SECURITY OPERATIONS CENTRE (SOC) IN A UTILITY ORGANIZATION

GIAC GSLC Gold Certification

Author: Babu Veerappa Srinivas, babuseenu@gmail.com
Advisor: Kees Leune

Accepted: September 17th 2014

Abstract

Cybersecurity breaches at various organizations are becoming common news published almost daily. Another trend we can see from ICS-CERT alerts is that security breaches in utilities are also increasing. Irrespective of the size or type of the utility organization, it is important to ensure that there is an appropriate team with right skills and tools to identify, detect and defend against such breaches. Building a dedicated security team that provides SOC (Security Operations Centre) functionality for most small to medium sized utility organizations is an expensive proposition. This paper discusses how an existing IT support team can provide SOC functionality to either provide new or enhanced security operations capability for monitoring, detection and remediation of cybersecurity incidents. Topics such as prioritizing *Events of Interest/ use cases* to monitor and respond for both Operations Technology (OT) and Information Technology (IT) domains are discussed. Although the target audience of this paper is information security managers at electricity distribution and transmission business, any utilities can adopt ideas from this paper to improve security incident response capability.

Throughout this paper the terms SCADA (Supervisory Control and Data Acquisition), ICS (Industrial Control Systems) and Control Systems may be used interchangeably as they have the same meaning.

1. Introduction

Cyber security threats are an increasing manifold, irrespective of the size of an organization. This is evident after reviewing many industry reports such as Verizon 2014 Data Breach Investigation Report (Verizon, 2014), Trustwave 2014 Global Security Report ((Trustwave, 2014) and Symantec Internet Security Threat Report 2014 (Symantec, 2014). To defend against such threats every organization must have good security incident detection and response capability. Many small to medium utilities in Australia lack a fully functional Security Operations Centre (SOC), which is the heart of a good Security Incident Management process. Some of the reasons for this lax could be attributed to shortage of trained security professionals, cost constraints, appropriate security tools and/or prudent incident management process. Compounding this is the issue of complacency. Many organizations believe that they are not susceptible to cyber-attacks because they haven't experienced any in their organization. The reality is that they don't know whether they are already compromised or not. We need to understand that the average number of days from the initial breach to detection is between 210 days and 254 days (Trustwave, 2014).

1.1. Survey Summary

The author, to understand utilities' current security incident response capability, carried out an informal survey of Australian electricity and gas utilities. The survey questions were framed to get information about the existing security operations capabilities, team composition & structure, types of functions performed by the team, incident response process, tools and technologies used and current staff's skills.

A short summary of the survey results in included in the Appendix A. Key takeaways from this survey include:

- Missing security operations team: It is common that there is no dedicated security operations team providing a security incident management and response function. At a few organizations the IT support function is outsourced but without any specific security monitoring and reporting requirements and associated SLA's.

- Small enterprise security team: A typical security team at most of these organizations is comprised of two or three dedicated staff members whose focus is on maintaining security policy, drafting tactical plans for the year, responding to audit plans and providing broader security advisory services. In some instances, contractors provide security architecture capability within IT projects but without the oversight of the security manager.
- Inadequate security monitoring and detective tools: Most organizations have basic protective controls such as firewalls, proxies, gateway antimalware tools and authentication controls. Some of the controls that are either nonexistent or minimally deployed are Security Information & Event Management (SIEM), Intrusion Prevention System (IPS), vulnerability scanners, database security controls, file integrity checking and web application firewalls. The implemented security tools were not acquired based on a well-articulated security strategy. They were introduced as part of tactical plans to address a point specific problem. Hence they don't integrate well with other tools to provide meaningful information that can be used for security incident and response management activities.
- Missing security incident management process: The existing Incident Management (IM) process do not factor security incidents at most organizations. With some, the IM process exists but lacks security monitoring tools to perform security monitoring and response functions. This resulted in the absence of a periodic security reporting regime. Hence security topics were not reported to the senior management
- Security training for support staff needs enhancement: Some of the support staff were trained and certified in firewall and IPS/IDS technologies but not the *core body of security knowledge* established by International Information Systems Security Certification Consortium (ISC2) or the SANS Institute training courses. Training and certifications, such as Global Information Assurance Certification – Certified Incident Handler (GCIH) that enhances security incident response capability, were not factored in the future training plan.

A sneak peek into some of the utilities in the form of this survey helped us to understand the current security response capability. The task ahead of most of the utilities is to build a basic SOC capability utilizing existing resources. The following sections of this paper articulate the steps an organization can take to build a SOC using existing resources and minimal investment.

Foundation of a good IM process is an operational SOC with the right tools and skilled resources. Section two and the subsections articulate and explains the key elements of a good SOC.

In the context of cyberattacks, risk assessment and gap assessments helps an organization to understand its current capabilities and gaps. This information can be used to prioritize implementation of risk mitigation controls. Section 2.1 briefly explains this process.

Business case must be aligned with the corporate strategy and objectives. Other elements of business case are discussed in section 2.2.

To manage a SOC efficiently and effectively, requirement of skilled resources is of utmost importance. Section 2.3 helps the reader in understanding the basic skills required and how to upskill the chosen SOC staff.

Human skills must be complimented with the right tools for effective IM process. Section 2.4 emphasizes the importance of having the right tools to operate a SOC. One of the important tools to run a SOC is SIEM; a brief introduction of SIEM capabilities is also highlighted in this section.

With the right tools and staff in place, section 2.5 introduces IM process. How to integrate security into the existing IM process or where to look for if a new IM has to be drafted are discussed in this section.

Threats, risks and risk tolerances are different to different organizations. Knowing what security events need to be monitored, remediated and reported is important. Section 2.6 introduces use cases that are important to utilities in monitoring and responding to security events.

Since staff from IT and OT team will operate the integrated SOC, it is important to understand few differences between IT & OT operations. Section 2.7 highlights some of those differences.

Building an internal SOC might not be a choice of every utility. Some may consider outsourcing this function to a Managed Security Services Provider (MSSP). Section 2.8 highlights some of the MSSPs offering service in Australia and discusses the positives and negatives of outsourcing SOC function to a MSSP.

