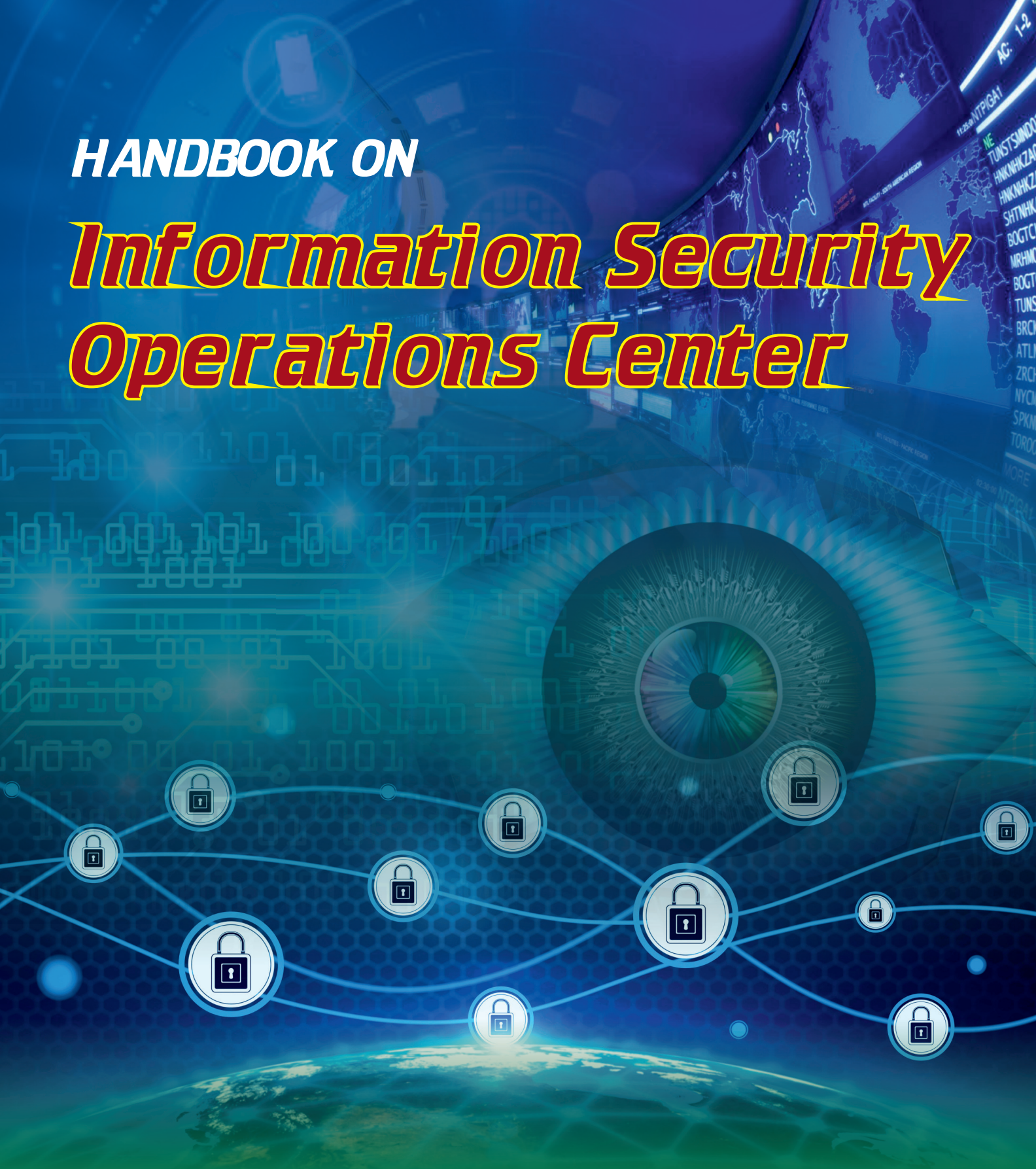


HANDBOOK ON

Information Security Operations Center

IDRBT
Explore, Enable, Excel

Institute for Development and Research in Banking Technology
(Established by Reserve Bank of India)

CONTENTS

Foreword

Early Warning System

WE are in the age of anytime anywhere banking. Technology innovation has moved banking to desktops, laptops, tablets and mobiles. The customer has grabbed banking into her palm.

Yet, she has issues with the new era digital banking because of the increasing trend in failed or fraudulent transactions. A few of the recent incidents in the banking sector have shaken her confidence. Banks have suffered financial losses on a few occasions, but their reputation loss is a matter of greater concern. The trust the customers need to have in banks for parking with their hard earned funds is critical for banking. After all, banking is based on trust.

It is the responsibility of the banks to put in place all necessary infrastructure and systems to ensure that digital banking is safe and secure. They have to ensure confidentiality, integrity and availability, the three key requirements of secured banking.

Banks have been working on security solutions at various levels. In order to put all such solutions together and to build a system that not only integrates the best features of the solutions but also a super structure that identifies abnormalities early and alerts stakeholders immediately, banks have started working on Information Security Operation Centers (ISOCs).

Though there has been considerable work done by academicians, security solution providers and banks in the realm of ISOC, there are still several issues and concerns at the stage of implementation of ISOC. IDRBT has been organizing training programmes on

ISOC for banks. During interaction with the concerned employees of banks, a need was felt to bring out a Handbook on ISOC to help banks.

Accordingly, IDRBT with the active participation of banks and solution providers, prepared the current Handbook on ISOC. It presents in detail the steps to be taken during conceiving, designing, building, maintaining and managing various phases of ISOC. It is expected that all security practitioners in banks would benefit from the handbook in every stage of ISOC implementation.

As the general principles and practices of security are common among several organisations, the handbook may be useful not only to banks but also to financial institutions and other organizations.

The team that worked on the handbook deserve best compliments.

Date: September 01, 2017
Place: Hyderabad

(Dr. A. S. Ramasastri)
Director, IDRBT

Chapter 1

Security Essentials

BUSINESS organisations are highly dependent on IT infrastructure, network system and sophisticated software applications. Through these components, they are able to carry transactions with uninterrupted flow of data and information across geographical boundaries. Along with the benefits like speed, automation, ease, etc., these components also brought threats and risks to the businesses in the form of attacks like DDOS (Distributed Denial of Service), data theft, malware, etc.

