possible features are actually used' Security, not IT Operations, focussed tool Participants have much better understanding of SIEM technology and potential usefulness in the SME context The commercial SIEM with formal support mechanisms is preferable to Open Source.

Table 4.19 - Prototype SIEM evaluation survey - participant commentary

4.5 ADR Stage 3 – Reflections & Learning

Throughout the course of the ADR project, the following reflections were recorded.

Reflections on Problem Identification, SIEM Data Source & Target System Selection

No.	Reflection
R-01	Perceived problems still emerged after the initial problem identification related engagement was complete; therefore it is important to identify all stakeholders as early as possible and run several iterations of problem identification before proceeding with the design.
R-02	The initial choices of key target data sources changed during the prioritisation process as the underlying systems of these target data sources had been ignored; therefore it is important to ask 'that system is critical, but what does it rely on; and what does that itself then rely on?'. An example – initially the finance server was identified as a critical data source, which is a Windows system, but it is a virtual machine that relies on VMware; and that itself relies on the Storage Area Network (SAN); and that SAN relies on its hardware system. All of these underlying infrastructure systems are capable of generating security-related events which should be considered in the prioritisation process.
R-03	The perceived prioritisation and selection of key data sources was influenced by the job role of the stakeholders. Those staff who maintained web servers prioritised these data sources over internal network systems; whereas those who supported internal systems prioritised these ahead of the web servers. Therefore, to engage all stakeholders and demonstrate the utility of the artefact prototype, these differing views should be factored into the ultimate selection of the initial data sources.
R-04	Candidate key target data sources continued to emerge after key target data source identification and prioritisation process was complete; therefore it is important to identify all candidate data sources as early as possible and run several iterations of target data source identification before proceeding with the design.
R-05	Initially selected key data sources had to be removed from prototype scope during artefact implementation as event collection was not technically possible by the selected SIEM software or was too complex and time consuming to be feasible in the time frame available to the prototype build. Therefore it is important to choose target data sources in the initial implementation phase that will be technically feasible to support in the available time frame.
R-06	Upon initial implementation of just eight key target data sources, the volume of data generated for analysis by the artefact was significant. Therefore to keep stakeholders engaged, enthusiastic and to increase the prospect of a successful prototype build in a challenging timeframe, the initial data source scope should be kept as *small as possible* (yet large enough to judge the success or failure of the prototype build).
R-07	A SIEM data collection sheet was used to document the key data sources of the SIEM, which target systems will supply the data and how the data is collected and various other aspects of the data collection related to that data source. This applied some rigor to the data collection and a tangible source of information for project participants concerning each data source.

Table 4.20 - Reflections on Problem Identification, SIEM Data Source & Target System Selection

Reflections on SIEM Implementation

No.	Reflection
R-08	Although initially dismissed as unimportant and already provided through a manual spread sheet based process, asset identification emerged as key to the SIEM operation as without it events could not be correlated. Therefore ensure asset identification is a core feature of SIEM selected.
R-09	When initially built with twice the suggested RAM memory the artefact performed poorly during certain operations with memory usage at 100%. This lead to criticism of the artefact and delayed the evaluation of the feature under analysis. By adding the maximum memory available (from 8GB to 20GB) this performance bottleneck was overcome. Therefore to prevent performance issues that delay the project work and demotivate participants, the maximum RAM available should be installed into the SIEM.
R-10	Whilst the key features of a SIEM is to collect, correlate, manage, alert and report on security-related log events, a number of the additional functions appealed to the project stakeholders as this functionality was not yet deployed in the SME and was available through one artefact. Therefore to encourage SME project team buy-in, consider the range of features available to the SIEM product, particularly features the project team may see as desirable or currently missing when selecting the SIEM.

Table 4.21 - Reflections on SIEM Implementation

Reflections on the SIEM Project Process in an SME Context

No.	Reflection
R-11	Running an ADR project with the additional rigor, discipline and documentation overhead was novel to the members of the SME stakeholder team and at any one time 60% of the project team of nine people working on the build of the project were unavailable due to troubleshooting IT failures, sickness, holiday, training or competing resource demands. Therefore this unfamiliarity with the additional requirements of such a research project and the potential resource challenges in this SME context should be factored into the scope and goals of the project phases. It is possible less progress will be achieved than expected.
R-12	When it became apparent that some of the initial expectations regarding the ultimate utility of the proposed artefact were higher than the artefact was likely to deliver, the enthusiasm of the project team faded. Therefore initial expectations should be set appropriately to avoid any demotivation as the project progresses.
R-13	Early in the project the ultimate operational benefits (rather than security benefits) of the proposed artefact were advertised and regularly reiterated which ensured buy-in by the project stakeholders (who were mainly operational, not security focussed). Therefore promoting the benefits that resonate most with the core project team is key for project member engagement.
R-14	To keep the interest and engagement and demonstrate utility, when findings related to operational benefits emerged, they were advertised and reiterated to show value and ensure on-going stakeholder buy-in. Therefore keeping a steady flow of demonstrated benefits of the artefact to the project team is important to maintain project team enthusiasm.

R-15	By choosing the financially less expensive open source SIEM solution, the project suffered through the lack of comprehensive documentation (documentation was either for earlier versions or for the commercial version of the SIEM), the lack of a dedicated helpdesk (support was via volunteer forums), the recent web site migration of historical support forums to a new, yet to be fully populated version and the fact the features and versions of the product changed during the course of the prototype build. Therefore the potential lack of system documentation and support resource for Open Source solutions should be factored into the selection process of the SIEM as it can impact productivity and delay project progress as project members struggle to find solutions to technical challenges during the implementation of the artefact.

Table 4.22 - Reflections on the SIEM project process in an SME context

These reflections were distilled into a set of potential Design Principles (DP) set out in Stage 4.

4.6 ADR Stage 4 – Formalisation of Learning

Below are the list of potential Design Principles. These were presented to the set of ADR Practitioners that formed the part of the ADR Team and their levels of agreement with the proposed Design Principle are listed underneath each principle.