Section 3 lists the key milestones of a SOC project, as a checklist, in chronological order. A SOC project manager might find this checklist useful to use in their project.

The conclusion section wraps up the paper highlighting the importance of a SOC to any organization. Few topics for further research in this domain are also highlighted.

2. Elements of SOC building process

The pertinent question to ask is: how do we improve security incident management capability without investing a lot of capital? The answer lies in understanding the current capabilities of people, process and technology. This can be achieved by performing risk or gap assessments against industry best practices such as *Responding to targeted cyberattacks* published by ISACA[1] (ISACA, 2013) or Information Security Forum's *Standard of Good Practice for Information Security*. Another important step to perform at this stage is to complete a baseline assessment of the existing security technologies and processes. The output of this assessment can be used in the risk assessment activities.

2.1. Risk assessment

Utilities planning to improve security IM process, by utilizing an integrated SOC, must first perform risk assessments to identify clear priorities. Recommended initial steps to consider are; compile a critical asset register by identifying critical business processes, the associated dependent technologies and the information assets to protect. Next, identify vulnerabilities, likelihood and threats for the critical business process. To ensure consistency in identifying all relevant information security issues, the IT Security Manager with the involvement of critical business process owners must facilitate these

[1] ISACA was previously known as Information Systems Audit and Control Association and is now goes by its acronym only.

risk assessment workshops. Once the risks are identified, based on probability and impact, each risk must be ranked. For ease of understanding, these prioritized risks can be plotted on a heat map (Lacey, 2013), as shown in ***figure 1***.

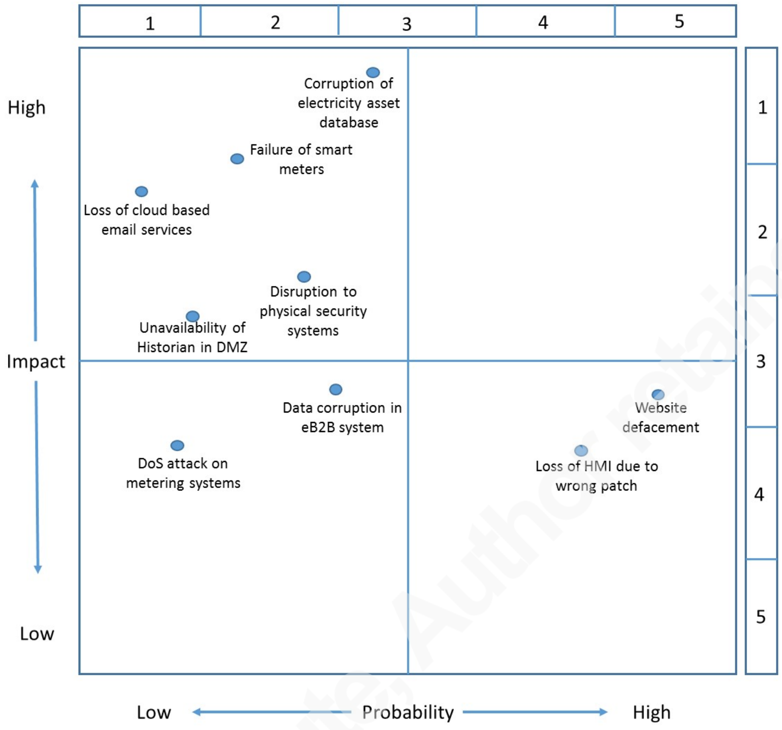

Figure 1

In addition to the outputs of risk assessments, a *red team* exercise or a penetration test will help identify technical issues in the network. The outcomes of such tests are limited by the time allocated for the test and the skills of the tester. To ensure that all key exploitable vulnerabilities are identified, it would be preferable to have penetration tests performed by two different providers for the same defined scope. The results of such a comprehensive test will provide actionable information for remediation that can be used in the development of Security Information and Event Management (SIEM) use cases.

The combination of risk assessment and penetration test results provides a clearer picture of current security posture. Equipped with this information and the list of assets to protect, SIEM business case and appropriate SIEM use cases can be developed.

2.2. Business case

Once the risk assessment is complete, SOC objectives must be defined. Some of the SOC objectives could be to detect attacks from the Internet, maintain a consolidated vulnerability review, monitor compliance with North American Electricity Reliability Corporation (NERC) requirements or any other objectives that are relevant for an organization. Post this, a business case should be developed addressing what business problem the SOC will solve and the mission statement, and specific requirements must be documented. Business cases help articulate benefits, goals and investment required. This would help to align expectations amongst stakeholders to provide a basis for measuring success. Requirements should factor both short and longer term objectives for example, align to ICT and business strategy, existing business problems, current IT infrastructure projects planned, mission statements, skills requirement of staff members, existing processes that need improving or new processes that complement the existing processes and the required SOC operating hours. In defining these requirements, important tip to consider is, start with the basics and keep *it simple*. Since most of the utilities are building this capability for the first time, starting small and simple will be one of the key factors in SOC's initial success.

It is recommended to include a section on staff skill requirements in business case. This section could include details such as; what is the staff skills required to run a SOC and, what are the current skills, and what training is required.

2.3. Staff skills and training requirement

Skilled people, appropriate processes and the right technology are the key requirements of a good security incident response (IR) process. Amongst these requirements, skilled staff plays a key role in defending the organization against cyberattacks (Homeland Security, 2013). Without appropriately skilled staff, any number of processes or technologies will not help in improving the security IR process. To run round the clock SOC function, a minimum of seven staff members are required, which is a distant possibility for many utilities (McAfee, I. 2013). Hence augmenting SOC function with the existing limited staff is a more practical and cost effective approach.

Identifying current skills versus required skills and planning for upskilling staff over a period of time will help organizations to build a skilled security IR team.

A SOC without SIEM is meaningless and a SIEM without skilled resources is a wasted investment. As highlighted earlier, not all utilities can afford a significant number of dedicated SIEM staff. To supplement this, during the initial days of SOC operations, utilities must identify staff from service-desk, network services, operating system support and SCADA support teams to perform some of the SIEM tasks. Time spent on manual log parsing by these staff can now be spent more efficiently on the SIEM console. In parallel, these staff must undergo incident management training, such as SANS GCIH or any other training with similar content. In the interim, to guide these resources in the right direction, help of an external expert organization should be formalized.