One of the major concerns is the ease and speed with which businesses are being attacked / brought down, without even the attacker paying a visit to the physical facilities of the business. Securing Information and Communication Technology (ICT) draws attention of the top management, regulators and law-enforcement alike.

As ICT evolved, securing business through ICT as well, evolved over a period of time. When PCs invaded small and big offices alike, without Internet connection, anti-virus was the security measure that was built into securing IT. When enterprise networks were built, the security was enhanced with some more devices like Firewalls, IDS (Intrusion Detection System) and IPS (Intrusion Prevention System), etc. When majority of the business transactions are stored in database and data leakage became a big concern, another concept DLP (Data Leakage Prevention) was brought in. In this manner, businesses reactively kept adding security functionalities as and when the need was felt.

At present, they are surrounded by too many security devices to deal with, which are not well-integrated. One of the major requirements of any security management is incident response. As the devices were not well-integrated, it became a bottleneck to detect threats and quickly respond to an incident. The idea of ISOC (Information Security Operation Center) emerged in order to address these concerns and the ever-changing security threat landscape.

Information Security Operation Center (ISOC) – "The ISOC is responsible for monitoring, detecting, and isolating incidents and the management of the organisation's security products, network devices, end-user devices, and systems. This function is performed seven days a week, 24 hours per day. The ISOC is the primary location of the staff and the systems dedicated for this function," defines the Wikipedia

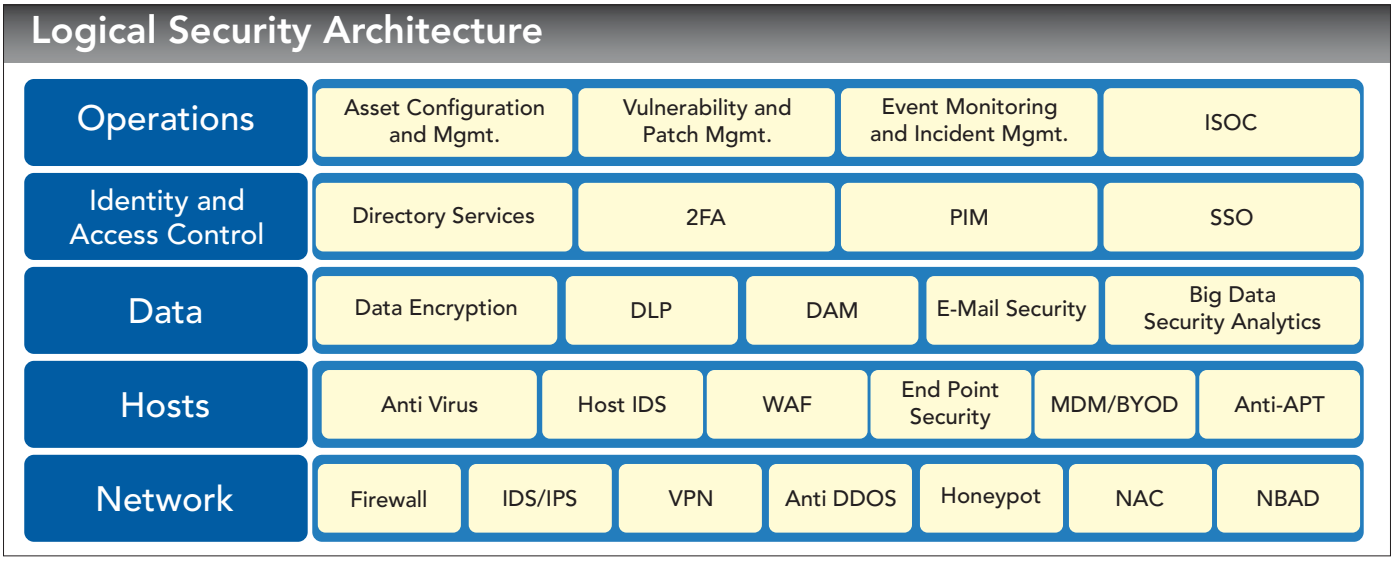
The recent attacks on financial systems prove that deploying defensive technologies like perimeter security and encryption, etc., are not sufficient and one needs to constantly monitor the security. Security is not a product that can be deployed and forgotten, rather it is a process that needs to be continuous.

The picture below shows the security features that became part of the overall IT security of a matured business organisation. This section provides an insight into how each of the security specific points found their place in the organisation. The Logical Security framework presents the defence-in-depth, layered approach to security. It is broken down into five main groups:

- **Operations:** Operating a security program requires the necessary tools to support change control and track assets based on asset classification framework. An effective security operations program is underpinned by IT Service Management. ITIL (Information Technology Infrastructure Library) is an industry respected framework to structure such a program.
- **Identity and Access Control:** People, process and technology are the pillars of any organisation and are interdependent on one

another in carrying business activities. Identity and Access Control technology can be used to initiate, capture, record and manage identities of user, device, service, system, etc., and their related access permissions in an automated fashion. This ensures that access privileges are granted according to single interpretation of policy and all individuals and services are properly authenticated, authorized and audited.

- **Data:** As organisations increasingly leverage automation of business processes through applications, more and more confidential data is held within these platforms. Securing this data gained priority as regulators and government agencies started mandating data security practices.
- **Hosts:** Security across endpoint devices that include desktops, servers, laptops and mobile devices is an essential and effective process to protect the underlying critical assets from compromise.
- **Network:** The underlying network architecture is critical to protect the applications, services, users and data from compromise. Fundamental controls are required to safeguard these assets while being connected to the network.



Securing IT in an enterprise evolved with a focus on domains like securing networks, securing hosts, securing data, deploying identity and access controls and with operations across all these domains.

1.1 Network Security

Network security is a basic necessity today. Network Security Appliances help in protecting the computer systems and other IT infrastructure inside the network from unwanted intrusions or attacks.

1.1.1 Firewalls: Network security started its journey with basic firewalls and is now capable of filtering based on content of the packet instead of just packet headers. Not able to go beyond the layer 4 intelligence of TCP/IP stack, firewalls just remained as main entrance security gateways in the entire enterprise security space.

