EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Guidelines for Planning an Integrated Security Operations Center

3002000374

Guidelines for Planning an Integrated Security Operations Center

3002000374

Technical Update, December 2013

EPRI Project

G. Rasche

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THE FOLLOWING ORGANIZATION PREPARED THIS REPORT:

Electric Power Research Institute (EPRI)I

This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ACKNOWLEDGMENTS

The following organization prepared this report:

Electric Power Research Institute (EPRI)
3420 Hillview Avenue
Palo Alto, California 94304-1338

Principal Investigator
G. Rasche

With consulting expertise provided by:

SRI International
333 Ravenswood Ave
Menlo Park, CA 94025-3493

Principal Consultants
G. Ciocarlie
Z. Tudor

EPRI would like to acknowledge the contributions of the following:
J.D. Senger, Oncor

This report describes research sponsored by EPRI.

This publication is a corporate document that should be cited in the literature in the following manner:

Guidelines for Planning an Integrated Security Operations Center. EPRI, Palo Alto, CA: 2013. 3002000374.

ABSTRACT

This report describes strategies and guidelines for utilities to plan and implement an Integrated Security Operations Center (ISOC) that includes corporate systems, control systems, and physical security. Currently, multiple groups and operators independently gather and analyze information from a datacenter, workstation networks, physical security, supervisory control and data acquisition (SCADA) systems, energy management systems (EMS), historians, and field equipment. Data is also collected and analyzed from Computer Emergency Readiness Teams (CERTs) and Information Sharing and Analysis Centers (ISACs). Correlating this data to find suspicious activity can be extremely challenging and often only occurs long after an incident happens.

An ISOC is designed to collect, integrate, and analyze alarms and logs from these traditionally siloed organizations, providing much greater situational awareness to the utility's security team. Additionally, an ISOC allows utilities to transition to an intelligence-driven approach to incident management, which is much more effective for handling advanced threats. Because of these advantages, creating an ISOC may provide significant value to utilities. However, building an ISOC requires significant technical resources, staff, and time.

This research focuses on the initial steps in the process of setting up an ISOC: developing the business case, potential organizational challenges, tradeoffs for different ISOC architectures, and planning the implementation process. These results are based on current research, engagement with utilities, and an examination of ISOC implementations outside of the electric sector.

Keywords
Cyber Incident Management
Incident Detection System
Security Event Monitoring
Security Status Monitoring
Security and Information Event Management
Security Operations Center

EXECUTIVE SUMMARY

This report describes strategies and guidelines for utilities to plan and implement an Integrated Security Operations Center (ISOC) that includes corporate systems, control systems, and physical security. Currently, multiple groups and operators often independently gather and analyze information from isolated and "stove-piped" systems that have been developed to provide security monitoring for physical, enterprise, and control system environments. As the threat landscape has evolved, there is a greater need to have a coordinated view of all aspects of an organization's security posture (situational awareness), events (both unintentional, such as a component failure; and malicious) that may impact an organization's security posture, and responses to those events.

An Integrated Security Operations Center (ISOC) is designed to collect, integrate, and analyze alarms and logs from these traditionally siloed organizations, providing much greater situational awareness to a utility's security team. Additionally, an ISOC allows utilities to transition to an intelligence-driven approach to incident management, which is more effective for handling advanced threats. Because of these advantages, creating an ISOC may provide significant value to utilities such as:

- Unified (corporate/OT) security incident management
- Optimization of security resources
- Improved threat analysis across utility domains
- Unified configuration/patch management
- More efficient forensics and root cause analysis

However, building an ISOC requires significant technical resources, staff, and time. Additionally, there may be considerable organizational barriers that must be overcome for the deployment to be successful.

The guidelines in this report represent an analysis of current guidelines from both enterprise and control systems security, integrated with results of questionnaires and interviews with organizations that have developed and deployed an ISOC. The guidelines are meant to assist organizations in identifying technical, business, and personnel requirements; developing ISOC architectures; and planning ISOC deployment and operations. Detailed plans, techniques, or operational guidance are beyond the scope of these report. Future work will focus on developing implementation guidelines for deploying an ISOC.

CONTENTS

LIST OF FIGURES

1
INTRODUCTION AND BACKGROUND

1.1 Purpose and Scope

This report assists asset owners and operators in planning and implementing technologies, processes, and procedures that consolidate cybersecurity preparedness, prevention, detection, and response capability oversight and collaboration. The quantity and types of cyber-physical systems continue to grow, and the complexity of the individual systems and their interactions and interdependencies has made human-to-human coordination of the disparate elements nearly impossible. Additionally, separate isolated and "stove-piped" systems have been developed to provide security monitoring for physical, enterprise, and control system environments. As the threat landscape has evolved, there is a greater need to have a coordinated view of all aspects of an organization's security posture (situational awareness), events (both unintentional, such as a component failure; and malicious) that may impact an organizations' security posture, and responses to those events.

This report presents an analysis of current guidelines for both enterprise and control systems security, integrated with the results of questionnaires and interviews with organizations that have developed and deployed an ISOC. The guidelines are meant to assist organizations in identifying technical, business, and personnel requirements; developing ISOC architectures; and planning ISOC deployment and operations. Detailed plans, techniques, or operational guidance are beyond the scope of these guidelines.

1.2 Integrated Security Operations Center (ISOC) Overview

1.2.1 Background Information

Security Operations Centers (SOCs) are common in physical security, business, and industrial control environments. Many organizations have one or more of these individual SOCs responsible for defined physical regions or business units. SOC capabilities range from providing basic environment or equipment status indicators to operating complex information gathering, alerting, and coordinating event responses.

ISOCs bring together the many isolated monitoring and response functions in a unified framework. The benefits of an ISOC over separate isolated SOCs include:

- Real-time intelligence
- Improved threat analysis across utility domains
- Efficient forensics and root cause analysis
- Unified (corporate/OT) security incident management
- Unified configuration/patch management
- Optimization of security resources.

While there are several security and business drivers for utilities to implement an ISOC, the process can impact the security operations of several groups in the organization and face some technological hurdles. Potential challenges to implementing an ISOC include:

- Organizational barriers between corporate and OT security groups
- Availability requirements of real-time systems limiting the quantity and frequency of event logs
- Lack of security technology available for field systems
- Lack of skilled staff to support an ISOC
- Budget constraints.

1.2.2 ISOC Architecture

Figure 1-1 shows a potential architecture for an ISOC. The ISOC integrates the security monitoring of multiple domains within a utility, including corporate IT systems, power delivery systems, generation systems, and physical security. The ISOC also includes vulnerability and threat information from external sources, such as Information Sharing and Analysis Centers (ISACs), Computer Emergency Readiness Teams (CERTs), and law enforcement.