Security Incident Management (IM) activities must be led by an experienced team leader. Typically, this role is absent at many small to medium sized utilities. To build an integrated SOC function, utilities must consider introducing this role. As a minimum, utilities must invest in recruiting at least one dedicated experienced security operations resource who can understand SOC functions, advice/mentor team members and prepare improvement plans for the future. This staff member should have GIAC-GCIH and GIAC Certified Intrusion Analyst (GIAC-GCIA) certification and minimum of 5 years experience as a SOC analyst / team leader. Consideration should be given to reporting lines for the SOC team so that any issues can be escalated appropriately within the organization.

Identifying gaps between the current and required skillset of the existing support staff should be the next step in formalizing a virtual SOC team. Formalize a training road map for each SOC team member based on the gap assessment results and then secure funds to execute training. An example training roadmap is illustrated in ***Table 1***:

Team Member	Current Skills	Required Skills
Network Support Team member 1	Firewall administration Firewall Log analysis VPN (Virtual Private Network) & Access control Routing & Switching concepts TCP/IP concepts	Incident triage – Yr1 TCP/IP packet analysis (GCIA) – Yr2 Basic ethical hacking skills – Yr2 CISSP contents – Yr1 SIEM training – Yr1
Network Support Team	IDS administration	Incident Handling (GCIH) – Yr2

member 2	Configure and fine tune IDS TCP/IP packet analysis TCP/IP concepts	OS security concepts – Yr1 SIEM training – Yr1 Malware Analysis (GIAC Certified Reverse Engineering Malware – GREM) – Yr2
Operating System Team member 1	Win Server OS administration Anti-virus, Proxy & mail gateway	SIEM training – Yr1 GCIH training – Yr 2 CISSP contents – Yr1 Incident triage – Yr1
Operating System Team member 2	Linux Server OS administration Mail server administration	TCP/IP packet analysis – Yr1 CISSP contents – Yr1 Incident triage – Yr1 Network security concepts – Yr1
SCADA Support Team member 1	Skillset 1 Skillset 2 Skillset3	Skillset 1 Skillset 2 Skillset3
SCADA Support Team member 2	Skillset 1 Skillset 2	Skillset 1 Skillset 2

Table 1

Most utilities have a Network Operation Centre (NOC) to monitor the IT network. SOC and NOC exhibit many similarities in their functioning but only the context is different. The context specific skills can be built by additional training for the existing staff. Staff experienced in servers, desktop and network support will have good troubleshooting skills, which are important skills required for SOC functionality and managing and investigating SIEM alerts. Additionally, they will have TCP/IP protocol suite knowledge and basic malware infection and propagation methods. Basic security training and certification, such as Certified Information Systems Security Professional (CISSP) and GIAC Certified Security Essentials (GIAC-GSEC), must compliment these skills. It is important to hire staff members based on the core requirements, historical knowledge of the organization, analytical mindset, process focused, attention to detail and good attitude. This recommendation is in line with the statement "bet on a great team rather than on a champion" by Yves Breta (Breta, Y. 2013).

Product specific SIEM training should be the next in line for the chosen staff members. Armed with the basic security skills and SIEM product knowledge, a training roadmap involving both on-the-job and formal training could be developed for the next two to three years to upskill the staff members. One of the key attributes of a good SOC is to learn from past incidents and feed these learnings back into the system for effective and quick response of the similar events in the future. One process that helps to build this is OODA Loop (Observe, Orient, Decide, Act). OODA Loop workflow training should be considered for all SOC staff to understand good feedback process and its benefits. This feedback loop mechanism helps in continuous improvement and establishing a good security incident response knowledgebase based on SIEM alerts (Boyd, J. 2012).

The job descriptions for the chosen virtual SOC team members must be modified to include minimum 25% of their time for SOC monitoring and management activities. Eight IT support staff members being identified for the virtual SOC activities translates to three fulltime staff for SOC activities including the SOC team lead. Time spent on these activities should be logged by every staff member for future assessment of resource utilization and, if necessary, justification for addition of new staff members. Specific SIEM use case alerts must be assigned to the right support group. For example, password brute force alerts must be forwarded to the operating systems support team, anomalous port scan alerts must be forwarded to the network support team and unexplained behavior of a HMI (human machine interface) or a Programmable Logic Controller (PLC) should be forwarded to the SCADA support team.

After consultation with each other, small and medium sized utilities in a particular geographic region should consider forming an alliance. This alliance will help information sharing and provide additional support staff for an incident investigation or heightened response phase of IM process. Confidentiality protocols need to be established before formalizing such arrangements.

2.4. Technology requirements

Based on the support team's current skillset and planned future training requirements, security managers should identify the complimentary security technologies that are required to improve the IR process. Some of the tools can be basic tools like antivirus, firewall and intrusion detection system. Others can be advanced tools such as data leak prevention, application security testing, database activity monitoring or automated vulnerability assessment tools (Lacey, 2013).

Various security technologies are used in utilities to improve security posture. Some are basic controls, and some are advanced. Basic security technology controls were present in all the utilities surveyed. However, it was noted that the required logs were not enabled on most of the systems, applications and network devices. Even where the logs were enabled, they were not centralized and hence did not provide useful correlated information. As a minimum, utilities must have all the basic security controls and SIEM to build the integrated SOC functionality (Lacey, 2013). ***Table 2*** below is an example of security technology controls categorized as basic, advanced and APT specific technology controls (Lacey, 2013).

Basic Security Technology Controls	Endpoint Antivirus, Gateway Antivirus, Firewall, Intrusion Detection, Penetration tests in corporate network, Strong authentication controls, syslog servers.
Advanced Security Technology Controls	Automated vulnerability scanners, Database security monitoring controls, Intrusion Prevention Systems, data leak prevention systems, Data diodes between Supervisory Control and Data Acquisition (SCADA) and corporate network, SIEM.
Specific APT Technology Controls	Web application firewalls, file integrity checking tools, Threat data feed into SIEM, advanced forensics, honeypots, Application whitelisting.
Best available practices	Security in Software Development Life Cycle (SDLC), Enterprise security architecture, information exchange forums, trusted computing.