1.1.2 IDS/IPS: Intrusion detection and prevention systems detect/prevent network attacks by:

- Filtering the traffic by applying known signatures of the malware and malicious attacks
- Analysing the traffic flow looking for deviations from normal behaviour and block the connection, if any anomaly found.

Both IDS and IPS solutions detect threat activity in the form of malware, spyware, viruses, worms and other attack types, as well as threats posed by policy violations. The IDS/IPS systems lack the visibility into application layer of TCP/IP stack and hence may not protect from application specific attacks.

1.1.3 Virtual Private Network (VPN): To protect data traversing on shared communication links from attacks like spoofing and tampering, encrypting the data on wire has become necessary. VPN creates private confidential networks on top of shared public networks like Internet by encrypting the data. VPNs thus are tamper-proof and provide secure remote employee log-in and remote branch office connection to the enterprise resources.

1.1.4 Anti-DDoS: Distributed Denial of Service (DDoS) is the fastest growing threat. It aims at bringing down the critical IT resources, by sending malicious traffic and thereby exhausting the critical resource capacity. DOS attacks can happen at any layer of TCP/IP, right from flooding the routers to opening huge number of connections to target applications. The solutions also vary at each layer. ISPs (Internet Service Providers) offer layer 3 and layer 4 DDoS protection services, guaranteeing clean pipes from volumetric DDoS attacks. However, to prevent layer 7 DDoS attacks, on-premise DDoS detection and prevention devices need to be put in place.

1.1.5 Honeypots: These are traps set up inside the network waiting for someone to attack. They work on simple concept; alert the security administrator the moment a contact is made to them.

1.1.6 Network Access Control (NAC): Non-compliant devices can be denied access to enterprise network using NAC, isolating these insecure devices from infecting the rest of nodes in the network. Examples of non-complaint devices include unauthorized devices, un-patched and not updated devices, etc.

1.1.7 Network Behaviour Anomaly Detection (NBAD): Preventative security measures are often defeated, by new polymorphic malware, and zero day exploits. Therefore, it is important to be on the watch for intruders. NBAD analyses the flow of data across all devices to understand the deviations from normal traffic. For example, certain type of traffic, say Skype from normal users can be acceptable, but the same type of traffic from servers is very suspicious. NBAD is useful in detecting the suspicious behaviour and can guide the security experts in forming rules to prevent such events to occur in future.

1.2 Host Security

Hosts are the main access points to the critical assets of the enterprise and hence it is imperative to secure the hosts.

1.2.1 Anti-Virus: The most common basic security deployed on every host is anti-virus.

1.2.2 Host IDS: As anti-virus systems work based on signature verification and cannot protect hosts from zero-day malware, the servers are protected by another layer of security, which is host based IDS. The main goal of host IDS is to keep the integrity of the server intact. It keeps monitoring the suspicious operations like configuration changes, registry changes, log re-writes, file deletes, etc. and immediately alerts/blocks as per policy.

1.2.3 Web Application Firewall (WAF): The fastest growing categories of attacks and data breaches are those that target applications. There are countless possibilities to exploit code vulnerabilities and

application modules. Almost every web-based application has one or more web application vulnerabilities listed in OWASP top 10 list. OWASP reported that 95% websites are compromised by cross-site scripting attack.

Application Threats: OWASP Top 10			
S. No.	Threat	Firewall	WAF
1	Injection (SQL, OS and LDAP)	No	Yes
2	Broken Authentication and Session Management	No	Yes
3	Cross-Site Scripting	No	Yes
4	Insecure Direct Object References	No	Yes
5	Security Misconfiguration	No	Yes
6	Sensitive Data Exposure	Yes	Yes
7	Missing Function Level Access Control	No	Yes
8	Cross-site Request Forgery (CSRF)	No	Yes
9	Using Components with Known Vulnerabilities	No	Yes
10	Unvalidated Redirects and Forwards	No	Yes

1.2.4 Endpoint Security: For overall enterprise security, it is essential to keep all endpoint devices clean, malware free and up-to-date with all required patches. EndPoint Security's main objectives include:

- Endpoints are authentic (2FA, AAA)
- Endpoints are configured properly (Configuration management)
- Endpoints are clean and virus free (Antivirus/HIPS)
- Endpoints are not vulnerable (vulnerability scanning and management)
- Endpoints are up-to-date with all necessary patches (Patch Management).

Only authentic and secure endpoints should be allowed to access the enterprise network resources.

1.2.5 Mobile Device Management (MDM): MDM software strengthens security through remote monitoring and control of security configurations, policy enforcement and patch pushes to mobile devices. Further, these systems can remotely lock lost, stolen or compromised mobile devices and, if needed, wipe all stored data.

1.2.6 Anti-APT: Advanced Persistent Threats (APT) are custom-made targeted attacks. They are capable of compromising the targeted systems with advanced coding techniques that circumvent the traditional signature based virus detection. The APT detection platforms are designed to execute the suspicious files/codes in a sandbox environment, understand their activity (registry changes, file read/write, botnet communication, etc.) and accordingly allow or deny the suspicious file to enter the enterprise network.

1.3 Data Security

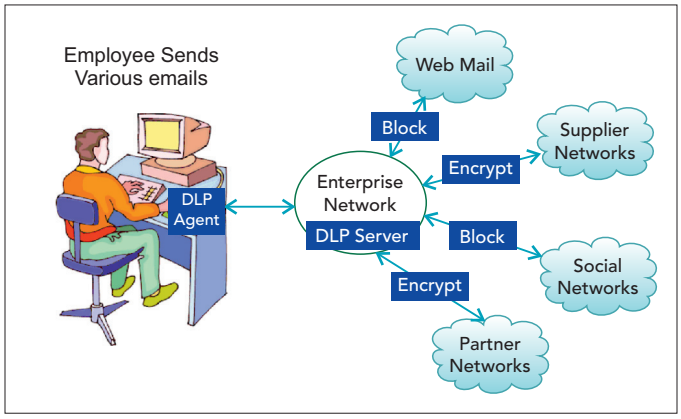
Data being one of the most critical assets, keeping the enterprise data safe and secure through various means is important.