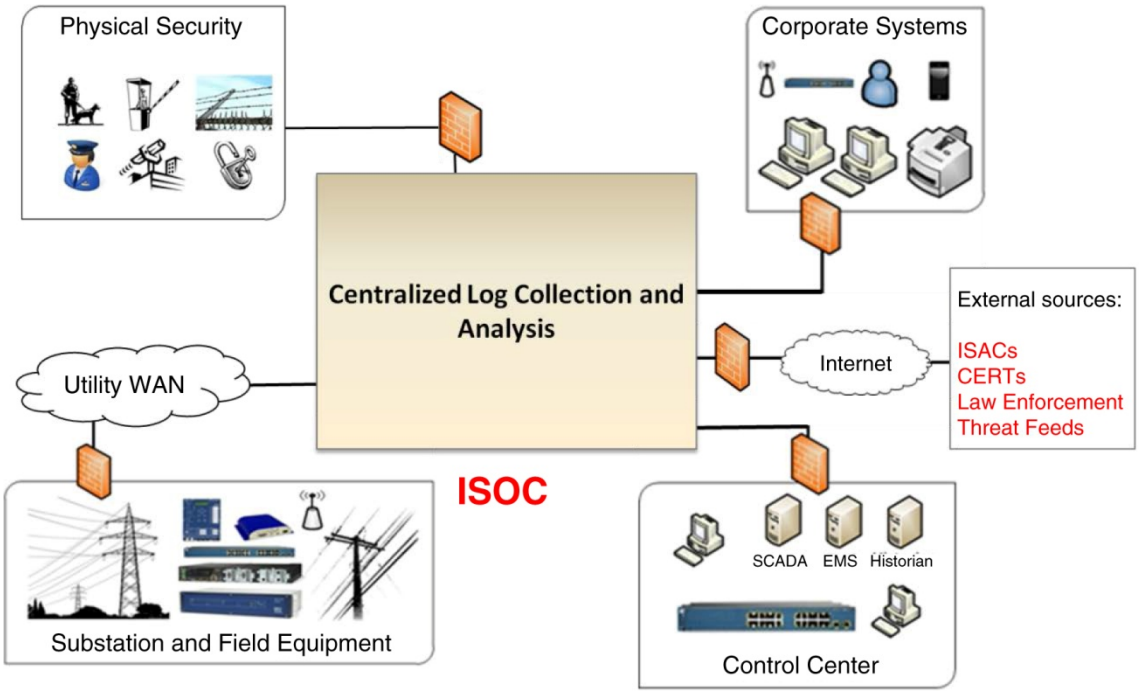

Figure 1-1
Example High-Level ISOC Architecture

1.2.3 Event Monitoring and Management

Most hardware devices, operating systems, and applications have the ability to detect and log important or interesting actions, errors, or events. Historically these event logs were in specific proprietary formats with different data elements, storage formats, and user interfaces. Recently more emphasis has been placed on using standard collection formats, transmission, and storage mechanisms to facilitate a consolidated view of events across large systems or enterprises.

Consolidated event management and log monitoring systems are at the heart of integrated security management, and a major component of an ISOC.

Many factors must be considered when developing an event log management system. There are different requirements and uses for logs and event analysis, including:

- Internal audit
- Regulatory compliance
- System performance management
- Error or malfunction diagnosis
- System misuse or attack detection
- Post-event analysis, or forensics.

When designing the event log management system, architectural issues to be considered include:

- System and application inventory
- Event types
- Logging guidelines (retention, deletion)
- Logging operations
- Logging model (distributed, centralized, hybrid)
- Log transmission
- Log storage
- Log security.

1.3 Guidelines and Standards

Although there are no specific standards or guidelines for ISOC development, many international and US government standards contain elements that may guide the development or functionality of operational elements needed for a successful ISOC. Additionally, there are best practice guides for many of the individual domains and tasks represented by an ISOC. Relevant guidelines and standards include:

- NIST Special Publication (SP) 800-92, *Guide to Computer Security Log Management* [10] provides guidance on developing enterprise logging and auditing processes.
- NIST Draft SP 800-94 Revision 1, *Guide to Intrusion Detection and Prevention Systems* [11] provides recommendations for designing, implementing, configuring, securing, monitoring, and maintaining IDPS technologies.
- NIST SP 800-83 Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops* [12] provides recommendations for improving an organization's malware incident prevention measures and provides recommendations for enhancing an organization's existing incident response capabilities.
- NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide* [13] provides guidance to help organizations develop computer security incident response capabilities and handle incidents efficiently and effectively.

- Department of Homeland Security *Recommended Practice: Creating Cyber Forensics Plans for Control Systems* [14] provides guidance for applying traditional cyber forensics concepts in control systems environments.
- Department of Homeland Security *Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability* [15] provides recommendations to help control system operators better prepare for and respond to a cyber incident.
- *The Open Source Security Testing Methodology Manual (OSSTMM)* [16] includes processes for several areas of interest in developing an ISOC including security testing, security analysis, operational security metrics, trust analysis, and operational trust metrics.
- *Information Security Management Maturity Model (ISM3)* [17], published by The Open Group, builds on standards such as ISO 20000, ISO 9001, CMM, ISO/IEC 27001, and includes general information governance and security concepts. ISM3 can be used as a template for building ISO 9001-compliant security management systems.
- *The Information Security Assurance - Capability Maturity Model (ISA-CMM)* [18], originally developed and sponsored by the National Security Agency, is based on the System Security Engineering Capability Maturity Model (SSE-CMM) and the INFOSEC Assurance Capability Maturity Model (IA-CMM) and is modified to address the information security assurance processes. The ISA-CMM appraisal focuses on a provider organization's capability to support Information Security analysts in conducting their mission objectives (i.e. to provide quality Information Security Assurance or Evaluation). The ISA-CMM is used to measure two things: the maturity of processes (specific functions) that generate products (e.g., identified vulnerabilities, countermeasures, and threats) and the level of compliance a process has with respect to an Information Security Training and Rating Program (ISATRP) methodology.
- *Information Technology Infrastructure Library (ITIL)* [19] is a set of practices for IT service management that focuses on aligning IT services with the needs of business.
- *ISO/IEC 27001* [20] is an international information security standard that is a specification for information security management systems (ISMS). An independent accreditor may accredit organizations that meet the standard.
- *Control Objectives for Information and Related Technology (COBIT)* [21] is a framework created by ISACA for information technology management and IT governance, and has tools relate control requirements, technical issues and business risks.
- EPRI's *Cyber Security Solutions for Instrumentation and Control Systems, Topic 3: Security Status Monitoring* [28] provides guidelines for security event monitoring in fossil generation plants.

Some of the representative IT industry organizations have also proposed guidelines for developing ISOC frameworks [22], [23], [24], [25].

1.4 Relevant Research

There are few research and development activities focused on implementing or deploying ISOCs:

- The DHS Science and Technology Directorate has funded a three-year research program to explore what makes and sustains good Computer Security Incidence Response Teams

(CSIRTs). The results should help organizations ensure that their CSIRTs fulfill their maximum potential and become an invaluable tool in securing a cyber infrastructure. The interdisciplinary team working on the new project includes cyber security and business researchers from Dartmouth College, organizational psychologists from George Mason University, and researchers and practitioners from Hewlett-Packard.

- Research efforts focus on ways in which the data collection can be done in an efficient manner. Kowtha *et al.* [26] propose an operations center characterization model to create a common underlying framework for collaboration, which enables rapid data collections and visual analysis.
- Other research efforts focus on building frameworks that are highly scalable. Wei *et al.* [27] address the need for coping with legacy systems, while providing modularity, scalability, extendibility, and manageability for protecting power grid automation.

2
DEFINITIONS AND ACRONYMS

This section provides definitions and acronyms for key terms as they are used in this report. When the definition is referenced from another document, the source is noted in brackets.

2.1 Definitions

Attack Vector: the channel, mechanism, means or mode that can be exploited to conduct an attack or to circumvent the security environment and system cyber security controls of a computer, digital device, or a network.

Change Management: the process of requesting, determining attainability, planning, implementing, and evaluating changes to a system. It has two main goals: supporting the processing of changes and enabling traceability of changes.