Table 2

As highlighted earlier, SIEM is an important and mandatory tool required for the SOC functions. Careful consideration must be given when choosing the appropriate vendor. There are many SIEM offerings from various vendors with different licensing and cost options. Suitability of a SIEM must be based on defined business requirements, identified use cases and ease of management. There are many open source SIEMs (egs., AlienVault), but organizations must exercise caution before going down this path. Open source SIEM tools require dedicated resources to constantly manage and maintain the tools, which could become costly for many small to medium sized utilities. Dr. Anton Chuvakin in his blog very clearly states “No open source SIEM ever” (Chuvakin, A. 2009), highlighting various other reasons not to build an open source SIEM.

Small utilities must avoid buying SIEM tools that involve writing a large number or regular expressions (regex), which is the key component of rule building activities in a SIEM. This activity will be very resource intensive and may not be sustainable for many utilities. Independent research reports from either Gartner or Forrester can be used for initial screening of various SIEM vendors. For brave hearts, who like challenges and would like to build their own SIEM and incident response toolkit based on open source tools, can refer to the The SANS Institute’s reading room article by Jonathan Sweeny (Sweeny, J. 2011).

Another important tool to consider in improving the integrated SOC capability is automated vulnerability scanning tools, such as Nessus, Wikto, Rapid 7 etc., for a small fee. It is recommended to run periodic scans on identified key systems. In addition to common vulnerabilities, these tools have the capability to check for missing patches and open ports on the target systems. The output of these scanners can be fed into SIEM for rich vulnerability information for monitoring, alerting, reporting and remedial activities.

ISACA’s *Responding to targeted cyberattacks* highlights some of the computer security incident response tools and team capabilities. Those capabilities are tabulated in ***Table 3*** (ISACA, 2013). Utilities should start with minimum recommended capabilities and plan to invest on preferred capabilities in a phased manner over a two to three year period.

Capability **(People, Process , Technology)**	**Minimum**	**Preferred**
Host level activity awareness	• Logs from end point software • Logs from operating systems	• Host based intrusion detection • Agent based, live memory analysis
Network level activity awareness	• Layer 3 network flow data • Proxy logs • Firewall logs	• Network intrusion detection logs • Full packet capture at critical egress points

		• SSL inspection
Search	• Local logging on each individual systems with manual retrieval and limited automation	• SIEM tool
Digital forensics	• Ad hoc, local analysis	• Remote enterprise acquisition • Case management systems
Malware analysis	• Dynamic malware analysis • Basic static and automated analysis	• In-depth static code analysis • Reverse engineering
Threat intelligence	• As hoc, open source research	• Subscription-based • Business partner information sharing • Repeatable, automated integration
Vulnerability identification	• Enterprise application inventory	• Enterprise vulnerability identification

Table 3

The key sources of information that trigger the identified use cases in a SIEM tool are system logs, device logs or application logs. Appropriate logs that support a particular use case must be enabled, logged and collated by the SIEM tool to monitor, alert and report an event. Based on the appropriateness and severity of these triggers, IM process will be initiated.

2.5. Incident management process

As highlighted in the survey response section, at most small to medium sized utilities, the security incident response (IR) process is not defined and established. In many instances, the security IR process is no different to the common IT IR process. Based on the existing and planned people and technology requirements, the security IR process can be intertwined with the IT IR process to form an integrated security operations center (SOC) capability. National Institute of Standards and Technology's (NIST) *Computer Security Incident Handling Guide* is a good reference document to build security IR process (Cichonski, P., et al. 2012).

Defining and configuring use cases is important in building a SIEM tool. Security incident management (IM) is built on the inputs from the triggers of SIEM use cases. Once the SIEM configuration is ready, to operationalize the incident management process, we need to define the use case response procedures (InfosecNirvana, 2012). These response procedures are also known as standard operating procedures that need to be followed once an alert is triggered.

There isn't much difference between IT incident management and security incident management process. Almost all incidents in an organization get initiated or reported as an IT incident. In many cases, with further analysis, an incident can be categorized as an IT or a security incident. The phases of an incident management process are, Identification → Response → Recovery → Post-Incident Review (ISACA, 2013). These phases are common for both IT and security incident management. What characterizes security incidents are the attributes of an incident such as password brute force attack, introduction of malware, defacing website, phishing attacks, etc. For security incidents, containment and eradication activities happen in the *Response* phase of the generic process.

Organizations that have established a mature IT incident response process can continue to use the existing process for security incident management with the addition of the following new processes or activities.

- Integration of SIEM outputs into the existing IM process
- Creation of roles and responsibilities matrix with the inclusion of security response activities
- New escalation process for security incidents
- Train servicedesk staff in basic security threats, vulnerabilities and response actions. Training contents, such as the SANS Institute's *SANS – Securing the human – Utility,* will be appropriate for the help desk staff. This training will equip servicedesk staff to identify security incidents based on the initial calls raised by the general staff.

- Factor budget to train SCADA support engineers and SOC engineers in ICS Security. Contents from *SANS Industrial Control Systems (ICS) Security Essentials* and *Security Infrastructure Solution* are appropriate to upskill IT support staff in ICS security and for SCADA engineers to understand security threats and vulnerabilities.

Utilities without a mature ICT incident response process can use either NIST's *Computer Incident Handling Guide* (Cichonski, P., et al. 2012) or Electric Power Research Institute's *Guidelines for planning an integrated security operations center* (Rasche, G. 2013) for building an appropriate IR process. The later document is very specific to electricity industry and has specific recommendations to comply with NERC (North American Electricity Reliability Corporation) compliance requirements, pros and cons of different SOC architecture and efficient ways to integrate IT and OT SOC environments.

To enhance SOC staff confidence in detecting and remediating security events, annual *red team – blue team* exercises are recommended. This will also provide an opportunity for the new SOC members to learn security incident management in a controlled and familiar environment. The outcome of such exercises can be used to improve the existing incident management process, refine the established training roadmap and enhance or improve a SIEM use case.