1.3.1 Cryptographic Techniques

Cryptographic techniques address two major security challenges – confidentiality and integrity. PKI (Public Key Infrastructure) in addition is able to address authentication and non-repudiation. While the cryptographic techniques are good at safeguarding the data at rest and data in motion, they are weak in protecting the data being in operation. Attacks like man-in-memory or man-in-browser target the data, once it was decrypted or just before it is about to be encrypted. Moreover, majority of times encryption technologies are overlooked by application developers and applications get deployed without proper usage of encryption.

1.3.2 Data Leakage Prevention

According to "Intel Security 2016 Data Protection Benchmark Study", over 25% of organisations do not monitor access to employee or customer information.



Data Leakage Prevention (DLP) solutions protect sensitive data and provide insight into the use of content within the enterprise. This includes three major aspects:

Monitoring Data at Rest: Content discovery by scanning of storage and other content repositories at regular intervals helps identify where sensitive content is located. For example, one can use a DLP product to scan the servers and identify documents with credit card numbers. If that server is not authorized to keep that kind of data, the file can be encrypted or removed, or a warning sent to the file owner.

Monitoring Data in Motion: This involves sniffing of traffic on the network to identify content being sent across specific communications channels. For example, DLP can sniff emails, instant messages, and web traffic for snippets of sensitive source code, credit cards, etc. Data in motion protection tools can often block data leakage based on central data security policies, depending on the type of traffic.

Monitoring Data in Use: This aspect is addressed by endpoint solutions that monitor data as the user interacts with it. For example, they can identify the transmission of sensitive document to a USB drive and block it (instead of blocking USB drive), including things like copy and paste, etc.

The success of DLP tools are very dependent on classification of data, identifying data ownership, data security policy and data governance.

1.3.3 Database Activity Monitoring (DAM)

Monitoring database activity is a critical component of database security, especially as information that is more sensitive is consolidated into larger databases.

Database Activity Monitoring involves the capturing and recording of all Structured Query Language (SQL) activity in real-time or near real-time. They can monitor database administrator activity, across multiple database platforms; and can generate alerts on policy violations. Database activity monitoring takes place at various levels by different tools. However, five features distinguish Database Activity Monitoring tools:

- **Monitoring:** Monitor and audit all database activity, like administrator activity and Select transactions. Tools can capture all SQL transactions: DML, DDL, DCL, (and sometimes TCL) activity.
- **Secure Storage:** Storing monitoring and audit data securely outside the database.
- **Correlation and Analysis:** These tools aggregate and correlate activity from multiple heterogeneous Database Management Systems (DBMSs). Tools can work with multiple DBMSs (e.g., Oracle, SQL Server & DB2) and normalize transactions from different DBMSs overcoming the differences among many SQL flavours.
- **Segregation of Duties:** Enforce separation of duties on database administrators. Auditing must include monitoring of DBA activity, and solutions should prevent manipulation or tampering of logs or any such recorded activity.
- **Alert Mechanism:** Generate alerts on policy violations. Not only just recording database activity, they also provide real-time monitoring and rule-based alerting. For example, a rule can be created to generate an alert whenever a DBA performs a select query on a particular column, say credit card.

1.3.4 E-Mail Security: E-mail is a popular attack vector and hence individual and business accounts need to be protected. E-mail acts as a launchpad for attacks like spam, phishing and spreading malware, etc. Secure e-mail gateway that scans all e-mails and filters the malicious e-mails is now common across all enterprises.

1.4 Identity and Access Control

Various tools should be used to enforce the application or resource usage policy via the mechanism of access to the applications. Identity and access management solution with central directory of identities are integrated with applications and its underlying platform with "need to know/access" policy defined by the business layer.

1.4.1 Directory Services

Directory is like a registry where all information about users, groups, computers, servers, printers, network shares, and more are stored. Each of these are considered objects and have attributes associated with them in the directory. Security policies can be built on top of this information. Based on these policies, directory services can carry out single sign-on to network resources; lock down desktop configurations and prevent access to specific operations such as software installation or registry editing; and set access control privileges on directory objects. Directory services are one of the first centralised (single point) controllers of all applications, users, databases, files, etc., in an enterprise network. However, due to platform dependency, today directory services control only few sections of the enterprise IT resources.

1.4.2 Two Factor Authentication (2FA)

2FA is an extra security layer that authenticates the user with one more factor over and above the usual password. Usually the second factor is a dynamic OTP (One-time Password) communicated with the customers (external users) over a different device they own and on a different channel, like OTPs sent over mobile for Internet Banking. For internal users, biometric is a norm used as second factor to operate sensitive critical applications.

1.4.3 Privileged Identity Module (PIM)

The IT personnel who maintain servers, network components, and software are given elevated permissions needed to manage and maintain the IT infrastructure. Called privileged identities, they are allowed unrestricted access to view and change data, alter configuration settings, and run programs. Business applications and computer services must also store and use privileged credentials to authenticate with databases, middleware, and other

applications when requesting sensitive information and computing resources.

Control on these administrative rights with Privilege Identity Management (PIM) tools is required. Through PIM, one can manage and monitor the actions of the privileged identities and enforce authentication policies including multifactor authentication and raise alerts in case of policy violations. PIM software auto-discovers and catalogues privileged accounts present on a wide range of systems and applications and then propagates password changes wherever the account is referenced in order to prevent account lockouts and service failures that can otherwise occur when manual processes deploy obsolete credentials.

1.4.4 Single Sign-on (SSO)

SSO allows user to login once with single-ID to access all applications and platforms. The user is authorised to access, and eliminates further prompts when they switch applications during a particular session. Single sign off allows logging out from all the systems with single log-out. However, logging off a particular application does not log them out of all applications they were accessing.

SSO is always treated as a convenience from user angle, however the main advantage of SSO is that when an employee leaves an organisation, it is easy to disable his/her access to all resources in one go, by removing his ID and thereby protecting all resources s/he was given access to.

1.5 Operations

Operating a security program requires the necessary tools to support change control, and track assets based on asset classification framework. An effective security operations program is underpinned by an IT Service Management.