Critical Cyber Asset: a digital component of a critical system or infrastructure that, if compromised, represents a risk. Also refers to BES cyber system and any associated cyber assets.

Compensating Controls: A compensating control is a cyber security control implemented as an alternative to a recommended control that provides equivalent or comparable control.

Intrusion Detection and Prevention System (IDPS): from NIST 800-94: [An *intrusion detection system* (IDS) is software that automates the intrusion detection process. An *intrusion prevention system* (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents. IDS and IPS technologies offer many of the same capabilities, and administrators can usually disable prevention features in IPS products, causing them to function as IDSs.]

Patch: software or firmware intended to fix problems or update a program or its supporting data. This includes fixing security vulnerabilities and improving usability or performance.

Patch Management: overall guiding process to implement patches for installed software and firmware.

Security Information and Event Management: a security product or service that combines the functionality of security information management with a security event manager. Capabilities of a SIEM typically include data aggregation, correlation, alerting, compliance, and data retention.

Technical Cyber Security Controls: cyber security controls (i.e., safeguards or countermeasures) for a cyber asset that are primarily implemented and executed by the cyber asset through mechanisms contained in the hardware, software, or firmware components of the asset.

Vulnerability: from NIST SP 800-40: [A flaw in the design or configuration of software that has security implications. A variety of organizations maintain publicly accessible databases of vulnerabilities.]

2.2 Acronyms

CISO	Chief Information Security Officer
DHS	U.S. Department of Homeland Security
EPRI	Electric Power Research Institute
ES ISAC	Electricity Sector Information Sharing and Analysis Center
ESP	Electronic Security Perimeter
HMI	Human Machine Interface
ICS	Industrial Control System
ICS CERT	Industrial Control Systems Cyber Emergency Response Team
IDPS	Intrusion Detection and Prevention System
IED	Intelligent Electronic Devices
ISAC	Information Sharing and Analysis Center
ISATRP	Information Security Training and Rating Program
ISOC	Integrated Security Operations Center
IT	Information Technology
LAN	Local Area Network
MSSP	Managed Security Service Provider
NERC	North American Electric Reliability Corporation
NERC-CIP	NERC Critical Infrastructure Protection
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
OS	Operating System
OT	Operations Technology
PC	Personal Computer
PLC	Programmable Logic Controller
RTU	Remote Telemetry/Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SEM	Security Event Monitoring
SIEM	Security Information and Event Management
SOC	Security Operations Center
SP	Special Publication
US CERT	United States Computer Emergency Readiness Team
VPN	Virtual Private Network
WAN	Wide Area Network

3
ISOC PLANNING AND REQUIREMENTS DEVELOPMENT

Building an ISOC can be a multi-year process that requires significant planning and investment. Once the business drivers and potential challenges have been identified, several internal stakeholders must be engaged to provide technical and budgetary support throughout the planning, implementation, and operational phases of the ISOC. This section describes the process for internal stakeholder engagement, and the requirements development phase.

3.1 Process for Planning an ISOC

Several steps are required to design and plan the implementation of an ISOC. Figure 3-1 provides a high-level view of the planning process and relates each step to a section in this report. Steps one and two focus on the engagement with internal stakeholders. Steps three and four develop the requirements for the ISOC. Step five is the architectural design of an ISOC. Step six focuses on planning the implementation of an ISOC. The level of effort for each step may vary depending on the size of the utility and the current level of centralization of its security functions.

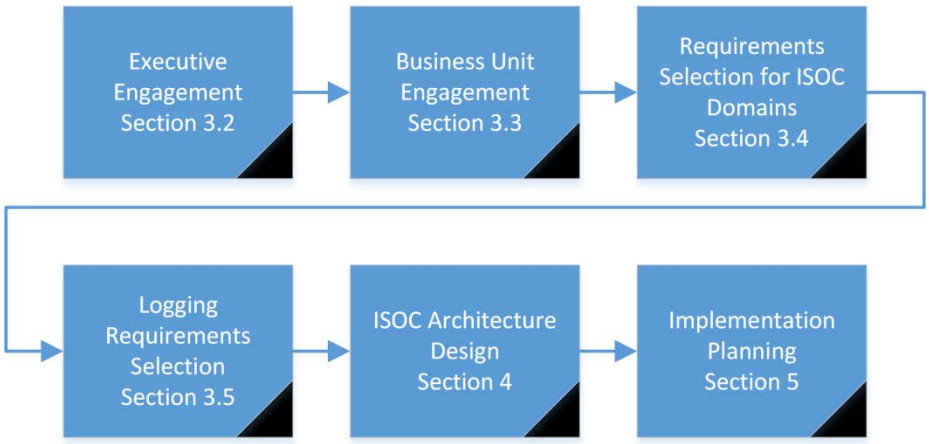

Figure 3-1
Planning Process for Implementing an ISOC

3.2 Executive Engagement

An ISOC consolidates the monitoring and incident management of systems from multiple business units within a utility, such as corporate IT, operations business units (OT), and facilities. For this to be successful, a clear directive from senior management to the heads of various business units is usually required to ensure long-term support for building an ISOC and implementing the necessary GRC processes. Additionally, financial commitments for capital investments, staff requisitions, and operating costs may require approval from senior management. Developing this executive support is a critical first step in the ISOC planning process.

While the senior management of most utilities are aware of the cyber threats facing their companies, further engagement may be required to convey the cyber security risk and the benefits of a consolidated approach to incident management. There are several ways to communicate the cyber security risk to the utility board and C-level management, such as routine presentations by the Director of IT Security or Chief Information Security Officer (CISO) on:

- Summaries of cyber event metrics, such as the number of failed and successful cyber attacks over a given time period
- Summaries of results from third-party penetration testing that expose vulnerabilities
- Detailed analysis of known threats
- Summary of overall risk to systems.

A key risk during this process is overstating the cyber security risk and losing credibility with senior management. Using the objective approach listed above to convey the security risks avoids this pitfall. There may be different security risks for IT and OT systems, based on the business functions and objectives of the two classes of systems.

Once senior management is familiar with the level of cyber risk, a clear business case for building an ISOC must be developed. In particular, the benefits of the following drivers need to be clearly stated and quantified (if possible) for senior management:

- Reduction in the redundancy of internal security resources and services
- Unified approach to incident management that covers corporate IT, business units, and physical security
- Unified configuration and patch management.

3.3 Business Unit Engagement

After senior management has provided its support and a clear directive for consolidating incident management, an ISOC champion will need to be identified to engage with the individual business units and OT domains. There are several steps involved in this process:

- Build trust with the business units;
- Explain the benefits of an ISOC to the business units;
- Educate the business units' OT staff on the operational impact of an ISOC.

A critical challenge in many utilities is a lack of trust between the corporate or central security group and the OT staff. Depending on how the utility is structured, these groups may not have a long history of interaction, or even worse, there might be open distrust or hostility based on past experiences. For example, OT staff often perceives that the corporate security group does not understand OT technology and the corporate security group perceives that the OT staff does not understand security risks and technology. Moreover, the level of cyber security expertise within utilities' business units can vary significantly from one utility to another. Depending on a particular organization's starting point, it may require a significant amount of time to build trust with the staff of the business units.