Proposed Design Principles Related to Problem Identification & SIEM Data Source Selection

Design Principle	Description		
DP-01. All stakeholders should participate in both initial problem definition and selection of key data sources. (Reflection R-01, R-03 and R-04)	- Use all available communication methods (e.g. email, group meeting, 1-1 and survey) to allow the voices of all stakeholders to be heard. - Run the selection and prioritisation process through several iterations to refine earlier selections. - Allow stakeholders to reflect on, challenge and revisit choices.		
Practitioner View of DP1	**Strong Yes**	**Yes**	**No**
% of responses	75%	--	25%

Design Principle	Description		
DP-02. The underlying infrastructure of a proposed data source should be considered as a potentially more important data source. (Reflection R-02)	- Underlying infrastructure, such as the virtual machine control system or disk storage system can be an even more importance source of security events than the initially identified data source. - When a potentially key data source is identified ask "what does it rely on?" and when this is identified, ask the question again.		
Practitioner View of DP2	**Strong Yes**	**Yes**	**No**
% of responses	50%	25%	25%

Design Principle	Description		
DP-03. Initial data source selection scope should be kept as small as is practicable to provide enough information on the potential utility of the prototype. (Reflection R-05, R-06 and R-12)	- A limited set of data sources should reduce information overload and a subsequent negative responses from the prototype build participants. - Choose only enough data sources to permit evaluation of the key features of the prototype.		
Practitioner View of DP3	**Strong Yes**	**Yes**	**No**
% of responses	100%	--	--

Design Principle	Description		
DP-04. A SIEM data collection sheet should be used to document the agreed aspects of the data collection concerning each data source. (Reflection R-07)	- A SIEM data source collection sheet adds rigor to the process of agreeing important aspects of data collection such as which target systems will act as data sources, how the data will be collected, how often, by agent or agentless. - This data source collection sheet should also include details of which events should trigger an alert, what action should be taken and if and when any regular reports are required.		
Practitioner View of DP4	**Strong Yes**	**Yes**	**No**
% of responses	75%	25%	--

Proposed Design Principles Related to SIEM Implementation

Design Principle	Description		
DP-05. Asset identification should be considered key to the successful operation of the SIEM. (Reflection R-08)	- The asset identification features of the SIEM should not be dismissed as of peripheral importance. To correctly correlate security events (such as vulnerability scanning, with inbound attacks with detected viruses) the asset database must be accurately populated.		
Practitioner View of DP5	**Strong Yes**	**Yes**	**No**
% of responses	100%	--	--

Design Principle	Description		
DP-06. The maximum possible physical memory should be made available to the SIEM (Reflection R-09)	- Insufficient memory will reduce the performance of the artefact and negatively impact the stakeholder views of the artefact and discourage their involvement with the work. - Without sufficient memory certain features will be less performant and the evaluation of these features will take longer and result in inaccurate conclusions around the utility of the artefact.		
Practitioner View of DP6	**Strong Yes**	**Yes**	**No**
% of responses	100%	--	--

<table>
<tr><th>Design Principle</th><th colspan="3">Description</th></tr>
<tr><td><u>DP-07</u>. The additional ‘non-typical’ SIEM features should be promoted to the project stakeholders.

(Reflection R-10)</td><td colspan="3">- Project stakeholders value the additional features of the SIEM, particularly if previously not deployed.

- Where features are already provided by currently deployed technology, there is a feeling of re-inventing the wheel, which devalues the SIEM.

- Leverage the fact that the artefact can deliver these extra features with just one dashboard.

- Examples of these additional features include HIDS, vulnerability scanning, automatic inventorying, file integrity checking.</td></tr>
<tr><th>Practitioner View of DP7</th><th>Strong Yes</th><th>Yes</th><th>No</th></tr>
<tr><td>% of responses</td><td>50%</td><td>50%</td><td>--</td></tr>
</table>

Proposed Design Principles Related to SIEM Project Process in an SME

<table>
<tr><th>Design Principle</th><th colspan="3">Description</th></tr>
<tr><td><u>DP-08</u>. The operational benefits of the SIEM should be promoted to the IT function ahead of security benefits to encourage IT function buy-in.

(Reflection R-13)</td><td colspan="3">- The SME IT function is largely operations focused with at most one dedicated security resource. To encourage project stakeholders to prioritise project work against competing resource demands, promote the operational efficiency benefits of the SIEM.

- Whilst security is seen to be important; features that save operator time such as automating daily morning system checks or reducing the number of dashboards to monitor are viewed as directly more valuable to SME IT staff.</td></tr>
<tr><th>Practitioner View of DP8</th><th>Strong Yes</th><th>Yes</th><th>No</th></tr>
<tr><td>% of responses</td><td>75%</td><td>25%</td><td>--</td></tr>
</table>

<table>
<tr><th>Design Principle</th><th colspan="3">Description</th></tr>
<tr><td><u>DP-09</u>. The operational benefits of the artefact should be regularly fed back to project participants as they emerge.

(Reflection R-14)</td><td colspan="3">- To keep operationally-focussed project members engaged, continually promote the benefits of the artefact as it is built and they are discovered.

- Examples might be the errors in system or service configurations that emerge from the log analysis and alerting that the SIEM provides.</td></tr>
<tr><th>Practitioner View</th><th>Strong Yes</th><th>Yes</th><th>No</th></tr>
<tr><td>% of responses</td><td>50%</td><td>50%</td><td>--</td></tr>
</table>

SIEM Planning & Implementation Checklist
One of the project outcomes of benefit for Information Security practitioners is the planning checklist for SIEM implementation forming Table 4.23 below.

This checklist was prepared using the results of this research and information taken from Miller et al. (2011), Gordon (2010) and Brandel (2009). These sources are cited in the table alongside additional checklist items that have emerged from this research project.

No.	Checklist Element
1.0	**Agree Project Stakeholders**
1.1	Identify all potential stakeholders in the SIEM design & implementation to involve them in the problem identification/SIEM requirements/prioritisation. (Brandel, 2009)
1.2	Agree roles & responsibilities for the work and who will be involved in agreeing the requirements, implementation and evaluation of the SIEM.
1.3	Agree communication channels for the work and frequency of communication.
2.0	**Define why you need a SIEM**
2.1	Agree the security/operational event collection problems do you need to solve
2.2	If the organisation must meet PCI or ISO standards compliance collect the exact requirements of these standards, such as log storage. (Gordon, 2010)
2.3	Is incident reporting key? If so, focus on historic reporting. (Gordon, 2010)
2.4	Is incident handing key? If so, focus on real-time alerting. (Gordon, 2010)
2.5	Is the ability to gather forensic evidence important? (Gordon, 2010)
2.6	What additional features of a SIEM may be valuable, such as built-in vulnerability scanning, availability monitoring and network traffic monitoring. (Gordon, 2010)
2.7	Prioritise the problems to solve and SIEM features to implement.
3.0	**Agree the data sources of the SIEM**
3.1	Which network devices (e.g. firewalls, switches, proxies) will be data sources? (Miller et al., 2011. Gordon, 2010)
3.2	Which servers will be data sources & which operating systems do they use? (Miller et al., 2011. Gordon, 2010)
3.3	Which network monitors will be data sources e.g. IPS, netflows, Ntop? (Miller et al., 2011. Gordon, 2010)
3.4	Which applications will be data sources? In house or commercial applications? (Miller et al., 2011. Gordon, 2010)
3.5	Revisit the list of data sources based upon underlying infrastructure e.g. underlying SAN or virtual infrastructure
3.6	Prioritise the data sources of the SIEM looking to minimise data overload
4.0	**Agree the target systems of each type of data source**