2.6. SIEM use cases

Monitoring multiple logs from various systems and devices requires a large team. To make most out of the existing support team and current tools, utilities should first understand the key cyber risks that they face. Based on these key risks, they should identify the top ten to fifteen use cases for security monitoring (McAfee, I. 2013). With a small number of appropriate use cases, a small team with limited resources will be able to focus on key events of interest for detection and remediation activities.

When the term *SIEM deployment and management effort* is searched in Google, search results reveal that many practitioners in their blog posts emphasize that SIEM is resource intensive and without dedicated staff, SIEM is of little use. Although this is true, SIEM will also reduce the time of a firewall administrator, who occasionally spends time in parsing the firewall logs – searching for a needle in a haystack. The same applies to IDS or operating system logs. With the appropriate SIEM use case developed, this time can be minimized and will free-up firewall administrator's time to perform other important security activities based on the outputs of the SIEM. A use case is defined as an actionable, logical and reportable component of a SIEM solution. It can be a rule, a report, an alert or a dashboard that solves a set of requirements. SIEM is a "force multiplier" (Chuvakin, A. 2014), meaning without any trained staff with the right capabilities, SIEM alone cannot do much. Zero staff with a SIEM tool will result in zero output. Hence appropriate use cases with staff time ensure some value from this tool (Chuvakin, A. 2014).

As highlighted earlier, SIEM use cases depend on the risks and priorities of an organization. Popular use cases can be identified based on the latest threat reports such as reports from Verizon, McAfee, Symantec, etc. Some of the popular use cases and the use cases specific to utilities are listed in section 2.6. Consider these after conducting risk assessment and penetration tests.

Detailed use case development methodology is not covered in this paper. Security managers interested in developing use cases can refer to *Effective use case modeling for SIEM* a SANS gold paper by Daniel Frye (Frye, D. 2009) and *HP attack life cycle use case methodology* white paper from HP (HP. 2014).

With a small virtual SOC capability, utilities must exercise diligence with data collection, as there is a limit to the amount of data that can be collected and analyzed. The focus must be on quality and not quantity. It is important to have a clear understanding of what the organization is looking to detect and remediate based on the *events of interest* (EoI). This information can be gathered by the outcomes of risk assessments, penetration tests, network architecture, list of critical assets and industry threat reports.

Popular use cases (Chuvakin, A. 2014, May 14) (Mehta, L. 2014) that are relevant to utilities:

- Authentication tracking: Implement this use case to track authentication information across various systems to detect unauthorized access.

- IDS/IPS alert validation: A properly configured and fine-tuned IDS and IPSs provide actionable alerts. Sometimes these alerts can be either false positives or false negatives. Hence, validation of these alerts is important and the SIEM tool can correlate these alerts with other artefacts such as an unauthorised outbound connection or deviation from a particular traffic pattern i.e., network traffic anomaly, etc.
- Monitoring of suspicious outbound connection: Information related to this type of network traffic can be found in firewalls, IPS/IDS and web proxy servers. Correlating events from all these sources by a properly configured SIEM can alert suspicious external activity or a compromised internal host.
- Excessive web or email traffic, either inbound or outbound: This can be due to compromised internal systems. By analyzing netflow information, destination addresses (to identify malicious destinations, threat intelligence feeds into IDS/IPS is necessary) and IPS alerts, suspicious activities can be identified and thwarted.
- Unauthorized server connection to Internet: In most cases, internal servers must not connect to the Internet. By analyzing destination address, netflow information and verifying antivirus logs on the server, potential server compromise can be identified and alerted by the SIEM tool.
- Password brute force attacks: An inventory of all key privileged accounts, system accounts, engineers' accounts and SCADA support users must be tabulated. Logging of number of invalid login attempts on these accounts must be enabled on either Group Policy Object settings or local security policy (Windows platform) settings. This can be extended to all other users during the second and third years of SIEM deployment.
- Anomalous ports, services, missing patches and vulnerability information of key systems and devices: The output of vulnerability scans must be fed into SIEM to detect malicious activities in the network. Missing patch

alerts must be forwarded to platforms support team and any port scanning activities must be forwarded to network services support team.

Industrial Control Systems / SCADA specific use cases:

- Ingress and egress filtering into ICS networks: Traffic into and from ICS networks remain fairly consistent. Profile this traffic, and any deviation from this pattern can be a potential intrusion, which needs to be investigated by the network support team. The same applies to other sensitive networks contained within ICS network that are segregated by a firewall.
- Traffic destined to the Internet service from ICS network: Usually traffic from the SCADA network is destined to applications and systems in SCADA De-Militarized Zone (DMZ) or very few corporate applications. If a particular traffic is destined to the Internet or some other host in the corporate network, it needs to be investigated.
- Mass disconnection and reconnection of smart meters: Disconnection and reconnection of smart meters must happen only during the meter firmware update process or certificate renewal process. If a large number of meters are getting disconnected and reconnected outside these reasons, it needs to be investigated.
- Unusually high number of Port scans and ICMP traffic: To check the availability or troubleshooting of IP based field devices, The Internet Control Message Protocol (ICMP) traffic is usually allowed in ICS environment. Excessive ICMP traffic could be an indication of a Denial of Service (DoS) attack. Such traffic and excessive port scans must be investigated.
- Out of disk space or significantly reduced free disk space: Systems and network devices usually do not generate excessive logs within the ICS environment. Logs are usually written in real time to historians located in

SCADA DMZ. High consumption of disk space either due to excessive logging or any other means must be investigated.

These use cases can be used during the first year (and possibly for second year as well) of the newly built integrated SOC. With periodic reporting of the security operations to senior management and depending on the results of the analysis performed, further investment in SIEM or SOC expansion activities may be justified. This investment can be spent on increasing the SIEM storage capacity, configuring more uses cases, and recruiting/promoting additional SOC team members for the second or third year of SOC operations.

In section 2.2, a recommendation was made to use automated vulnerability scanners to enhance the SIEM monitoring activities. Vulnerability scanning tools are usually very intrusive and generate large amount of network traffic. Using such tools is generally acceptable in the corporate network since most of the systems and devices are designed to handle high loads. The same is not true in the SCADA networks. It is recommended to use passive vulnerability scanners in the SCADA networks. These tools sniff and buffer the network traffic for further analysis rather than bombard the target with packets.