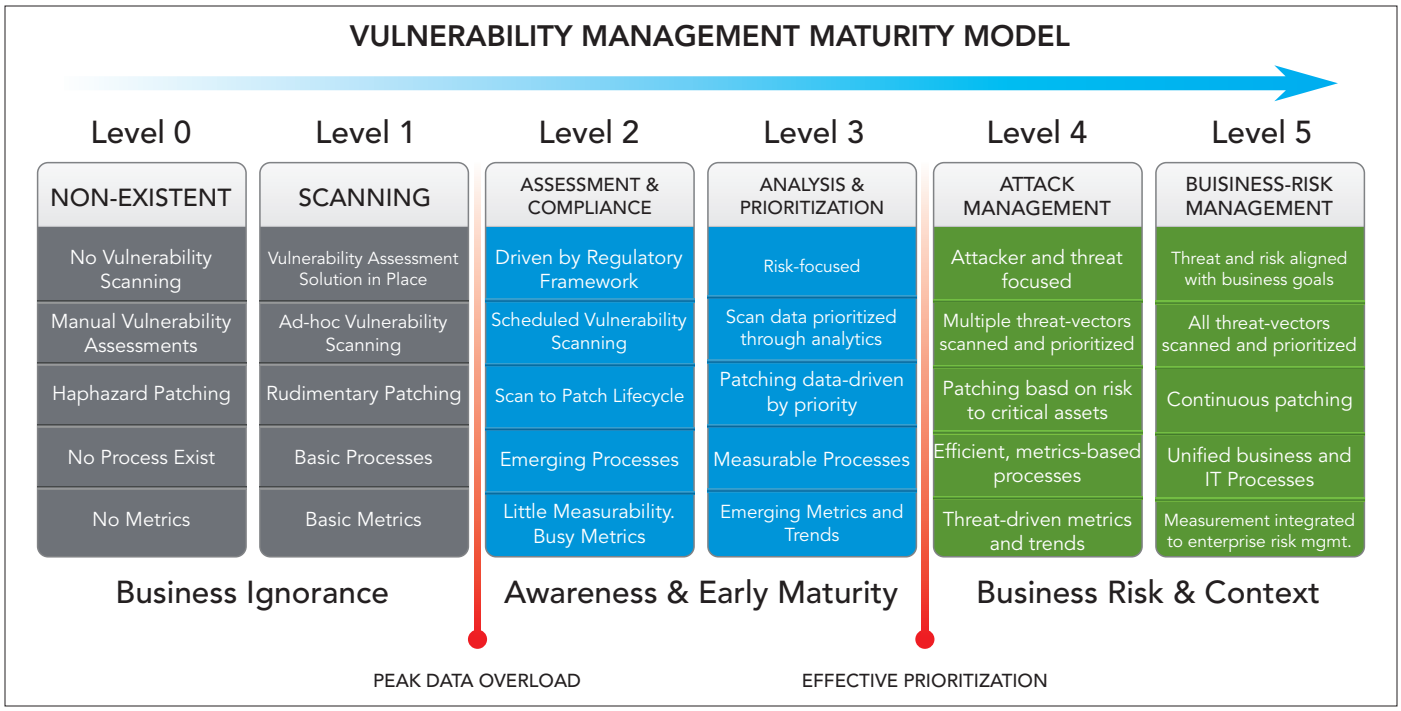
1.5.1 Service Asset Configuration and Management (SACM)

According to ITIL, SACM is the process responsible for ensuring that the assets required to deliver services are properly controlled, and that accurate and reliable information about those assets is available when and where it is needed. This information includes details of how the assets have been configured and the relationships between assets. The ITIL standard gives complete details about Service Asset Configuration and Management.

The ITSM (IT Service Management) tool to deploy ITIL best practices comes in as a central ITSM tool with various modules. The heart of this tool is a CMDB (Configuration Management Database), which holds the detailed information of all the assets, its inter-linkage, configurations, etc. This becomes an ideal source of any information about IT assets. All the other modules for ITSM will take the asset information from this central tool to correlate the information and provide meaningful intelligence. Modules like Service Desk, Change Management, Asset Management, Problem Management, Knowledge Management, CMDB, Vulnerability Management, Fault, Performance Availability and Incident Management should be integrated to take in data from one module, perform the function and pass on to the next module for automated escalations and management. Annexure 1.1 provides the maturity model for Asset Configuration and Management.

1.5.2 Vulnerability and Patch Management

It has become very common for vendors of hardware, software, network devices, security solutions, etc., to keep releasing patches to close the vulnerabilities. Not patching the systems leave the enterprise in a greater risk. Manual patching takes too long a time and leaves no audit trail of the whole exercise. Modern enterprises are automating the process of vulnerability and patch management through centralised tools.



Source: https://www.rsaconference.com/blogs/growing-up-a-roadmap-to-vulnerability-management-maturity

1.5.3 Security Incident and Event Management (SIEM)

SIEM is a tool that collects logs and events from various security infrastructure, systems and applications and stores it centrally. It also helps in normalizing the logs/events of different types from different nodes to a standard pattern. The collection and storing are done in a compressed form to save the network and storage resources. Once collected, these logs/events are analysed, correlated and meaningful intelligence is provided on a central console with various customizable dashboards for faster reaction and identification of root cause of the incident. More details on SIEM are available in the upcoming chapters.

1.5.4 Security Operations Center

Security Operations Center is a generic term describing a platform set up for the purpose of providing detection and timely reactive services to security incidents.

ISOC solution is an integrated deployment of advanced cyber security products/services, expert human resources and industry best practices and processes. ISOC implementation and operationalization plays crucial role in achieving the objective of providing in-depth centralized visibility into organization's IT infrastructure to monitor, detect, prevent and mitigate security incidents. Organisations need to focus more on rapid detection and response mechanisms, apart from technologies that prevent intrusions. Quick detection and remediation is possible only by automating the security operations. Such automation frees up analysts from mundane tasks and allows them to concentrate on higher priority risks affecting the most critical assets and data. ISOC automation capability is going to be a major distinguishing factor in assessing an ISOC product/technology.

An advanced implementation of Information Security Operations Center (ISOC) may have following additional components. Upon implementation of a basic version of ISOC, organisations may build these functionalities in their ISOC.