As part of the engagement with the business units, it will be critical to demonstrate the value of the ISOC to their operational responsibilities. There are two areas in particular that can show short-term value: improved log management and dedicated monitoring of critical assets such as NERC CIP assets. Managing security logs from a large number of assets requires significant resources. Pulling logs from OT systems into the ISOC provides dedicated staff and resources for managing the logs, while also making the log information available to the OT staff. The ISOC can also provide support for monitoring NERC CIP assets, though that will require training the new ISOC staff to understand the event logs of the OT systems. By offloading this to the ISOC, the OT staff will be able to focus more resources on the monitoring of the power system operations. However, the ISOC champion should be sensitive to potential concerns regarding job security for the OT staff.

Finally, a significant amount of education may be required to help the staff of the operations groups understand the impact of the ISOC on their control systems. For example, the security group may have to provide guidance to the operations groups on the process of setting up syslog and other tools. The operations group may also require detailed descriptions of any potential impact on the performance or availability of the control systems. This process may require a significant amount of time depending on the level of trust between the groups.

3.4 Selecting Requirements for ISOC Domains

Step 3 in the ISOC planning process is to develop the requirements for the various ISOC domains.

3.4.1 Corporate Systems

Currently, most utilities monitor their corporate networks and systems in a security operations center (SOC). The types of components monitored typically include:

- Routers
- Switches
- Firewalls
- Network IDS/IPS
- Web servers
- Databases
- Host systems connected to corporate networks (laptops, PCs, etc).

There is a considerable amount of literature available from NIST and other organizations to provide guidance in this domain. There are also many tools to support incident management for corporate systems as well as companies that provide managed security services. The following NIST documents, described in Section 1.3, provide an excellent resource for developing ISOC requirements for corporate systems:

- NIST Special Publication (SP) 800-92, *Guide to Computer Security Log Management* [10];
- NIST Draft SP 800-94 Revision 1, *Guide to Intrusion Detection and Prevention Systems* [11];

- NIST SP 800-83 Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops* [12];
- NIST SP 800-61 *Revision 2, Computer Security Incident Handling Guide* [13].

3.4.2 Business Units and Control Systems

Developing ISOC requirements for the business units and their associated control systems can be very challenging due to the many types of systems, devices, and vendors in power delivery systems and generation facilities. It will be critical for a utility to prioritize the systems that are included in each phase of implementing an ISOC. More information on planning the phased implementation process is provided in Section 5.1.1 below. For example, a utility may choose to create narrow requirements for the ISOC's first implementation phase and focus only on NERC CIP requirements. This could include assets such as [28]:

- Critical cyber assets within an ESP:
  - Network devices: routers, switches, modems
  - Workstations, databases, historian, etc
  - Human-machine interface (HMI), data acquisition devices, application servers
  - Field devices: intelligent electronic devices (IED), programmable logic controllers (PLC), remote terminal units (RTU), etc.
- Boundary devices
- Security software and devices within the electronic security perimeter (ESP).

3.4.2.1 ISOC Requirements for NERC CIP Systems

The impact of NERC CIP must be considered when developing the ISOC requirements. The logs and alarms for critical cyber assets must be securely transported from an ESP to a secure storage for analysis. Additionally, the ISOC should be treated as a critical cyber system, following the applicable NERC CIP requirements for physical and electronic security.

Relevant NERC CIP requirements for security event monitoring with an ISOC that includes logs from systems containing Critical Cyber Assets include the following:

- Security Status Monitoring CIP **Version 4** is addressed by:
  - CIP-007-4 R6 Security Status Monitoring, "The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security."
  - CIP-008-4: Incident Reporting and Response Planning
  - Other related requirements include:
    - CIP-003-4 R4 Information Protection, "The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets."
    - CIP-005-4a R3 Monitoring EAP Access, "Where technically feasible the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses."

- CIP-007-4 R5.1.2 Account Management, "…historical audit trails of individual user account activity for a minimum of 90 days"
- CIP-007-4 R5.2.3 Logging Account Use, "…an audit trail of the account use (automated or manual)…"

- Security Event Monitoring CIP **Version 5 (draft)** is addressed by:
  - CIP-007-5 R4 Security Event Monitoring, "Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:
    - 4.1.1. Detected successful login attempts;
    - 4.1.2. Detected failed access attempts and failed login attempts;
    - 4.1.3. Detected malicious code."
  - CIP-008-5 Incident Reporting and Response Planning
  - Other relevant requirements include:
    - CIP-005-5 R1.5 Detecting Malicious Activity, "Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications."
    - CIP-010-1 R2.1 Configuration Monitoring, "Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes."
    - CIP-011-1 R1.2 Identify and Protect Cyber System Information, "Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use."

3.4.3 Physical Security

In most utilities, physical security is under the management of the Facilities Department. However, separate management of physical security can make it difficult to correlate physical events with cyber events in real time. An example of this would be the real-time correlation of a physical breach of a substation with the detection of a rogue device on the substation LAN or a communications failure with a substation device. The inclusion of physical security events and alarms in the ISOC should be implemented using a phased approach, with critical and/or NERC CIP assets integrated first.

3.4.4 External Sources for Security Alerts

In addition to the utility's internal systems, there are several external sources of information that should be included in the ISOC design and requirements. These provide the utility with awareness of current threats and vulnerabilities that might impact the various risk profiles. Several SIEMs and vendors provide a service to incorporate threat and vulnerability information into a security operations center. Four frequently used sources of information for the electric sector are listed below:

- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- United States Computer Emergency Readiness Team (US-CERT)

- Electric Sector Information Sharing and Analysis Center (ES-ISAC)
- Law Enforcement (e.g., Federal Bureau of Investigation).

3.5 ISOC Logging Requirements

Step 4 in the ISOC planning process is to develop the requirements for transporting and storing the event logs.

3.5.1 Log Transport and Storage

The log transport and storage requirements will be highly dependent on which electric sector domains are included in the ISOC as well as on applicable regulations. For example, including a large AMI deployment in an ISOC could have a tremendous impact on the storage requirements because of the number of smart meters that are deployed. Utilities will need to work closely with their SIEM vendor to determine the storage requirements.

3.5.1.1 Retention Period for Logs and Captured Data

The retention period for logs and captured data is impacted by operational considerations as well as regulatory requirements. The utility will need to determine the period of logs that need to be at 'ready access' versus long-term storage. For example, a good practice is to keep at least one year's worth of logs at ready access. Moreover, regulation such as Sarbanes-Oxley (SOX) and NERC CIP will impact the overall retention period for logs as well as the process for destroying logs that are no longer needed. For example, NERC CIP 008-4 R2 requires utilities to keep documentation related to reportable cyber incidents for three calendar years. Other factors that need to be considered are the granularity of network traffic that is stored (e.g., headers, netflow information, full packet, etc.) and the granularity of the logs and alarms.

4
ISOC ARCHITECTURE DESIGN

Step 5 in the ISOC planning process is to select design options for an ISOC architecture and the key technologies of an ISOC.

4.1 ISOC Design Considerations

The architecture and management of an ISOC will be determined based on the requirements that have been developed, the enterprise's current monitoring and response capabilities, and the resources available to devote to ISOC development.

4.1.1 Management of the ISOC

One key design consideration is the use of third-party security service providers for managing the ISOC. Managed security service providers (MSSPs) provide monitoring and management of intrusion detection systems and firewalls as a service. MSSPs may also support other security functions, such as patch management and security audits. By outsourcing these services, a company may reduce its own security staff and focus on its core business. Many utilities currently rely on MSSPs to provide analysis and support for their corporate security operations centers.