4.1	Which specific systems will be within scope of the event collection? (Miller et al., 2011. Gordon, 2010)
4.2	Which system events will specifically need collection? E.g. failed logins? (Gordon, 2010)
4.3	Will the target systems push the events to the SIEM (agent-based collection) or will the SIEM pull them (agentless collection) from the target systems? (Miller et al., 2011)
4.4	Calculate the number of events per second (EPS) the SIEM will need to handle? (Gordon, 2010)
4.5	What type of alerts will need generation based on the specific events collected? E.g. email alerts, SMS messages or the running of a script? (Gordon, 2010)
4.6	What types of reports will need to be created (content and frequency) based upon the events the target systems will generate? (Gordon, 2010)
4.7	What action are human stakeholders required to take when certain events, alerts or reports are generated? (Gordon, 2010)
4.8	Create a Data Source Collection Sheet, populated with Target Systems for each Data Source
4.9	Prioritise the target systems and consider a phased approach to keep event numbers low in prototype and initial production phases.
5.0	**Agree the selection criteria for the SIEM**
5.1	Can the SIEM collect, correlate and analyse the events of the target systems identified? (Brandel, 2009)
5.2	Can the SIEM support the number of expected EPS? (Gordon, 2010)
5.3	Will the SIEM provide the additional features required? E.g. vulnerability scanning? (Gordon, 2010)
5.4	Is the SIEM easy to customise? (Brandel, 2009)
5.5	What is the cost to purchase and deploy the SIEM? (Gordon, 2010)
5.6	Will the SIEM be an open source or commercial product? (Gordon, 2010)
5.7	What is the scalability of the SIEM and ability to factor in growth over the lifetime? E.g. increased EPS or multiple sites. (Brandel, 2009)
5.8	What are the training requirements and on-going support requirements - both in-house support and vendor-based support? (Brandel, 2009)
5.9	How useful are the out-of-the-box pre-configured rules around alerting and reporting? (Miller et al., 2011)
5.10	Does the SIEM include a built-in ticketing mechanism? (Miller et al., 2011)
5.11	How is the SIEM delivered? Is it hardware, software or a virtual hardware device? (Brandel, 2009)
5.12	What equipment is required to host the SIEM? (Gordon, 2010)
5.13	Does the SIEM include a dashboard to show events, generate reports and configure the system? (Miller et al., 2011. Gordon, 2010)
5.14	What features of the SIEM dashboard are useful?
5.15	Can the SIEM be evaluated prior to implementation and is the evaluation version limited in functionality?

5.16	Can the SIEM meet the alerting and reporting requirements of the project? (Gordon, 2010)
5.17	Does the SIEM permit the administrative granularity that may be required in an organisation e.g. multi-site, multi-admin organisation? (Gordon, 2010)
5.18	Once the SIEM is selected agree the evaluation criteria for the selected SIEM after prototyping or initial deployment. (Gordon, 2010)
6.0	**Implementation of the SIEM**
6.1	Use a network map to break down assets into specific groups.
6.2	Understand the administrative model for the organisation and group assets accordingly.
6.3	Understand how business processes may affect implementation e.g. the SIEM may assist daily morning checks.
6.4	Prepare the underlying hardware the SIEM will use, including network taps or mirror ports for network monitoring.
6.5	Install the SIEM software and configure appropriately, including system configuration such as time synchronisation and alerting mechanisms such as email.
6.6	Install the SIEM agents on a test system and start collecting events.
6.7	Asset scan the network to populate asset groups.
6.8	Run a vulnerability scan to import or generate vulnerability information for the assets.
6.9	After a period of stability using test systems, install agents on low risk systems and collect events.
6.10	After a period of stability using low risk systems, install agents on the remaining target systems and collect events.
7.0	**Evaluation and acceptance of the SIEM**
7.1	Evaluate the SIEM against the criteria set in 5.18
7.2	Consider re-visiting earlier steps 3 (Data Sources) and 4 (Target Systems) now the capabilities of the SIEM are clearer.
7.3	Move forward to the next phase of the project e.g. wider range of target systems or additional SIEM features deployment.

Table 4.23 - SIEM Planning & Implementation checklist

5. DISCUSSION

This chapter discusses of the outcomes of the SIEM prototype build, links the proposed Design Propositions to academic theories and comments on the usefulness of ADR as a research methodology in the context of the SME research project. Finally the outcomes of the research are considered in the context of IT and Open Source Software adoption in SMEs.

Four aspects of the results merit discussion: SIEM design and implementation, the use of ADR in an SME context, IT adoption in an SME context and Open Source Software (OSS) adoption in an SME context.

5.1 SIEM Design & Implementation

The Design & Implementation of the SIEM was possible
The research project demonstrated that it was possible to design and implement a prototype SIEM for an SME that met the initial goals to address the prioritized perceived problems listed in Table 5.1 below,

No.	Prototype SIEM Project Goals (Evaluation Criteria) linked to Perceived Problems (PP)
G-1	SIEM must show a correlated view of security vulnerabilities across IT managed systems (PP-04, PP-11)
G-2	SIEM must provide a dashboard to display security events, log reporting and alerting, including events generated by DCs (PP-01, PP-02, PP-16)
G-3	SIEM must offer automated means to save the time and resources spend on manual monitoring of security events (PP-03)
G-4	SIEM must link events and show patterns across multiple systems (PP-15)
G-5	SIEM must give visibility of changes to key system files and visibility of accidental or malicious system changes (PP-10, PP-13)

Table 5.1 - Project goals and perceived problems

Whilst the majority of the project members (the “End Users”) surveyed agreed the project goals were met, all agreed the SIEM prototype requires further tuning to be as effective as possible in addressing the perceived problems.

The project members also expressed a concern over the level of people resources needed to carry out this further tuning of the prototype SIEM and then the likely amount of people and time resource needed to fine tune, maintain operation and improve the SIEM in the future.

Concerns were also raised over the informal nature of the technical support available for this Open Source SIEM; project members noting that the detail, quality and availability of documentation related to the SIEM was poor, expressing a preference for the commercial software support mechanisms such as telephone and email-driven helpdesks, ticket systems and comprehensive technical documentation.

The volume of events detailed by the system dashboard were cited as an issue and project members remarked that finding the specific ‘interesting’ information amongst the volume of events was a challenge, particularly due to some idiosyncrasies of the event filtering mechanism and perceived deficiencies around the SIEM dashboard; the dashboard displaying too much data, not intuitive and difficulties drilling down to the important data.

Interestingly, a number of the SIEM evaluators expressed an opposite opinion, in that the dashboard was fast, layered well, professional, clutter-free and easy to read, with slick-looking automatically generated graphs to display the information cleanly. Clearly more research might be desirable to understand why evaluators held these opposing views.

One project participant also voiced concerns that by making visible the correlated view of system vulnerability (and addressing PP-15); the IT Operations team would be expected, but not have the resources, to fix the vulnerabilities identified, possibly giving a negative impression to management on the effectiveness of the team. This is a curious observation, given that the IT Operations team initially agreed that no correlated view of system vulnerability was the most important perceived problem to address.