Since the integrated SOC staff come from IT and OT support teams, relevant use cases must be assigned to relevant teams based on their skills. Over a period of time, with appropriate training and experience, IT and OT support teams can handle any use case whether IT related or OT related.

2.7. Difference between IT and OT operations

Information Technology (IT) is different than Operational Technology (OT) in several important areas such as network architecture, support agreements and the culture of the system owners. Apart from utilities, ICS environments are common in places with a strong engineering and operations culture (SANS-ICS, Cole, E. 2014). OT systems requirements mandate real-time production networks whereas IT network SLA's differs depending on the application. Because of these differences, in-house OT teams have provided support of OT infrastructure. Detection and monitoring controls, such as SIEM, were usually deployed in the corporate network but not in the ICS environments. Due to segregation of duties (SoD) requirement, and the sensitive nature of OT operations, OT has traditionally not factored either implementing SIEM type solution or forwarded logs to an enterprise SIEM tool (EY, 2013).

Understanding some of the differences in IT and ICS world (SANS-ICS, Cole, E. 2014) will help both IT and OT support staff to respect each other's requirements in determining appropriate use cases for SOC activities. SANS ICS/SCADA Security Essentials training material highlighted some of the key differences between IT and OT networks, as illustrated in ***Table 4***.

IT	ICS
High throughput required for systems, applications and network devices	Real-time operations, delays are not acceptable and quick turnaround times are required
Availability of network depends on various application requirements, but predetermined maintenance windows are factored for system maintenance	Availability is king and any system changes are meticulously planned for outages or managed with high redundant systems
Security tools are designed for corporate applications	Security tools need to be adapted for the implementation in ICS environment. Although this trend is now being reversed with ICS specific tools such as data diodes, application firewalls, etc.
Common Windows / Linux operating systems	Mixture of Windows, Linux and real time operating systems
General skills and competencies readily available	Specific engineering roles with additional IT skills, very rare to get the skilled resources
Enormous system computing power and storage is available	Computing power, storage and memory are often constrained in field devices
Standard protocols are common	Industrial and proprietary protocols are common
Hardware lasts 3 to 5 years	Hardware lasts 10 to 15 years
Common maintenance and support options are readily available	Maintenance and support typically comes from the supplier of the devices
Latest personal computing devices are easy to integrate	Personal device integration is difficult due to computing resource constraints.

Table 4

Dedicated SIEM collectors can be installed in ICS/SCADA environment. Consolidated logs can be securely transferred to SIEM tool through data diodes to ensure that the network segregation between IT and OT network is maintained. Many SIEM vendors provide role based access control (RBAC) and SoD capability. While selecting a SIEM solution, it is important to ask specific questions about this feature so that the OT team is comfortable when working with the IT team in SOC activities. Some vendors offer preconfigured ICS specific reports and use cases. It is worth evaluating these options as part of SIEM evaluation (AlienVault, 2011).

With the virtual SOC team (shared resources), tools, process and use cases in place, the integrated SOC will be able to publish periodic reports. These periodic reports will help the team to prepare executive reports for the senior management's information. With some tangible information about the security status of the organization, the team now has a place at the senior management's table. The continued interaction with senior management will help in educating and raising awareness of cyber issues and eliminating complacency. This should be helpful in securing additional funds for enhancing SOC capabilities in a phased manner over multiple years.

The reporting regime to senior management should not change whether the SOC is internal or outsourced to a Managed Security Services Provider (MSSP). Reporting security status by an MSSP may be valued more due to their specialist skills in providing such services to multiple customers. This may help a utility to get management's support for security projects.

2.8. Outsourcing SOC to a MSSP

Due to the challenges in recruiting skilled resources and the cost to build an internal SOC, some utilities might opt to outsource security monitoring to a MSSP. After understanding the risks to their organization by performing a risk assessment and gap analysis, some organizations may decide not to build their own integrated SOC. With management's approval for additional funding, it might be practical to outsource the SOC function to a MSSP. For this arrangement to be successful, organizations must understand what they want from a MSSP and include appropriate use cases with metrics and Service Level Agreements (SLA) that meet the defined requirements and scope of works.

For after-hours response, many utilities have on-call IT support staff. Some of the SIEM alerts can be forwarded to these staff for initial investigation. Based on the alert type, it can be prioritized, and further investigation can be initiated later by the dedicated SOC analyst (more details about this resource are covered in the second paragraph of *Training Requirements* section). If the SOC needs to be monitored 24 hours a day, 7 days a week and a MSSP provides after hours service, then clear alerting requirements, escalation process and other SLA's must be defined. Amongst the three security pillars – confidentiality, integrity and availability, most of the utilities infrastructure operators' key requirements are infrastructure and information availability followed by integrity and then confidentiality. Technologies, processes, staff skills and use cases to build SOC capabilities must be based on the priorities of these key requirements (HP, 2011).

MSSP service cost depends on the number of devices and the type of device being monitored. To minimize the cost of such a service, it is important to identify critical business assets, enable logging either on those assets or devises holding such assets instead of all the devices/assets in a particular IP subnet. Once the critical assets are tabulated, risk assessments must be performed to identify appropriate monitoring and response use cases.

Even though it may be a lower cost option to outsource SOC function to a MSSP than building in-house (Rothke, B. 2012), utilities must understand that they will not get all the functionality provided by an in-house built SOC. In most cases, outsourcing the SOC function of a corporate network is plausible but not the ICS network. In many instances, ICS networks are part of critical infrastructure, and many utilities wouldn't prefer to outsource any services related to critical infrastructure. If a particular utility goes down that path, a thorough assessment of MSSP's business plan, staff profile, scope of works along with the use cases, performance metrics and SLA's must be agreed upfront. The outsourced SOC reporting and escalation process must be tightly integrated with the organization's incident response process.

Some of the advantages of an outsourced SOC are,

- Upfront capital cost avoidance
- Access to pool of talented resources
- Additional threat intelligence feeds

- Scalable and flexible in terms of capacity

The downside of an outsourced SOC are lack of customization, loss of control of end to end incident management process, loss of intellectual property, limited knowledge of organizations environment and log data that might not be archived.