4.1.1.1 Externally Managed ISOC

This approach extends the externally managed ISOC to include logs from operations systems and physical security. More guidance on using externally managed security services is provided in Section 5.1.3.

Pros:

- Reduces the skill and training requirements for the utility's ISOC staff
- Takes advantage of large MSSPs global footprint, allowing them to detect new threats and attack signatures early
- Reduces operational costs for the ISOC
- Potentially provides the utility with access to a 'package' of services, including remote perimeter management.

Cons:

- Most MSSPs do not have expertise in power systems
- A MSSP may not be able to meet utility-specific requirements for managing data from critical systems
- Utilities lose insight and control over the process for identifying incidents, making it difficult to tune the process to reduce false positives.

4.1.1.2 Internally Managed ISOC

The other end of the spectrum is the internally managed ISOC. With this approach, the utility has internalized the management and staffing of all aspects of its ISOC.

Pros:

- Provides full control by the utility over the incident analysis and response processes
- Reduces concerns about the storage and transport of security logs and sensitive data
- Develops strong internal cyber incident response capabilities for the utility.

Cons:

- Requires the utility to maintain 24x7 staffing support
- Requires utility staff to be trained in multiple security disciplines
- Requires utility staff to track new threat information and may require them to obtain government security clearances
- Necessitates that the ISOC security tools are fully maintained by the utility staff and constantly tuned by the utility to reduce false positives and false negatives.

4.1.1.3 Hybrid Management

A hybrid management approach seeks to combine the prior two approaches to match the capabilities and resources of the utility. For example, a utility may choose to staff the ISOC during normal business hours, but rely on a MSSP to enable 24x7 monitoring.

Pros:

- Reduces staffing requirements for the ISOC
- Takes advantage of the security expertise and threat tracking capabilities of the MSSP
- Develops internal incident response capabilities for the utility.

Cons:

- The utility loses control over part of the incident management process
- This requires knowledge transfer in both directions: power systems knowledge from utility to MSSP and security knowledge from MSSP to utility.

4.2 ISOC Architectures

There are many possible ways to design an ISOC that meets a set of requirements. Every ISOC will be unique, but all will have common elements. This section examines two approaches to the architecture of the ISOC.

4.2.1 Multi-Center Distributed Architecture

A multi-center distributed architecture relies on a hierarchical ISOC approach and is illustrated in Figure 4-1. In this architecture, each business unit is responsible for managing alarms in real-time and only critical alarms are brought to the attention of the ISOC staff. All logs and alarms may be sent to the ISOC, but event correlation would likely be performed offline.

Pros:

- Reduces training expenses for the ISOC staff since they do not need to be experts in all of the utility's domains
- Requires fewer staff for the ISOC
- Reduces likelihood of false positives for ISOC staff since only critical alarms are brought to their attention.

Cons:

- ISOC staff does not have a real-time view across the enterprise, making it difficult to correlate events and alarms that may appear non-critical to the domain staff
- ISOC staff must develop detailed policies and procedures for each business unit to identify critical alarms that should be brought to the ISOC's attention.

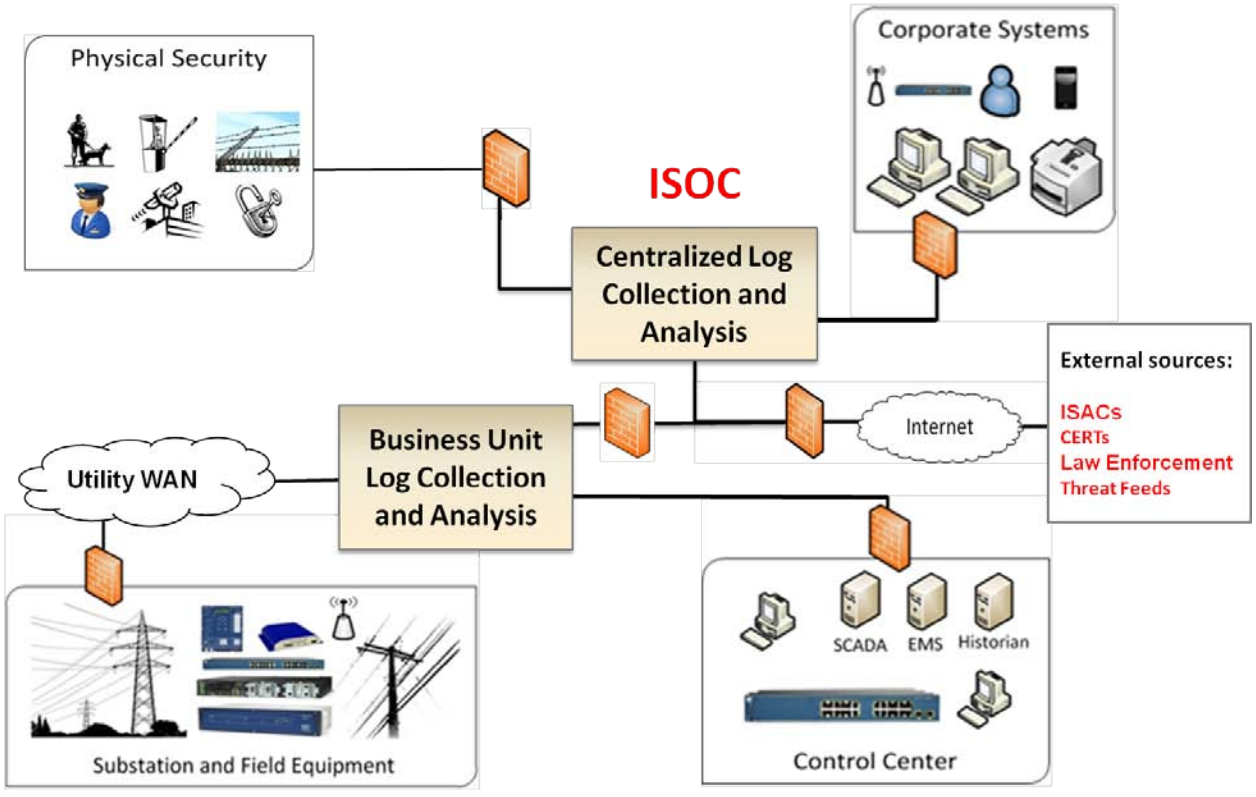

Figure 4-1
Multi-Center Distributed Architecture

4.2.1.1 Fully Integrated Architecture

A fully integrated architecture (see Figure 4-2) provides real-time monitoring for all of the business units in the utility: corporate systems, operations units, and physical security. This approach would likely be used by large utilities with significant resources to apply to cyber security.

Pros:

- Provides real-time situational awareness across the entire enterprise
- Easier detection of cross-business unit incidents since the ISOC staff can correlate events across the enterprise
- Develops internal capabilities for identifying and responding to incidents across multiple business units
- Supports an intelligence-driven approach to incident detection.

Cons:

- Requires staff to be experts in multiple utility business units (corporate IT and OT domains)
- Requires staff to be well trained to provide incident response capabilities and forensics support to different business units.