The additional features of the implemented SIEM were perceived by some members of the project team to be useful. The built-in Snort IDS and OSSEC HIDS were both cited as examples of valuable features bundled with the OSSIM software, that other evaluated SIEM solutions did not provide.

Clearly it was not possible to satisfy every stakeholder of this SIEM research project while a small number of participants left the project impressed with what the SIEM prototype offered and a small number left unimpressed with the prototype SIEM, the majority felt the SIEM offered value in addressing the perceived security event management problems, but only if time and resources were made available and a number of key features were made operational.

Perhaps the variation in satisfaction and enthusiasm for the SIEM project can be linked to the work on changing organisational routines by Feldman and Pentland (2003). Routines and operating procedures – such as those related to daily system checking and security log management – can be a source of stability and lead to inertia and mindlessness. Staff prefer easy, repetitive actions and whilst the research project participants acknowledge the shortcomings of the current routines, they may resist any plans to vary them.

Indeed, according to Feldman and Pentland (2003) changes in organisational routines often result from managerial pressure to improve performance, exert control and monitor compliance, which can lead to feelings of anxiety and loss of security amongst those who operate the routines. Interestingly, the most enthusiastic supporters of the SIEM project work were the IT Operations Manager and the IT Security Manager. The least enthusiastic members of the SIEM project team – who continued to point out the limitations and time and resource overheads of the solution – were those project team members from IT Operations who would ultimately be involved in the maintenance, fine tuning and operational routines of the SIEM if the project moved beyond the prototype stage and towards a live, production SIEM system.

Project members were not asked directly about the perceived usefulness of Survey Monkey as a tool to gather project member views, however the researcher felt that this online survey tool helped significantly to address the difficulty of gathering all project participants from a very busy SME IT Operations team in one place at the same time. Without Survey Monkey it would have taken far longer to collect views, agree priorities and evaluate the final SIEM prototype.

Ultimately 86% of the ADR team surveyed felt that the project should continue past the prototype stage to move the SIEM into production, though 72% set out a number of caveats that resources must be available and certain features must be made operational in future SIEM work within LTO Limited.

Validation of Previous DPs
Originally the research project set out to design and implement a prototype SIEM in the context of an SME, using and potentially validating design principles from earlier SIEM research.

Of the twenty SIEM papers identified in the literature review, only two previous examples of SIEM research (Romano et al., 2012 and Coppolino et al., 2012) explicitly generated design principles related to SIEM design and implementation. These nine Design Principles are documented in Table 24, located in the Appendix.

As this project progressed it became apparent that the scope precluded the testing of seven of these nine design principles. Examples of design principles that could not be tested included those related to physical location of sensors, fault tolerance and high volume event processing environments. It was possible to validate two of the nine previous design principles through the SIEM design and implementation as part of this research project, also documented in Table 8.1 of the Appendix.

As this research project has generated nine design principles explicitly relevant to the SIEM design and implementation in an SME context and the focus of this discussion lies on these.

DPs & related theory
The fifteen reflections made by the research team during the course of the project fell into three areas – firstly reflections related to the initial problem identification, SIEM data source and target system selection, reflections on the SIEM prototype implementation itself and finally reflections concerning the running of this SIEM research project in the context of an SME.

These reflections were condensed into nine proposed Design Principles that are believed to be generalizable to SIEM design and implementation within the SME context and indeed generalizable to a wider context of SIEM design and implementation in *all* contexts.

No.	Design Principle
DP-01	All stakeholders should participate in both initial problem definition and selection of key data sources.
DP-02	The underlying infrastructure of a proposed data source should be considered as a potentially more important data source.
DP-03	Initial data source selection scope should be kept as small as is practicable to provide enough information on the potential utility of the prototype.
DP-04	A SIEM data collection sheet should be used to document the agreed aspects of the data collection concerning each data source.
DP-05	Asset identification should be considered key to the successful operation of the SIEM.
DP-06	The maximum possible physical memory should be made available to the SIEM
DP-07	The additional 'non-typical' SIEM features should be promoted to the project stakeholders.
DP-08	The operational benefits of the SIEM should be promoted to the IT function ahead of security benefits to encourage IT function buy-in.
DP-09	The operational benefits of the artefact should be regularly fed back to project participants as they emerge.

Table 5.2 - Nine proposed Design Principles

Although Design Principles DP-02 (Underlying infrastructure), DP-05 (Asset Identification) and DP-06 (Make maximum system memory available) are not directly informed by any related theory, earlier

SIEM research by Montesino et al. (2012) speaks of the requirement for network asset identification by business role to allow SIEM rule execution and Romano et al. (2012) note the importance of resource consumption by SIEM designs, particularly on shared hardware resources.

Design Principle DP-01 and SME Adoption of IT
Stakeholder participation and the need to recognize all actors (Eze et al., 2012) are key factors in the successful SME adoption of IT technology (Caldeira, 2003), echoing the requirement in DP-01 for full stakeholder involvement in initial problem definition and selection of key SIEM data sources.

Design Principle DP-03 and Information Overload/Theories of Bounded Rationality/Performance Dashboard Design
Over exposure to information affects productivity (Strother and Ulijin, 2012; Hemp, 2004) as well as decision making and innovation (Hemp, 2004). When machines generate information faster than humans can process it, distraction, stress and increased error rates occur (Edmunds & Morris, 2000). Short information processing times can lead to confusion, demotivation and a decreased satisfaction with a product (Eppler and Mengis, 2004).

Indeed, Simon’s Theories of Bounded Rationality (Simon, 1972) are founded on the limited information processing capacities of humans when faced with large, complex problem spaces. To make a satisfactory decision, the decision-maker needs a radical simplification of the real-world situation.

Design Principle DP-03 sets out a requirement to keep the scope of the prototype build restricted to a small number of SIEM data sources to keep the problem space small, thereby reducing the likelihood of information overload and negativity towards the SIEM prototype from the research project team members.

The dashboard is a key element of the SIEM system, displaying information for decision-makers to take action based upon the content of that dashboard – for example, security events might indicate a security breach and the IT or Security Team will need to take action to isolate and lock down systems, block attackers and commence forensics. Earlier research by Lempinen (2012) into performance dashboards and decision making highlights the challenges of information overload, limitations of human cognition and resulting decision inaccuracy when presenting information to decision makers. Therefore the SIEM dashboard, as with the Performance Dashboard in Lempinen’s study should only deliver the right amount of information via the most effective visual interface. Limiting the number of SIEM data sources – in the same way Lempinen limits the number of Key Performance Indicators (KPIs) – feeding into these dashboards helps prevent information overload and the resultant decision-related challenges.