- **User and Entity Behaviour Analytics:** Attackers tend to compromise legitimate user accounts to access the target system. However, different users exhibit different pattern of activities. Analysis of user behaviour data helps to create a baseline of normal user and reports suspicious anomalous behaviour. This fact leads to differentiate a legitimate user from an intruder. Machine learning based techniques have successfully demonstrated detection of this kind of compromise. Recently, user behaviour analytics transformed to user and entity behaviour analytics for effective detection of various frauds including insider threat. Signature-less behaviour-based analytics is a new approach for detecting insider and targeted cyber threats.

- **Digital Forensic Capabilities:** Though this capability is mentioned as one of the basic functions of ISOC, very few organisations plan and implement this. As a future expansion, ISOC may develop forensic capabilities for identifying, preserving, recovering, analyzing, and presenting digital evidences to establish a digital crime. This capability of ISOC team will lead to a quick response to any adverse situation.

- **Big Data Analytics:** Storing and querying large amounts of data collected by ISOC also requires database technologies capable of handling such huge volumes and also which supports future scaling up. Relational databases to store and query data might not scale well and could pose a problem for organisations as information requirements continue to grow. Big Data platforms can store and process large amounts of data and would be the way forward for a futuristic ISOC, which requires contextual retrieval of large amounts of data. This should also be compatible with the traditional log management and SIEM tools.

  The future of ISOC lies in analysing data across all systems, instead of just glancing at logs, flows and packets. The future is the accuracy and speed of detection for security threats that can exceed the ability of attackers to hide in the noise.

- **Cyber Threat Hunting:** Cyber threat hunting, according to Wikipedia, is “the process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions.” This is in contrast to traditional threat management measures, such as firewalls, intrusion detection systems (IDS), and SIEM Systems, which typically involve an investigation after there has been a warning of a potential threat or an incident has occurred.

  Cyber hunting platform, which work in real-time and are network-based are available now. They empower the cyber hunter to identify zero-day threats by quickly deploying constant analytics at large scale. They use dynamic – on the wire – analysis. Being on the network allows the organisation to be proactive. They believe that packets do not lie. The malware author's “tricks” for obfuscation, cannot divert or mislead these platforms.

- **Deception Networks:** Unlike a honeypot – these are just a set of devices set up to appear like a real network to induce an adversary to attack – a deception network is all or part of the actual enterprise that is instrumented and protected such that the adversary is allowed to engage and the engagement is captured forensically but does no harm. The benefit is that the adversary does not know that s/he is being tracked and manipulated. They use “Deceptions Everywhere Technology" to neutralize targeted attacks and advanced persistent threats by creating a deceptive layer across the entire network. This provides an endless source of false information, disrupting and detecting advanced attacks with

real-time forensics and without disruption to business. Taking a very different approach to honeypot, this approach makes every endpoint part of the deception. The adversary must try everything because he does not know what is good and what is not.

Conclusion

This chapter glanced though the existing important security solutions that are essential in the present environment for any enterprise. The solutions explained here are not exhaustive but are indicative only. Enterprises need to place SOP (Standard Operating Procedures) for all these security solutions.

The following challenges remain despite rolling out majority of the security solutions:

- Security data overload – Too many devices, too much data
- Lack of event correlation across multi-vendor sevices – IDS, Firewalls, Anti-Virus, and Hosts
- Excessive false positives
- No timely and targeted reporting
- Minimizing risk against key assets
- Incident response mechanism.

References

- http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/white-paper-c11-736595.pdf
- https://www.rsaconference.com/writable/presentations/file_upload/sec-w04_final.pdf
- https://securosis.com/assets/library/reports/DLP-Whitepaper.pdf
- https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/technology/lu_dlp-data-lost-prevention-solution_02102014.pdf
- https://securosis.com/assets/library/reports/DAM-Whitepaper-final.pdf
- http://iasaglobal.org/itabok/capability-descriptions/access-and-identity-management/
- http://www.oregon.gov/DAS/EISPD/ITIP/docs/ArchCh6_AssetMgt_v1_0.doc pp. 3-5 (March 2004)
- Author cited by source: Patricia Adams of Gartner (Sep 10, 2003) in article: "Management Update: IT Asset Management Stages Form the Stairway to Success"
- Next-Generation Security Operations – Preview https://nigesecurityguy.wordpress.com/2016/09/26/next-generation-security-operations-preview/
- Is logging dead in the future of security threat detection? by Alex Taverner, December 2016, https://www.cio-asia.com/print-article/105558/
- Next-generation security monitoring and analytics by Peter Stephenson, December 14, 2016 https://www.scmagazine.com/next-generation-security-monitoring-and-analytics/article/577705/
- Next-Generation Security Operations – Preview by Nigel Willsonhttps://nigesecurityguy.wordpress.com/2016/09/26/next-generation-security-operations-preview/
- "Cyber threat hunting: How this vulnerability detection strategy gives analysts an edge - TechRepublic". TechRepublic. 2016-06-07

Chapter 2

ISOC Planning and Design

2.1 Why ISOC?

ENSURING Confidentiality, Integrity and Availability in today's modern IT-dependent enterprise is a mammoth task. Banks would require enterprise level visibility in order to comfortably provide assurance to business and customers on the security of their information and trustworthy engagement. There are several operational challenges, which need to be overcome, including:

- Enterprise level security posture through appropriate reports and dashboards
- Adhering to multiple legal and regulatory compliance requirements like RBI Cyber Security Guidelines, PCI DSS, ISO Security Standards, etc.
- Prioritization of incidents which need immediate attention and remediation
- Automating the patch management
- Identifying and detecting more sophisticated attacks such as blended threat, APT, etc., which could bypass the existing solutions.
- Real-time response and remediation
- Carrying out forensics analysis to track down the sequence of events that allowed the compromise.

The timely availability of this kind of visibility is of paramount importance, as it would determine the response strategy and reduction of impact because of security incidents. In order to have this visibility, the following are required:

- Robust policy backed by management commitments to define the requirements of security around business processes
- Security architecture with capability to provide contextual information about devices, users, network, location and applications
- Consolidation and centralization of all security contextual information to correlate and analyze for proactive alerting and intelligence
- People and resources to manage and operate a structured process oriented operations.