Some of the leading SOC service providers in Australia are Symantec, Wipro, Verizon and Earthwave. *Outsourcing Managed Security Services* by Software Engineering Institute – Carnegie Mellon University (Allen, J., Gabbard, D., & May, C. 2003) is a good reference document to build a MSSP contract.

3. Conclusion

It is expected that organizations across the globe will be spending $70 billion on information security this year (Head, B, 2014). Cyber-attacks cannot be prevented and will continue to occupy newspaper headlines. At best organizations can try to defend against those attacks and demonstrate to the stakeholders that best possible security controls were implemented. Demonstration of such prudency begins with a good incident response process with a practical SOC solution. Even though it can be expensive to build a fully functional SOC that operates round the clock, with careful planning, an effective SOC can be built with limited resources. This paper was written as a starting point for the security managers at utilities to think how this can be achieved.

It is difficult to find and retain good information security resources. Providing an opportunity to existing IT support staff with a clear career growth path in information security domain could be also a good retention strategy.

By no means are the contents of this paper an exhaustive plan to build an IM process and SOC journey. Much work needs to be done in building utility specific detailed use cases that can be readily implemented by utilities. Standard operating procedures to manage SOC alerts and tighter integration with incidence management process is a domain that needs more work.

Team members with the right skills, an appropriate SIEM tool, and the associated processes are required to build a good security incident management capability. Security managers would have to undertake a series of activities to build a SOC that meets the organization's needs. A checklist with the chronological order of activities that need to be considered is listed in the appendix B. This list was compiled after reviewing many artefacts listed in the reference section.

All security practitioners know that it is not a matter of *if* but *when* a cybersecurity attack compromises an organization. Implementing detective controls to identify such attacks, before someone else outside the organization does, is the best thing to do. Hence utilities as a priority should consider options and not be afraid to take first steps to establish a SOC.

4. References

AlienVault. (2011, January 1). AlienVault ICS SIEM Datasheet. Retrieved September 8, 2014, from http://176.9.232.147/docs/AlienVault-Datasheet-ICS-SIEM.pdf

Allen, J., Gabbard, D., & May, C. (2003, January 1). Outsourcing Managed Security Services. Retrieved September 9, 2014, from http://repository.cmu.edu/cgi/viewcontent.cgi?article=1578&context=sei

Boyd, J. (2012, January 1). OODA Loop methodology for decision making. Retrieved September 8, 2014, from http://www.valuebasedmanagement.net/methods_boyd_ooda_loop.html

Chuvakin, A. (2009, June 20). Why No Open Source SIEM, EVER? Retrieved September 7, 2014, from http://chuvakin.blogspot.com.au/2009/06/why-no-open-source-siem-ever.html

Chuvakin, A. (2014, July 14). "Stop The Pain" Thinking vs the Use Case Thinking. Retrieved September 7, 2014, from http://blogs.gartner.com/anton-chuvakin/2014/07/17/stop-the-pain-thinking-vs-the-use-case-thinking/

Chuvakin, A. (2014, May 14). Popular SIEM Starter Use Cases. Retrieved September 7, 2014, from http://blogs.gartner.com/anton-chuvakin/2014/05/14/popular-siem-starter-use-cases/

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August 1). Computer Security Incident Handling Guide. Retrieved September 7, 2014, from http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

Cole, E. (2004, March 23). SANS ICS/SCADA Security Essentials, Sydney

EY. (2013, January 1). Security Operations Centers against cybercrime. Retrieved September 8, 2014, from http://www.ey.com/Publication/vwLUAssets/EY_-_Security_Operations_Centers_against_cybercrime/$FILE/EY-SOC-Oct-2013.pdf

Frye, D. (2009, September 21). Effective use case modeling for SIEM. Retrieved September 7, 2014, from http://www.sans.org/reading-room/whitepapers/bestprac/effective-case-modeling-security-information-event-management-33319

Head, B. (2014, September 9). Banks in hackers' sights despite $70b spent on security. *The Age*. Retrieved September 9, 2014, from http://www.theage.com.au/it-pro/security-it/banks-in-hackers-sights-despite-70b-spent-on-security-20140908-10dtav.html

HP. (2011, January 1). Building a successful security operations centre. Retrieved September 7, 2014, from http://h71028.www7.hp.com/enterprise/downloads/software/ESP-BWP014-052809-09.pdf

HP. (2014, January 1). HP Attack Life Cycle use case methodology. Retrieved September 7, 2014, from http://h20195.www2.hp.com/V2/GetPDF.aspx/4AA4-9490ENW.pdf

InfosecNirvana. (2012, June 21). SIEM use cases - What you need to know. Retrieved September 8, 2014, from http://infosecnirvana.com/siem-use-cases/

ISACA. (2013). *Responding to targeted cyberattacks*. Rolling Meadows, IL: ISACA. Retrieved September 7, 2014, from http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Responding-to-Targeted-Cyberattacks.aspx

Lacey, D. (2013). Security technology measures to mitigate APT attacks. In *Advanced persistent threats how to manage the risk to your business*. Rolling Meadows, IL: ISACA.

McAfee, I. (2013, January 1). Creating and maintaining a SOC. Retrieved September 7, 2014, from http://www.mcafee.com/au/resources/white-papers/foundstone/wp-creating-maintaining-soc.pdf

Mehta, L. (2014, May 15). Top 6 SIEM Use Cases - InfoSec Institute. Retrieved September 6, 2014, from http://resources.infosecinstitute.com/top-6-seim-use-cases/

Rasche, G. (2013, December 1). Product AbstractGuidelines for Planning an Integrated Security Operations Center. Retrieved September 8, 2014, from http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002000374

Rothke, B. (2012, March 1). Rothke rsa 2012 building a security operations center (soc). Retrieved September 8, 2014, from http://www.slideshare.net/Benrothke/rothke-rsa-2012-building-a-security-operations-center-soc

Sweeny, J. (2011, June 20). Creating Your Own SIEM and Incident Response Toolkit Using Open Source Tools. Retrieved September 7, 2014, from http://www.sans.org/reading-room/whitepapers/incident/creating-siem-incident-response-toolkit-open-source-tools-33689