Design Principle DP-04 and Performance Dashboard Design
Lempinen’s research into Performance Dashboards (Lempinen, 2012) proposes as part of a Design Principle that a ‘record sheet to identify data sources for each performance measure’ as a tool to ‘analyse systematically how each measure should be put into operation’. Given each SIEM system provides a dashboard, fed by security events from data sources, to display real-time and historical security event information to IT and Security personnel, this formal recording of data source identification and how each source should be put into operation applies equally in the SIEM context as of that of performance dashboard.

Design Principles DP-07, DP-08 and DP-09 and Conflict Positive Organisational Change
With a small IT Operations team, focused primarily on operational, not security requirements and resource limited by requirements to fire fight technical issues, encouraging full engagement in and

support for an innovative new SIEM, regardless of the acknowledged need for better security event management, was a challenge for the research project.

As noted earlier research into SME technology adoption shows full stakeholder engagement (Eze et al., 2012) is necessary for positive outcomes and this is echoed by research into organizational change management. Widened circles of involvement enhance innovation, adaption and learning and can create a critical mass for change (Axelrod, 2001).

Given the IT Operational resource challenges and with a widened circle of involvement, potential debate over the usefulness of the artefact, conflict is bound to arise. Research into organizational behaviour suggests that conflict, when managed well, can be good to help participants understand issues, strengthen relationships and make quality solutions (Tjosvold, 2008).

Design principles DP-07, DP-08 and DP-09 are related to promoting the value of the extra features a SIEM can offer, particularly those with operational benefits (not just security benefits) and regularly providing feedback on these operational benefits as they emerge and are demonstrated through the design and build process of the SIEM.

Stakeholders who feel the SIEM project is obstructing the activities of the IT Operations team are likely to be emotionally engaged and therefore available intellectually to discuss the ‘change proposal’ of the SIEM implementation. By engaging them in the change process, being available to discuss and debate the project in regular meetings (or other communications channel) and frequently demonstrating the benefits of the artefact to their activities the hope is the stakeholders recognize the benefits of the SIEM and may even become early adopters and even ‘champions’ of the beneficial features of the SIEM.

5.2 The Use of ADR in an SME Context

Did ADR result in a better outcome?
Current examples of ADR research are mainly from larger organizations such as Volvo (Sein et al., 2011) and Hansel (Lempinen and Tuunainen, 2011) with a much wider project team and longer timeframe. The use of ADR to design and implement a SIEM in the SME over a far shorter timeframe would be a test of the research method in this different context.

The SME project participants, who responded, when asked, were unanimous in their view that the additional discipline, rigor and documentation resulted in a better outcome for the build of the prototype SIEM.

According to Murphy and Ledwith (2007), SME projects of this size are typically run without a project manager, this suffer from poor project planning, unclear priorities and objectives. By adopting a more formal approach through the rigor of ADR - with the setting of roles/responsibilities, holding of meetings, taking of actions, setting of well-defined goals and milestones - combined with the time taken to iteratively identify the problems, set clear evaluation criteria, document decisions and actions, the project delivered a quicker working SIEM prototype.

As noted earlier in the paper, full stakeholder participation is essential for technology adoption success in SMEs (Eze et al., 2012) and positive outcomes for organizational change management (Axelrod, 2001). The inclusive nature of the problem formulation and evaluation stages of ADR provided this wider stakeholder participation; and even though the ‘researcher’ and ‘practitioner’ elements of the IT Operations Team were engaged in every cycle of BIE, project progress reports and attendance at project update meetings was available to the entire set of SIEM stakeholders.

The reflection and learning stage of ADR permitted those with different learning styles to contribute (some project members needing additional time to reflect); and the project progress update meetings and use of different communications channels allowed conflicts to surface, be debated and resolved as well help participants understand issues. All participants (heavily involved or not) also felt they knew far more about SIEMs and their use by being involved with problem formulation, data source identification, target system prioritization and ultimate evaluation of the prototype SIEM.

Role of the Impartial Observer
This ultimately added no value in this instance as the insight offered by the impartial observer was very much related to concerns over the manpower required and resource overhead, which echoed and reinforced the comments of more heavily involved participants and was probably a direct function of his job as the IT Operations Manager.

It is possible the role was not fully explained to the participant, reducing the quality of anticipated feedback or that by being less engaged with the project work, detailed observation and reflection was not possible.

Mechanics of the ADR BIE in the SME research project
As covered in the BIE commentary under the Results section of this Thesis, the small number of project participants and fact the artefact would be designed, built and used solely by the IT Team made the distinction between practitioner and end-user difficult in the IT or Organizational-dominant BIE stage of ADR.

To address this challenge, the IT Team was divided into two groups – the practitioners were those who were heavily involved in the project, particularly the implementation phase, whilst all of the IT Team were considered End-Users and involved in problem identification, then parts of the intervention and evaluation phases of BIE.

This resulted in an ADR BIE Stage that was a hybrid between IT and Organization-dominant BIE as pictured in figure 5.1 below. The hybrid BIE should still be considered IT-Dominant, given that the SIEM prototype artefact was not already present in the organization, the IT Team made up the Practitioners and End-Users and the prototype of the artefact was evaluated by the entire IT Team (the ultimate End-Users).