These can be done from a central place termed as CSOC - Cyber Security Operations Center. Further, the Reserve Bank of India, vide its notification dated 2nd June, 2016, has mentioned that "Banks should proactively initiate the process of setting up of and operationalising an Information Security Operations Center (ISOC) to monitor and manage cyber risks in real-time."

2.2 Definition of ISOC

The ISOC is responsible for monitoring, detecting, alerting, raising and responding to security incidents and the management of the organisation's security products. A SOC typically functions on a 24×7 basis in a week.

2.3 Securing Executive Support

Securing Executive Support is imperative for the success of a Security Operations Center. To gain executive support, a proposal may be placed before the top management with the following details:

- Need for a ISOC
- Regulatory and compliance requirements
- Short and long-term visions of ISOC aligning with organisation's Business and IT objectives
- People, Process, Technology and Governance required to achieve the objectives of ISOC
- Strategy for setting up the ISOC (In-house or outsourced)
- Budgetary requirements for ISOC
- Advantages of setting up a ISOC.

2.4 ISOC Framework

ISOC functions under the larger umbrella of Information Security Framework within an organisation, headed by a Chief Information Security Officer (CISO), directly reporting to the Head of Risk Management.

Based on the established Information Security framework, Security Operations Center needs to help in proactively monitoring and managing cyber risks in real-time.

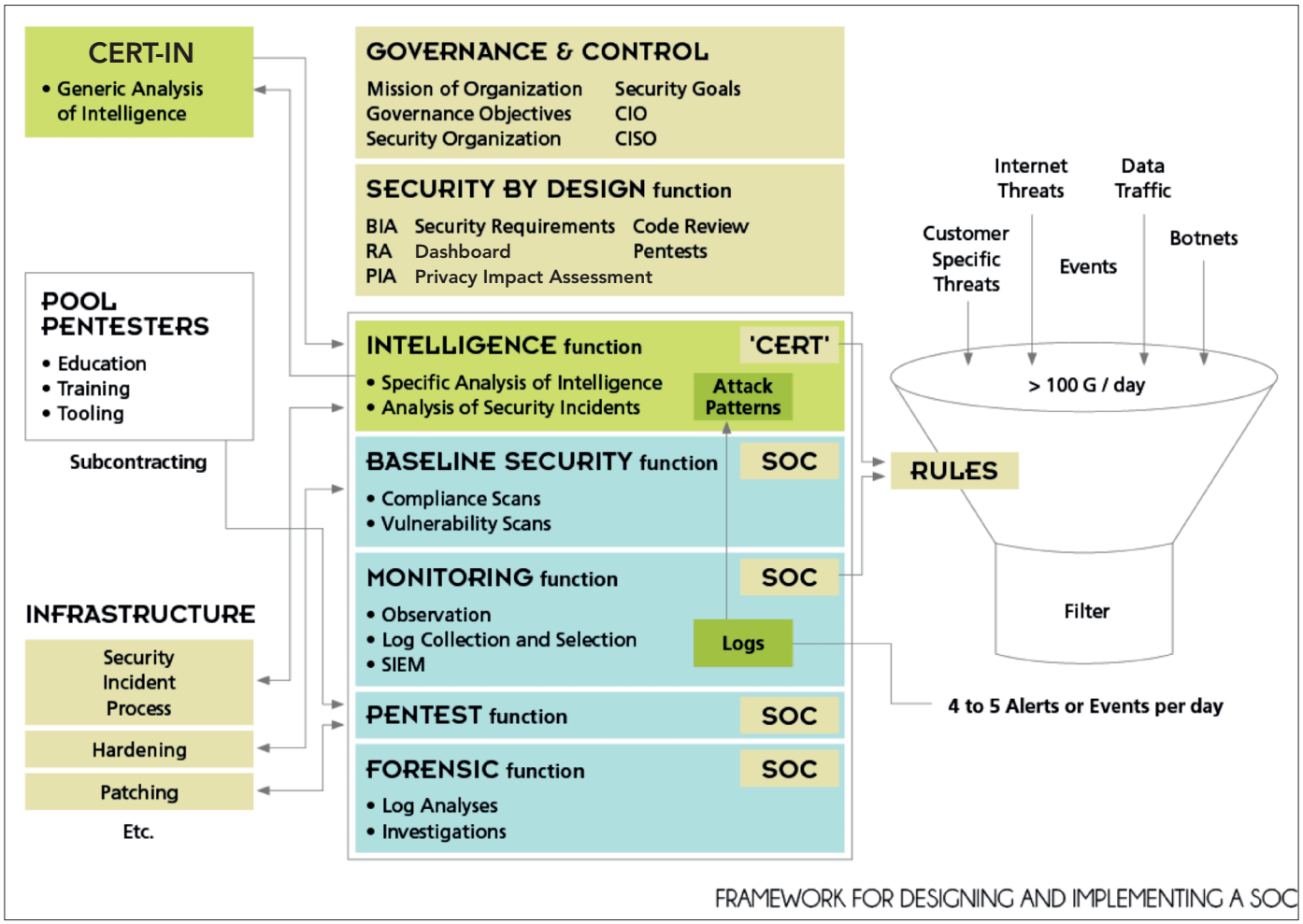
Based on such minimum baseline cyber security and resilience framework, Security Operations Center would help in proactively monitoring and managing cyber risks in real-time.

2.5 ISOC Functions

The major functions of ISOC may be classified into the following areas:

2.5.1 Intelligence Function

This is the core of the ISOC, equipped with the intelligent tools required for the processing and analysis of millions of events per second, and raising alerts in real-time. Competent and skilled resources of ISOC would analyse the threat patterns, refine and implement rules for alerts, coordinate with internal and external agencies and provide guidance to the operational staff for faster incident response.



FRAMEWORK FOR DESIGNING AND IMPLEMENTING A SOC

2.5.2 Monitoring Function

In order to identify anomalies and alerts in real-time, ISOC collects, monitors and stores large number of events per second, from security solutions like PIM, DAM, URL monitoring tool, phishing and brand abuse monitoring tool, etc., logs from end devices, servers, etc., and other parameters such as telemetric data (network flows and packet capture) and SNMP trap. Relevant alerts or events are identified by fine-tuning rules within the Security Information and Event Manager (SIEM).