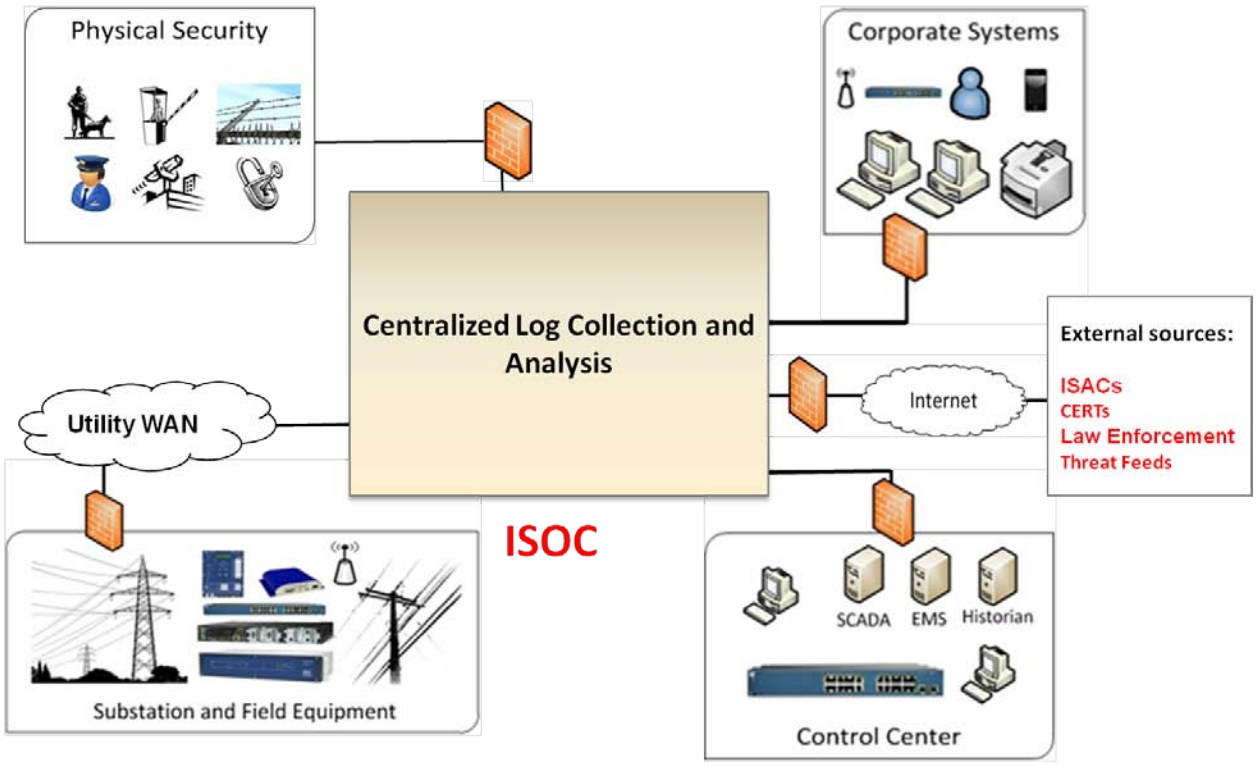

Figure 4-2
Fully Integrated Architecture

4.3 Key Technologies

The major technologies used in an ISOC can be grouped into four categories (Figure 4-3):

- Logging
- Data management
- Analysis
- Workflow

Within each of these categories there are basic applications that are reasonably simple and inexpensive to deploy, as well as robust, highly capable (and expensive) applications that can be tailored to individual enterprise needs. One key consideration for the OT domain is how to deploy detection and monitoring equipment that will have no negative impact on critical operations. Many common enterprise technologies such as intrusion detection systems and anti-malware systems are less common in the OT environment, and operating and maintaining these systems in the OT domain requires careful planning.

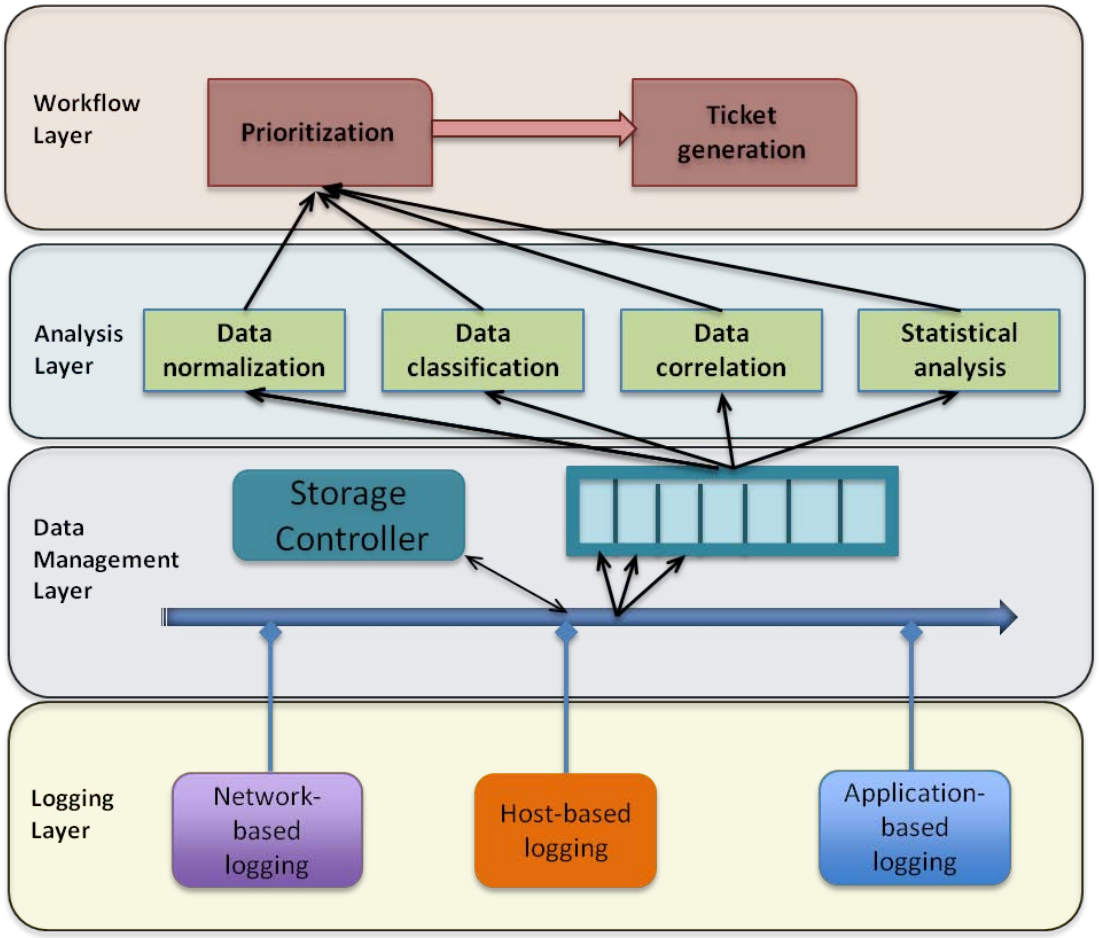

Figure 4-3
Key Technologies Used at the Different Layers of an ISOC

4.3.1 Logging

The logging layer is intended to include the basic coverage necessary to drive the ISOC analysis. Ideally, an ISOC should collect the minimal set of information needed to achieve coverage of the events happening inside a utility, but as additional data sources are available it should be able to include them seamlessly. The complexity of the logging applications can vary as well as the scope of their functionality.

4.3.1.1 Network-based Logging

Network traffic monitoring systems are designed to analyze the inbound and outbound communication flows for the network in scope. The logging layer can include several traditional network-sensing tools to extract such information (IP addresses, ports, etc.), session layer audit records (Netflow, RMON) and overall network monitoring information (SNMP). More advanced event generation applications include anti-virus, malware detection, and IDPS.