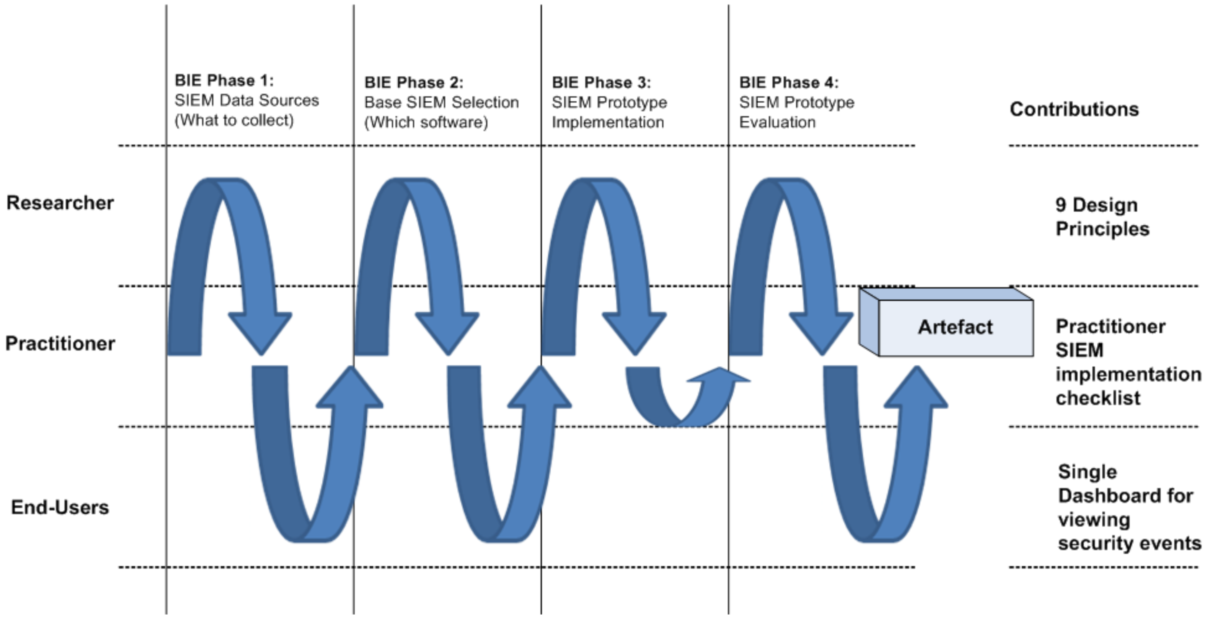

Figure 5.1 - SIEM Research Project - BIE Cycles

To Continue ADR at the Company
Project stakeholders agreed that the outcome of the design and implementation of the prototype SIEM was positive, though concerns were voiced around the people and time resources that will needed to continue the project from prototype to production SIEM.

The stakeholders agreed they now know so much more about SIEM technology and the capabilities of the OSSIM product that the earlier phases of the BIE stage could be re-run to reduce 'noise' from the SIEM by revisiting the analysis of the SIEM data sources and key target systems and re-evaluation of the features of the OSSIM software to enable or disable those based on the learning from the first BIE four-phase cycle. Some desirable features were never made fully operational in the SIEM prototype, such as email alerting on certain security log events and importing of log data from the Check Point IPS. Further BIE cycles must enable these features.

In addition to re-evaluating the SIEM data sources, aspects of the even earlier problem identification stage of ADR might be revisited. A deeper analysis of the exact security event problems to address could be carried out. For example, a lack of Windows Domain Controller event collection was identified as a generic problem, but the actual events that should be collected were not identified. Similarly an absence of file system event collection was identified as a problem; and this problem could be refined to a more granular level that included which files and what type of access or activity -read, write, ownership, or deletion – should be the focus of event collection. Such further analysis would result in a more targeted approach to the BIE phases of the next stages of the project.

5.3 IT & Open Source Software Adoption in an SME Context

IT Adoption in an SME Context
A significant body of research exists into the adoption of Information Technology in the SME context. Whilst the primary goal of this research project was not centred on the validation or extension of this research, certain aspects are worth discussion.

As noted earlier in this work the importance of the recognition and involvement of all actors is a key factor in the success of IT adoption (Eze et al., 2012). The successful design and implementation of the prototype SIEM in this research project involved all SIEM project stakeholders in the problem formulation and evaluation stages with stakeholder access and input into other stages of the research. Senior management, in the form of the IT Security Manager ('researcher') the IT Operations Manager (stakeholder and 'independent observer') and the IT Director (as project sponsor) were involved as project stakeholders and all three were visibly supportive of the SIEM research project. This management support is essential for successful adoption of IT in the SME context (Caldeira and Ward, 2003).

The promotion of perceived operational benefits emerged through reflection to become Design Principles. The perceived benefits of IT innovation are a significant factor in the success of SME systems adoption (Ramdani and Kawalek, 2007) as are improvements in operational efficiency (Fink, 1998).

Open Source Software (OSS) Adoption in an SME Context

One of the choices for the project stakeholders was which base SIEM software to use to build the prototype SIEM. Ultimately the Open Source OSSIM SIEM was selected and whilst the focus of this research work was not to analyse why OSS was selected some discussion is merited as previous research exists into OSS adoption in the SME context.

Perhaps the primary factor in selecting OSS as the base SIEM was cost. The project was allocated hardware and people resource, but no financial resource. This was a key consideration in choosing the OSSIM software, though it should be noted that commercial products were available with 30+ days evaluation versions and a successful SIEM prototype implementation would lend weight to the application for budget to take the evaluated prototype into production.

With reference to the OSS adoption framework in SMEs of Macredie and Mijinyawa (2011) the perceived cost benefits of OSS is one of the initial perceptions of SMEs looking to adopt OSS. Whilst cost might be seen as a favourable benefit, this SIEM research project saw the second perceived construct of the OSS adoption framework – that of complexity - as a definite blocker to adoption. The project team was clear in the survey feedback and reflections (specifically R-15) that the lack of comprehensive documentation, lack of dedicated helpdesk support, changes to the location of online discussion forums and changes in features as new versions of the software were released throughout the project contributed to dissatisfaction with the choice of Open Source SIEM software.

The perception was that the additional time taken to troubleshoot implementation snags without the help of a dedicated helpdesk or access to accurate system documentation outweighed any cost savings and feedback was that the commercial version (with documentation and formal support channels) would be preferable for the next stages of the project work.

6. SUMMARY & CONCLUSIONS

The research project's implications for both academic theory and practitioner are summarised in this section. The chapter ends with a brief discussion of the limitations of the research and suggestions for future SIEM and SME related research.

This research project successfully identified the security event management problems perceived in the SME context; prioritised these problems and solved them through the design and implementation of a prototype SIEM.

The research project makes contributions in three areas – contributions to design theory in terms of Design Principles, contributions to practitioners in terms of a successful SIEM prototype build and a checklist for future SIEM design and implementation and finally contributions to research methodology and the successful application of ADR in the SME context.

6.1 Theoretical Implications

State of the Art Summary

Although the primary purpose of this research was not a literature survey or review, no recent analysis and summary of current SIEM research is readily available. The literature review available in this Thesis and identification of research themes contributes towards a summary of the state of the art in SIEM research.

Existing DPs

Potential SIEM-related Design Principles were extracted from two of the twenty previous research papers reviewed. Of these nine DPs, seven were not tested as the scope of this SIEM research project precluded it; however two of these earlier Design Principles were successfully validated.

New DPs

Nine new Design Principles emerged from this research, related to problem identification and SIEM data source selection, SIEM implementation and the process of running a SIEM project in the SME context. These DPs were linked to or validated through earlier research work or existing academic theory.

6.2 Implications for the Practitioner

Working SIEM Prototype

The research project delivered a working SIEM prototype, knowledge of SIEM technology was increased across all project participants. Based upon the learning s from the research so far, the organization is well placed to move through a second round of BIE to take the SIEM prototype closer to full production status.

SIEM Planning & Implementation Checklist for SIEM Implementation in a wider context

A planning checklist for future SIEM design and implementation was created as a result of the research work. Through the incorporation of existing practitioner 'best practice' and findings from this research project this checklist should be applicable for SIEM design and implementation across all contexts, not just the SME context.

6.3 ADR in SME Context

Project participants agreed the use of ADR to operate the SIEM project resulted in a better outcome for the prototype SIEM design and implementation. SME projects often suffer from poor project management (Murphy and Ledwith, 2007) so the additional discipline, rigor and documentation demanded by ADR contributed to the successful outcome.