Trustwave 2013 GLOBAL SECURITY REPORT PREVIEW. (n.d.). Retrieved September 7, 2014, from http://www2.trustwave.com/rs/trustwave/images/2014_Trustwave_Global_Security_Report.pdf?aliId=24782742

Verizon. (n.d.). Verizon 2014 Data Breach Investigations Report. Retrieved September 19, 2014, from http://www.verizonenterprise.com/DBIR/2014/

Symantec. (2014, April 1). Internet Security Threat Report 2014. Retrieved September 19, 2014, from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

Homeland Security, D. (2013, July 1). Best Practices for Planning a Cybersecurity Workforce. Retrieved September 19, 2014, from http://niccs.us-cert.gov/research/best-practices-planning-cybersecurity-workforce

5. Appendix A – Survey Results

An *informal* survey of Australian electricity and gas utilities was carried out to understand their current security incident response capability. The survey questions were framed to get information about the existing security operations capabilities, team composition & structure, types of functions performed by the team, incident response process, tools and technologies used, staff's current skill levels and periodic reporting regime.

Survey questions were sent to 12 respondents and only 8 responded. Of the eight, four responses were received by email and the remaining four were telephone conversations. Most of the respondents requested not to publish the detailed response; instead they were okay with publishing the summary. Hence a summarized version of the responses in a tabular format is included in this paper.

	Utilities (U) 1 to 8							
Question summary	**U1**	**U2**	**U3**	**U4**	**U5**	**U6**	**U7**	**U8**
Full time resources	2	2	2	1	3	8	3	2
Part time resources	0	0	0	0	0	0	0	0
Contractor resources (Projects)	2	0	1	As needed	1	1	0	As needed
Augmemted resources	0	0	4 to 5	1	2	0	5 to 8	0
Average security experience	7 Years	6 Years	6 years	4 Years	8 Years	7 years	9 Years	8 Years
Staff Certifications	CISSP, Degree Eq	CISSP, CISM	CISSP, CISM, CISA	CISSP	CISSP, CISM, GSEC	CISM	CISSP, GSEC, GCIH	CISA, CISM
External threat intelligence feed	MSSP Provider	CERT, AusCERT	CERT, Vendors, AusCERT	No Info	Vendors, AusCERT	CERT, SIEM feed, AusCERT	CERT, AusCERT, Vendors	CERT, SIEM feed, AusCERT
Security information exchange forum	NIE	AISA, ISACA	AISA, ISACA		AISA, ISACA	AISA, ISACA	AISA, ISACA	AISA, ISACA
Security operations function performed by	In-house	In-house	IT Infra team	No Info	In-house	In-house	In-house	In-house IT Infra
Any dedicated security operations resource	No	No	No	No Info	No	Yes	Yes	No
Is security operations outsourced	No	No	No	No	No	No	Planning	No
What periodic security reports are produced	30 day security incident report	Audit reports only	30 day report, no details	None apart from AV report for IT support	Pen test and VA report, annually	180 day firewall report, IPS events and OT VA	Set various periodic reports to IT and OT managers	30 day various reports
Who provides OT security support	in-houst IT team	None	In-house OT team	None	In-house	In-house OT team	Hybrid	In-house OT team
How many OT security staff provide support	na	0	1	0	1	No Info	1 + Augment	No Info
Do you compile periodic security incident statistics	Yes	Yes, no info	No	No	Only PIR for major incidents	Yes, many types of reports	Yes for IT and OT teams	Once SIEM is in place, now no
What reports are presented to senior management	Serious incidents	Audit reports only	Only incident briefing	No	Only incident briefing	Audit reports only	Statistics & incidents	Only incident briefing
Is a formal security incident management process established	Under development	No	Yes	No	Yes	Yes	Yes	Under development
Security training plan for IT support staff established?	No	No	No	No	No	No	Yes	No
Is a SOC capability planned? If yes, in-house or outsourced?	Outsourced	Yes, outsourced	Yes, outsourced	No	Yes, In-house	Yes, in-house	Yes, Outsourced	Yes, outsourced
Current security technologies used	Firewall, IPS (External), AV, 2FA	Firewall, IDS, AV, remote access	Firewall, IPS, Anti-virus, SIEM (recent)	Firewall, Anti-Virus, Authentication	Firewall, IDS, Gateway content filter, AV	Firewall, IPS, Anti-virus, SIEM (recent)	F/W, IPS, SIEM, AV, 2FA, encryption,	No Info
Any specific measures to deal with APT's	Prevention, detective controls	No	No	No	No Info	Prevention, detective controls	Planning	No Info

6. Appendix B – Checklist

To build a capable Security incident management capability, a series of activities would have to be considered. These considerations were discussed in section 2 of this document. This checklist provides a view of the steps to follow to build a good incident management capability along with an integrated virtual SOC.

- □ Compile a list of critical assets
    - □ Information Assets
    - □ Business processes
    - □ Technologies supporting critical business processes
- □ Perform facilitated risk assessments
- □ Perform red team exercise or penetration test
- □ Prioritise and rank risks
- □ Define SOC mission, objectives and requirements
- □ Draft business case that aligns to ICT and organization strategy and includes, mission, objectives, requirements, staffing requirements, options to consider and SOC operating hours, measures of success and any relevant Key Performance Indicators (KPI)
- □ A separate business case for MSSP if an organisation decides to use SIEM for after office hours
- □ Identify virtual SOC team members and assess training needs
- □ Develop training roadmap
- □ Release *request for proposal / request for tender* - for SIEM product and integration activities.
- □ Develop SIEM use cases based on risks, priorities and *events of interest*
- □ Review current IT incident management process if exists and incorporate changes to accommodate for security incidents

- □ Develop new security incident management process if an IT incident management process doesn't exist. Ensure that standard operating procedures are defined for all alerts triggered by a use case.
- □ Start security training for SOC team members – complete training within the first year
- □ Purchase and integrate SIEM
- □ Complete SIEM training
- □ Pilot/test SOC functionality and incident management process targeting a small sub-set of critical assets
- □ Red team or ethical hacking exercise after deploying SIEM and operationalizing SOC to improve security incidence response process
- □ Reporting to management
- □ Evaluate SOC operation periodically against business case objectives