4.3.1.2 Host-based Logging

Host logging applications capture activity on privilege-escalation events, log destruction, and internal host activity. However, these internal activity sensors are themselves subject to increasing attack, possibly resulting in the disabling or complete removal of the security service. Consequently, in addition to host-based logging applications, more advanced event generation applications that monitor the behavior of the host sensors could detect host-security disablement. Applications that aim to provide data loss prevention are also relevant at this level.

4.3.1.3 Application-based Logging

At this layer, applications are instrumented at the source code or binary level. There are advanced technologies that offer these capabilities and generate logging information. Given the highly critical deployment environment of control systems, the host-based and application-based logging might not be suitable when resource constraints are also in place.

4.3.2 Data Management

The data management layer includes two different functions: first, to disseminate data from the logging layer, and second, to store data reliably. Both processes need to be achieved in a secure fashion (for both data in transit and data at rest). There are different architectures that can be employed for data management, depending on whether the ISOC provides real-time capabilities, or a centralized or distributed approach is employed. Other factors, such as data normalization for consistent semantics and data replication minimization over network links to enable scalable collection, must also be considered. At this level, data can be further filtered and only the relevant information is stored.

There are two types of architectures that can be employed:

- A centralized approach –data is collected and stored in a central location, and is then analyzed. This approach is appropriate for non real-time and more flexible scalability requirements.
- A distributed approach –data is stored using distributed file systems. This approach is appropriate for higher scalability requirements. However, if real-time requirements are necessary, data can be analyzed as a stream, while storage mechanisms are only used for forensic analysis. In this case, the data dissemination mechanism has to provide real-time support.

4.3.3 Analysis

Once data is collected, the analysis layer processes it to extract relevant security events across both IT and OT domains, identifying any propagation of events from one domain to another. The majority of SIEM technologies focus on one or more of the following analysis tasks:

- Data normalization – provides a common format for the collected data at network, host, and application levels, enabling further semantics analysis.
- Data classification – provides a classification of the different events given their semantics. This process is enabled by the use of taxonomies or ontologies that can extract semantics automatically.
- Data correlation – provides capabilities that start with minimal functionality in terms of the types of events that are correlated across multiple entities in both IT and OT domains and across the two domains. Correlations can also take into account the physical and logical location information. Technologies can evolve towards more advanced capabilities that can detect multi-stage attacks.
- Statistical analysis - extends the correlation capabilities with more statistical analysis on the events collected at the three levels, operating across time and space (across multiple devices) to detect more relevant events.

Two factors that need to be considered when evaluating a technology are the detection rate and false positive rate. Individual sensors will have their own detection performance; however, the analysis module will have to improve upon their performance. Note that if the individual sensors are not able to collect events related to attacks, the analysis component will be also powerless.

4.3.4 Workflow

Once cyber events are generated, they are prioritized for action taking. Most of the time, cyber events are prioritized based on business relevance. To be resolved, they can also be categorized based on the technical skills needed. ISOC supporting technologies must also enable the dispatch of working tickets. Common trouble ticketing systems provide customizable workflow features that can be tailored to each specific process. Many commercial security management suites also include workflow features to enable cyber event response tracking.

4.4 Alternatives to Building an ISOC

Small organizations may believe that the resources required to deploy and operate an ISOC are beyond their capability, so they decide to forgo the attempt to develop greater monitoring, analysis, and response capabilities. Once requirements analysis has been completed, discrete requirements can be individually implemented to achieve benefits for a narrower scope. Examples include:

- Local monitoring and analysis of one or more key technical devices or domains
- Third party (e.g., MSSP) monitoring of critical devices, such as firewalls or edge routers
- Increasing internal analysis and response capabilities.

Organizations can achieve many ISOC benefits using free or low cost open source tools. Although they lack the full set of features and support that are provided with commercial applications, tools such as Wireshark, NMap, BackTrack, and Security Onion provide much of the basic functionality of commercial tools.

5
IMPLEMENTATION PLANNING

5.1 Implementation Considerations

Step 6 in the ISOC planning process is to identify and prioritize the order in which systems are incorporated in the ISOC. Once the initial requirements have been developed, current capabilities identified, and a gap analysis performed, an implementation plan can be developed. The decision to implement an ISOC with internal resources versus external, or some combination of the two, will determine the key steps to be taken. In many cases, hiring an experienced consultant to advise on implementation options and industry best practices will improve the chances of a successful implementation.

5.1.1 Considerations for Phased ISOC Deployment

One key consideration is to not attempt to instantly create a highly functional ISOC. A phased implementation allows the team to absorb new work and process demands over time and the team's capabilities will improve over time. The following paragraphs suggest an ordered approach to developing an ISOC capability:

- **Develop the ISOC Policies and Procedures.** Once the systems for inclusion in the ISOC have been identified, policies and procedures must be developed for the ISOC. These should include areas such as [28]:
  - Purpose, organization and resources
  - Regulatory requirements
  - Strategy including devices and software for logging, collection, aggregation, alerting, and forensics
  - Type/list of cyber events to be logged
  - Content of log records
  - Log retention and storage
  - Collection and aggregation of logs
  - Response to log processing failures
  - Log monitoring, detection, alerting, and review
  - Event correlation and forensics
  - Time stamp/clock synchronization
  - Protection of log information.
- **Hire Initial ISOC Staff**. An experienced ISOC engineer or manager can assist with ISOC architecture development, external versus internal resource decisions, tool selection, and policy and procedure development. Also, the initial ISOC hiring process will give management and HR an indication of how the hiring process will proceed for later candidates. The ability to adequately staff an ISOC may be weighed in external resourcing decisions.

- **Practice ISOC procedures under current capabilities**. The initial ISOC staff can begin trial ISOC operations to determine the effectiveness of current capabilities and processes. They will also be instrumental in developing new processes and procedures for new ISOC operations.
- **Select external partners and develop service level agreements (SLAs).** If parts of the enterprise currently use a MSSP, existing SLAs can be reviewed for effectiveness and used, as appropriate, for future external partner SLAs. The initial ISOC staff can assist in developing new SLAs and modifying existing SLAs.
- **Select and deploy SIEM and analysis tools.** The event integration and management tools are critical elements of ISOC operation. Exercising the tools as early as possible in the process will allow the ISOC staff, management, and event data providers (such as network managers) to refine roles, responsibilities and procedures.
- **Integrate new event sources into the ISOC.** Depending on the existing state of the organization's event management and operations, existing event data sources and information from MSSPs should be individually phased in. This will allow the ISOC team to adjust to the new workload, each new source, or new event management process. An effective approach to identifying new event sources is to prioritize the business processes within each business unit. The components and systems that support high-priority processes should be incorporated into the ISOC first. Staffing levels, and team skills and expertise should be reviewed in the subsequent phases to ensure ISOC goals are being achieved. The selection of sources to be deployed can be based on the ease of deployment, security impact, risk reduction, or compliance requirements.

5.1.2 Considerations for ISOC Success

Regardless of what architecture or resourcing option is selected for the ISOC deployment, some of the most important criteria for success include:

- Trained and experienced staff
- Management attention and support
- Sufficient resources for personnel and tools
- Well-defined processes.

5.1.3 Considerations for an Externally Managed ISOC

Selecting an ISOC outsourcing partner is a critical decision. Potential customers should interview managers and analysts from the outsource agency and their current customers. Once again, an experienced consultant can assist in identify credible outsourcing companies, and in contacting other outsourcing customers to collect reviews and critiques of outsources.