According to previous research, aspects of ADR operation naturally benefit IT adoption in SMEs and successful organisational change management. Full stakeholder participation during the problem formulation and BIE stages of ADR contribute to IT adoption success (Eze et al., 2012) and organizational change management (Axelrod, 2001).

Additionally the time allocated to dedicated reflection within the reflection and learning stage benefits the different learning styles of the project participants and project progress meetings allied with the use of multiple communication channels permitted conflicts over resourcing constraints and differences of opinion over prioritization of perceived problems, data sources and target systems to be surfaced.

The actual mechanics of running ADR in a SME context were shaped by the size of the IT Operations Team. Given the entire team will be 'End Users' of the project, the team was broken into highly-involved 'practitioners' and less-involved 'End Users'. This resulted in a hybrid BIE for the ADR project (see Figure 5.1) however this hybrid should still be considered IT-dominant (due to the fact no SIEM technology was already in place within the case organization).

6.4 Limitations of the Study & Future Research

6.4.1 Limitations of the Study

The study is initially limited by the breadth of research data on SIEM research out there. Only papers written in English were used as data sources and it is not possible to accurately find and review all possible research that might have taken place in the field. This limitation also applies to the analysis of the findings and attempts to find theory to frame the practical findings of the research.

It could be argued that the very nature of running research in the SME context is a limitation. The number of project participants is small and the actions and opinions of just a couple of project members may inappropriately influence the results.

Similarly the case study organization may have only 85 staff, but as an Internet-based technology SME it has a large number of computer systems within its infrastructure and IT staff with advanced technical capabilities. Compare this to a manufacturing SME with less Internet-facing infrastructure and a focus on perhaps plant machinery or compare the case organization with a legal firm with just ten staff. The definition of SME based on company turnover and number of staff and therefore covers a broad spectrum of organisations.

6.4.2 Future Research

The most obvious future research opportunity would be to continue this ADR research project through another cycle of BIE (and possibly perceived problem re-formulation or re-prioritisation) to move closer to a production SIEM for the SME in the case study.

Alternative research opportunities could include the validation of the nine Design Principles emerging from this research through SIEM design and implementation in the SME or other context. Similarly a validation of DPs extracted from previous SIEM research that were not tested through this SIEM design and implementation might be tested through a future SIEM project where the DPs do apply e.g. a SIEM that includes security events from physical security systems.

Given the conflicting feedback from project participants on the SIEM dashboard – some said it lacked intuitiveness, clarity and was hard to find information, whilst others said it was easy to read, layered well and clutter free – a possible avenue of research might be that into the SIEM dashboard's perceived effectiveness at presenting the right levels of data to the audience.

7. REFERENCES

Axelrod, R. H. (2001). Terms of engagement: Changing the way we change organizations. *The Journal for Quality and Participation*, 24, 22-27.

Brandel, M. (2009). *SIEM Security Info and Event Management Dos and Don'ts*. Retrieved June 8, 2013, from http://www.csoonline.com/article/509553/siem-security-info-and-event-management-dos-and-don-ts.

Caldeira, M., & Ward. J. (2003). Using resource-based theory to interpret the successful adoption and use of information systems and technology in manufacturing small and medium-sized enterprises. *European Journal of Information Systems*, 12, 127-141.

Conradi, M. (2007). Legal developments in IT security. *Computer Law & Security Review,* 23(4), 365-369.

Coppolino, L., D'Antonio, S., Formicola, V., & Romano, L. (2011). Integration of a System for Critical Infrastructure Protection with the OSSIM SIEM Platform: A dam case study. *Lecture Notes in Computer Science*, 6894, 199-212.

Coppolino, L., Jager, M., Kuntze, N., & Reike, R. (2012). A Trusted Information Agent for Security Information and Event Management. *The Seventh International Conference on Systems ICONS 2012*. Saint Gilles, Reunion Island. February 29 – March 6, 2012.

Cowan, D. (2011). External pressure for internal information security controls. *Computer Fraud & Security*, 2011(11), 8-11.

Daneshgar, F., Low, G. C., & Worasinchai, L. (2013). An investigation of 'build vs. buy' decision for software acquisition by small to medium enterprises. *Information and Software Technology*, 55(10), 1741-1750.

Edmunds, A., & Morris, A. (2000). The problem of information overload in business organisations: a review of the literature. *International Journal of Information Management*, 20, 17-28.

Eppler, M.J., & Mengis, J. (2004). The Concept of Information Overload: A Review of Literature from Organization Science, Accounting, Marketing, MIS and Related Disciplines. *The Information Society*, 20, 325-244.

Eze, S., Duan, Y., & Chen, H. (2012). Factors Affecting Emerging ICT Adoption in SMEs: An Actor Network Theory Analysis. *Communications in Computer and Information Science 2012,* 361-377.

Feldman, M. S., & Pentland, B. T. (2003). Reconceptualizing Organizational Routines as a Source of Flexibility and Change. *Administrative Science Quarterly,* 48(1), 94-118.

Fink, D. (1998). Guidelines for the Successful Adoption of Information Technology in Small and Medium Businesses. *International Journal of Information Management*, 18(4), 243-253.

Gabriel, R., Hoppe, T., Pastwa, A., & Sowa, S. (2009). Analyzing Malware Log Data to Support Security Information and Event Management: Some Research Results. *First International Conference on Advances in Databases, Knowledge, and Data Applications*. Cancun, Mexico. March 1-6, 2009.

Gartner Inc. (2012). *Gartner Magic Quadrant for Security Information & Event Management (2012)*. Retrieved June 8, 2013, from http://insight.q1labs.com/GartnerSIEMMQ2012.html.

Ghobakhloo, M., Sabouri, M., Hong, T., & Zulkifli, N. (2011). Information Technology Adoption in Small and Medium-sized Enterprises: An appraisal of Two Decades Literature. *Interdisciplinary Journal of Research in Business*, 1, 53-80.

Gordon, S. (2010). *Operationalising Information Security – Putting the Top 10 SIEM Best Practices to work*. Retrieved June 8, 2013, from http://whitepapers.theregister.co.uk/paper/view/2584/opinfosec-siemtop10bestpractices-122210.pdf.

Hadziosmanovic, D., Bolzoni, D., & Hartel, P.H. (2012). A log-mining approach for process monitoring in SCADA*. International Journal of Infrastructure Security,* 11, 231-251.

Hemp, P. (2009). Death by Information Overload. *Harvard Business Review*, 87(9), 82-89.

Iivari, J. (2013). *Two Strategies for Design Science Research*. Retrieved July 22, 2013, from http://www.researchgate.net/publication/243459048_TWO_STRATEGIES_FOR_DESIGN_SCIENCE_RESEARCH.

Karlzen, H. (2009). *An Analysis of Security Information and Event Management Systems: The Use of SIEMs for Log Collection, Management and Analysis* (Master's Thesis). Chalmers University of Technology, University of Gothenburg, Gothenburg, Sweden.

Kufel, L. (2013). Security Events Monitoring in Distributed Systems Environment. *Security and Privacy,* 11(1), 36-43.

Lempinen, H. (2012). Constructing a Design Framework for Performance Dashboards. *Scandinavian Conference on Information Systems, Lecture Notes in Business Information Processing,* 124, 109-130.

Lempinen, H., & Tuunainen, V. K. (2011). Redesigning the supplier reporting process and system in public procurement – case Hansel. *International Journal of Organisational Design and Engineering*, 1, 331-346.

Macredie, R., & Mijinyawa, K. (2011). A theory-grounded framework of Open Source Software adoption in SMEs. *European Journal of Information Systems,* 20, 237-250.

Metzger, S., Hommel, W., & Reiser, H. (2011). Integrated Security Incident Management – Concepts and Real World Experiences. *Sixth International Conference on IT Security Incident Management and IT Forensics (IMF)*. Stuttgart, Germany. May 10-12, 2011.

Miller, D. R., Harris, S., Harper, A. A., VanDyke, S., & Blask, C. (2011). *Security Information and Event Management (SIEM) Implementation*. New York: McGraw-Hill.

Montesino, R., Fenz, S., & Baluja, W. (2012). SIEM-based framework for security controls automation. *Information Management & Computer Security*, 20(4)4, 248 – 263.

Murphy, A., Ledwith, A., (2007). Project Management tools and techniques in high-technology SMEs. *Management Research News,* 30(2), 153-166.

Okoli, C., & Schabram K. (2010). A Guide to Conducting a Systematic Literature Review of Information Systems Research. *Working Papers on Information Systems*, 10(26), 1-49.

Payment Card Industry (PCI). (2010). *Payment Application Data Security Standard: Requirements and Security Assessment Procedures, Version 2.0*. Retrieved June 8, 2013, from https://www.pcisecuritystandards.org/documents/pa-dss_v2.pdf.

PriceWaterHouseCoopers (PWC). (2013). *Information Security Breaches Survey 2013.* Retrieved June 8, 2013, from http://www.pwc.co.uk/assets/pdf/cyber-security-2013-technical-report.pdf.

Ramdani, B., & Kawalek, P. (2007). SME Adoption of Enterprise Systems in the Northwest of England. *International Federation for Information Processing*, 235, 409-430.

Romano, L., D'Antonio, S., Formicola, V., & Coppolino, L. (2012). Protecting the WSN Zones of a Critical Infrastructure via Enhanced SIEM Technology. *Lecture Notes in Computer Science*, 7613, 222-234.

Salleh, S. M., Teoh, S. Y., & Chan, C. (2012). Cloud Enterprise Systems: A Review of Literature and Its Adoption, in Pan, S. L., & Cao, T. H. (Eds.) *Proceedings of the 16th Pacific Asia Conference on Information Systems (PACIS 2012).* Ho Chi Minh City, Vietnam. July 13-15, 2012

Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., & Lindgren, R. (2011). Action Design Research*. MIS Quarterly,* 35(1), 37-56.

Simon, H. A. (1972). Theories of Bounded Rationality, in McGuire, C., & Radner, R. (Eds.) *Decision and Organization* (pp. 160-176*).* Amsterdam: North Holland Publishing Company.

Sohn, G., & Na, J. (2012). System Architecture for Physical/IT Security Event Integration. *International Journal of Computer Science and Network Security*, 12(1), 66-70.

Strother, J. B., & Ulijin, J. M. (2012). The Challenge of Information Overload*. 2012 IEEE International Professional Communication Conference (IPCC).* Orlando, Florida. October 8-10, 2012.

Tjosvold, D. (2008). The conflict-positive organization: it depends on us*. Journal of Organizational Behavior,* 29, 19-28.

Verizon Communications Inc. (2013). *Verizon 2013 Data Breach Investigations Report*. Retrieved June 8, 2013, from http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf.

Welsh, J.A., & White, J.F. (1981). A small business is not a little big business. *Harvard Business Review,* 59 (4), 18-32.

8. APPENDIX

The table in this appendix shows the Design Principles (DPs) from the two previous pieces of SIEM research that this research sought to validate. The context of the research work is shown, along with the author, the DP as stated in the paper and whether it was possible to validate the DP through this research project.

Design Challenge / Context	Source	Design Principle (DP)	DP Validated through this research
Dealing with attacks on critical infrastructures and risks to wireless sensor network technologies / Critical Infrastructure	Romano et al. (2012)	DP1: Data collectors should be able to integrate legacy and novel information sources in an effective and flexible way, by interpreting multi-layer and multi-domain data formats, typically characterized by heterogeneous syntax and semantics.	Yes – The SIEM provides the ability to custom write data source plug-ins to read data from any kind of data log.
		DP2: SIEMs should limit the consumption of shared resources as much as possible (e.g. bandwidth, central server processing).	No – the SIEM was installed as software on a dedicated hardware device so no storage or central processing resources were shared. The volume of network traffic generated during the project was not sufficient to impact shared network bandwidth.
		DP3: SIEM should provide mechanisms to treat and pre-correlate data at the edge of the (SIEM) architecture, very close to the field devices.	Yes – the SIEM can use OSSEC agents which can pre-correlate Windows event, file integrity and registry change events locally before passing important events to the central sensor.
		DP4: SIEMs should be capable of high data volume performance at the edge of the network, specifically in data treatment components, such as data collectors, data parsers and event correlators.	No – in the SME context the network infrastructure and volume of data generated was not enough to test this DP.
		DP5: SIEM storage systems should provide high capabilities in terms of: data authenticity of event sources; fault and intrusion tolerance; control of data access by authorized parties. Forensic events, and only such events, must be kept, while unnecessary details must be deleted or made anonymous ("least persistence principle").	No – the SIEM was designed using Open Source software that does not support fault tolerance or data authenticity of event sources.

		DP6: SIEM should be able to disseminate events in a reliable manner by means of resilient architectures	No – the SIEM was designed using Open Source software that does not support fault tolerance or resilient architectures.
SIEM sensors are exposed to attack, so agents must be trusted / Critical Infrastructure	Coppolino et al. (2012)	DP 1: When physical access to the sensoring devices cannot be inhibited, an effective security solution must address detection of manipulations.	No – Physical access to the sensor devices was inhibited in the research project. The sensor devices were in a locked server room.
		DP2: Whenever a certain control decision is made, the input information that presumably led to it must be authentic.	No – Authenticity of input information was not in the scope of this research project.
		DP3: A risk assessment of the deployed monitoring capabilities is necessary.	No – Whilst data source choice was influenced by the location of key information assets, which was a result of earlier risk assessments, the limited deployment of monitoring capabilities did not require such a detailed risk assessment.

Table 8.1 - Design Principles from earlier SIEM research