Some questions to ask when selecting an outsourcing partner include:

- How long has it been in business?
- What is its reputation?
- Does it already service customers in my industry?
- Does it service customers of my size?

5.1.3.1 Service Level Agreements (SLA)

The most important element of an outsourcing arrangement is the development and maintenance of SLAs. SLAs define the requirements, benchmarks, processes, and measurement mechanisms that guide the actions and interactions of the customer and outsourcing organizations. An SLA may include:

- Maximum time to perform a service
- Level of service or coverage expected
- Coverage times and frequency
- Reporting requirements
- Data destruction processes.

SLAs should be stable enough to track performance over time, but should allow flexibility when they do not meet the needs of the organization. Outsourcing SLAs should be developed for each of the key ISOC process areas that the outsourcer manages.

5.2 Key Process Areas for an ISOC

ISOC operations are heavily process dependent. ISOC processes identify roles and responsibilities, required resources, action steps, escalation criteria, and reporting requirements.

5.2.1 Key ISOC Processes

ISOC performance is process oriented. Developing and maintaining appropriate processes will allow measuring and improving the ISOC performance. Key ISOC processes include:

- Event log monitoring
- Notification
- Escalation processes
- Daily ISOC watch and watch turnover
- Shift logging
- Incident logging
- Compliance monitoring
- Reporting
- Incident investigation.

5.2.2 ISOC Staffing

Recruiting and retaining ISOC personnel are difficult given the required breadth and depth of knowledge and experience that are required. Moreover, ISOC staff must receive regular training to refresh their skills and learn new skills needed to operate new tools, or identify and respond to new threats. Management must allocate a significant training budget as the ISOC is being set up and once it has moved into an operational state. The ISOC director should also routinely run internal tabletop and training exercises.

ISOC staff requires expertise and continuous training in the following areas:

- Operating systems
- Multiple hardware platforms
- Networking systems (routers, switches, firewalls) and protocols
- Directory systems
- Database technologies
- Applications for corporate and OT domains
- Power system protocols
- Malware analysis
- Intrusion detection and prevention systems
- Programming or scripting
- Investigative/forensics processes
- Chain of custody issues
- Ethics
- Corporate policy.

6
CONCLUSION

This report provides an overview of the process for planning an ISOC, including stakeholder engagement, requirements development, and implementation planning. The centralized approach for incident management described in this report provides utilities with greater situational awareness of security events across their entire enterprise. Other advantages of implementing an ISOC include:

- Optimization of security resources
- Improved threat analysis across utility domains
- Centralized configuration/patch management
- More efficient forensics and root cause analysis.

However, building an ISOC requires significant technical resources, staff, and time. Additionally, there may be considerable organizational barriers that must be overcome for the deployment to be successful.

In the next phase of this project, guidelines for implementing an ISOC will be developed. The guidelines will examine potential challenges associated with retrieving logs from field devices, normalizing logs and alarms across different equipment vendors, and identifying gaps in the types of security alarms that are available in devices. The goal is to provide guidance for utilities as they begin the deployment phase of their ISOC.

7
REFERENCES

[1] North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards CIP-001 through CIP-009 Revision 4, CIP-010-1 Revision 5 (draft), CIP-011-1 Revision 5 (draft): www.nerc.com

[2] NIST Special Publication (SP) 800-53, Rev 3: Recommended Security Controls for Federal Information Systems and Organizations, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

[3] NIST Interagency Report 7628, "Guidelines for Smart Grid Cyber Security" Volumes 1-3, August 2010.

[4] Department of Homeland Security (DHS): "Recommended Practice: Creating Cyber Forensics Plans for Control Systems"

[5] Department of Homeland Security (DHS): "Recommended Practice: Developing an Industrial Control System Incident Response Capability"

[6] NIST SP 800-92: "Guide to Computer Security Log Management"

[7] SANS Institute: "Benchmarking Security Information Event Management (SIEM)" February 2009; http://www.sans.org/reading_room/analysts_program/eventMgt_Feb09.pdf

[8] SANS Institute: "Successful SIEM and Log Management Strategies for Audit and Compliance" November 2010; http://www.sans.org/reading_room/whitepapers/auditing/successful-siem-log-management-strategies-audit-compliance_33528

[9] CSO On Line; SIEM Do's and Don'ts, http://www.csoonline.com/article/509553/siem-security-info-and-event-management-dos-and-don-ts

[10] NIST SP 800-92, Guide to Computer Security Log Management, http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

[11] NIST Draft SP 800-94 Revision 1, Guide to Intrusion Detection and Prevention Systems, http://csrc.nist.gov/publications/drafts/800-94-rev1/draft_sp800-94-rev1.pdf

[12] NIST SP 800-83 Revision 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf

[13] NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide, http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

[14] Department of Homeland Security (DHS) Recommended Practice: Creating Cyber Forensics Plans for Control Systems, http://ics-cert.us-cert.gov/sites/default/files/Forensics_RP.pdf

[15] Department of Homeland Security (DHS) Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability, http://ics-cert.us-cert.gov/sites/default/files/final-RP_ics_cybersecurity_incident_response_100609.pdf

[16] The Open Source Security Testing Methodology Manual (OSSTMM), www.osstmm.org

[17] Information Security Management Maturity Model (ISM3), www.ISM3.com

[18] The Information Security Assurance - Capability Maturity Model (ISA-CMM), http://www.isatrp.org/isacmm.php

[19] Information Technology Infrastructure Library (ITIL) http://www.itil-officialsite.com/home/home.aspx

[20] ISO/IEC 27001, www.iso.org

[21] Control Objectives for Information and Related Technology (COBIT), www.isaca.org

[22] McAfee® Foundstone® Professional Services, Creating and Maintaining a SOC: The details behind successful Security Operations Centers, http://www.mcafee.com/us/resources/white-papers/foundstone/wp-creating-maintaining-soc.pdf

[23] “How to Build Security Operations Center (SOC)”, ftp://ftp-eng.cisco.com/cons/workshops/SP-Powersession-Thailand-Jan-2007/SPSEC-610-Security-Operations-Centers-Basics-Version-2.pdf

[24] “Building An Intelligence-Driven Security Operations Center”, http://www.emc.com/collateral/technical-documentation/h11533-intelligence-driven-security-ops-center.pdf

[25] “Building A Successful Security Operations Center”, http://h71028.www7.hp.com/enterprise/downloads/software/ESP-BWP014-052809-09.pdf

[26] Kowtha, S.; Nolan, L.A.; Daley, R.A., "Cyber security operations center characterization model and analysis," Homeland Security (HST), 2012 IEEE Conference on Technologies for , vol., no., pp.470,475, 13-15 Nov. 2012.

[27] Dong Wei; Yan Lu; Jafari, M.; Skare, P.; Rohde, K., "An integrated security system of protecting Smart Grid against cyber attacks," *Innovative Smart Grid Technologies (ISGT), 2010* , vol., no., pp.1,7, 19-21 Jan. 2010

[28] *Cyber Security Solutions for Instrumentation and Control Systems, Topic 3: Security Status Monitoring*. EPRI, Palo Alto, CA: 2013. 3002001322.

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI's members represent approximately 90 percent of the electricity generated and delivered in the United States, and international participation extends to more than 30 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together…Shaping the Future of Electricity

3002000374

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com