2.5.3 Baseline Security Function

There could be some baseline security functions, such as conducting regular Vulnerability Assessment and Penetration Testing, hardening servers, carrying out compliance scans against security best practices, conducting Application Security and Code Reviews, Risk Analysis, etc. In certain cases, the ISOC team may also take up such activities.

2.5.4 Forensic Function

As security logs are being monitored and retained for a specific period as per the legal and regulatory requirements, any forensic analysis done would involve ISOC. The skilled analysts in SOC could help in the forensics investigation, in findings details and anomalies, collecting electronic evidences and ensuring the required details are provided to the forensic agency. In certain cases, the entire forensic analysis may also be taken up by the ISOC team.

2.6 ISOC Capabilities

The minimal capabilities an ISOC should have is indicated below:

Real-Time Analysis: Real-time Monitoring and Triage

Threat Intelligence: Cyber Threat Intel Collection, Distribution and Analysis, Threat Assessment

ISOC Tool Life-Cycle Support: ISOC Infrastructure O&M, Rules Tuning and Maintenance, Custom Signature Creation

Incident Response: Incident Response Management

Scanning and Assessment: Vulnerability Assessment, Penetration Testing.

"Ten Strategies of Word-class Cybersecurity Operations Center" by Zimmerman, C., could be handy to choose additional ISOC capabilities, as per the size of the organisation and requirement.

2.7 Planning and Designing ISOC

Planning

Creating a plan for various phases of implementation is critical to the success of a Security Operations Center. It is imperative to capture details required for decision-making, including the organisation's vision and objectives, environment, threat landscape, budget, etc. Also required is the management and other stakeholders' support in setting up ISOC for necessary budget, resource sanctions, integration of systems with ISOC, etc. This support needs to be developed during the planning phase.

2.7.1 Define Business and IT Objectives

Security management requirements may vary with organisations and hence should align with the organisation's Business and IT objectives to enable them to achieve their goals by reducing security risks. COBIT model shall help in defining and aligning the business and IT objectives. Strategy for ISOC deployment should be derived out of these defined objectives.

2.7.2 ISOC Mission Statement

The ISOC monitors the security posture of networks, systems and applications operated by IT, with the objective of detecting and reacting to Information security incidents that could negatively impact the organisation's business operations.

2.7.3 ISOC Scope Statement

The ISOC Scope Statement helps an organisation to focus on what tasks the SOC should perform. It may cover the following:

- Monitoring of all systems managed and operated by IT
- Detecting and responding to security threats and malicious activities
- Leading the Computer Security Incidents Response team
- Conducting awareness sessions when required .

2.7.4 Gather Information

Information collected during the planning phase is instrumental in giving the final shape of ISOC. Based on these collected data, the strategy for implementation, deployment and even the expenditure would be derived. Collecting accurate and complete information during this stage is necessary.

2.7.4.1 IT Environment

IT environment in an organisation is a major deciding factor, in choosing the ISOC Technologies and Architecture. Collect details on overall IT Architecture, IT Infrastructure, in-house or outsourced operations, technologies in use, virtualization, use of cloud based services, etc. The technologies implemented in ISOC should be compatible with the existing IT established in the organisation, as the goal is to monitor and manage security risks with respect to these very systems. Details on number of each type of assets (hardware/software), data size, log size, bandwidth utilization, transaction related parameters, number of users, etc. would be required to size hardware and software procurement and would also influence the licensing model adopted. Future IT Plan and strategy regarding adoption of new technology should also be captured during the data collection phase, in order to accommodate them in ISOC planning.

2.7.4.2 Threat Landscape

Threat landscape for every organisation varies, based on the type of business, location of business, type of technologies employed, standards and procedures adopted for business, etc. Common threats include DDoS, Phishing, Spamming, Malware, Backdoor, Privilege Escalation, Advanced Persistent Threat, Man-in-the-Middle attacks, Website Defacing, etc. Threat landscape keeps evolving at a fast pace. Understanding of evolving threats in other organisations and other parts of the world is necessary in order to plan, keeping in view the future threat vectors.

It would be a good idea to understand the past security incidents within an organisation and ensure that the ISOC meets the requirement to mitigate such incidents. The type of technologies to be adopted and services to be subscribed, would depend on the current and evolving threat landscape.

2.7.4.3 Regulatory and Compliance Requirement

The RBI in its notification regarding Cyber Security Framework in Banks, dated June 2, 2016 has mentioned the need for arrangement of continuous surveillance.

Regulatory and compliance requirements of the country on Information Security and Cyber Security need to be identified, in order to accommodate them in the scope of ISOC.

2.7.5 Measure the Maturity

A good practice is to carry out Gap Analysis (Security Maturity) before and after deploying ISOC, with respect to IT Security Technologies, Processes, Organisations, Metrics and Governance. Gap analysis process will help in identifying and evaluating potential opportunities to strengthen and improve overall security posture and to achieve higher security maturity level. The logical security architecture as explained in first chapter can help the organisation to judge its maturity level.

2.7.6 Budget for ISOC

Budget allocated by the organisation for Information Security would decide the strategy and scope of ISOC. Depending on provision of Capex/Opex budget, organisation would need to decide whether deployment strategy would be in-house or outsourced ISOC, the technologies to be deployed and the licensing methodologies.

The gap analysis done and detailed study conducted on the cost of various models of implementation would assist an organisation in deciding the budget to be allocated (Capex-intensive in-house model or perpetual licensing model vs. Opex-intensive outsourced model or consumption license model vs. hybrid model).

Organisation can also explore newer technologies like virtualization and cloud based services wherever possible, which could bring down the total expenditure requirement. Annex 2.4 provides template for ISOC Budget.

2.7.7 Formulate ISOC Strategy

Selecting the optimal ISOC strategy depends on the Business and IT requirements, threat landscape, regulatory requirements and financial constraints. The ISOC strategy should be arrived at based on roles and responsibilities, various stakeholders, the model of operation (own, outsourced), processes and resources required, priorities with respect to operation. A roadmap may be accordingly developed.

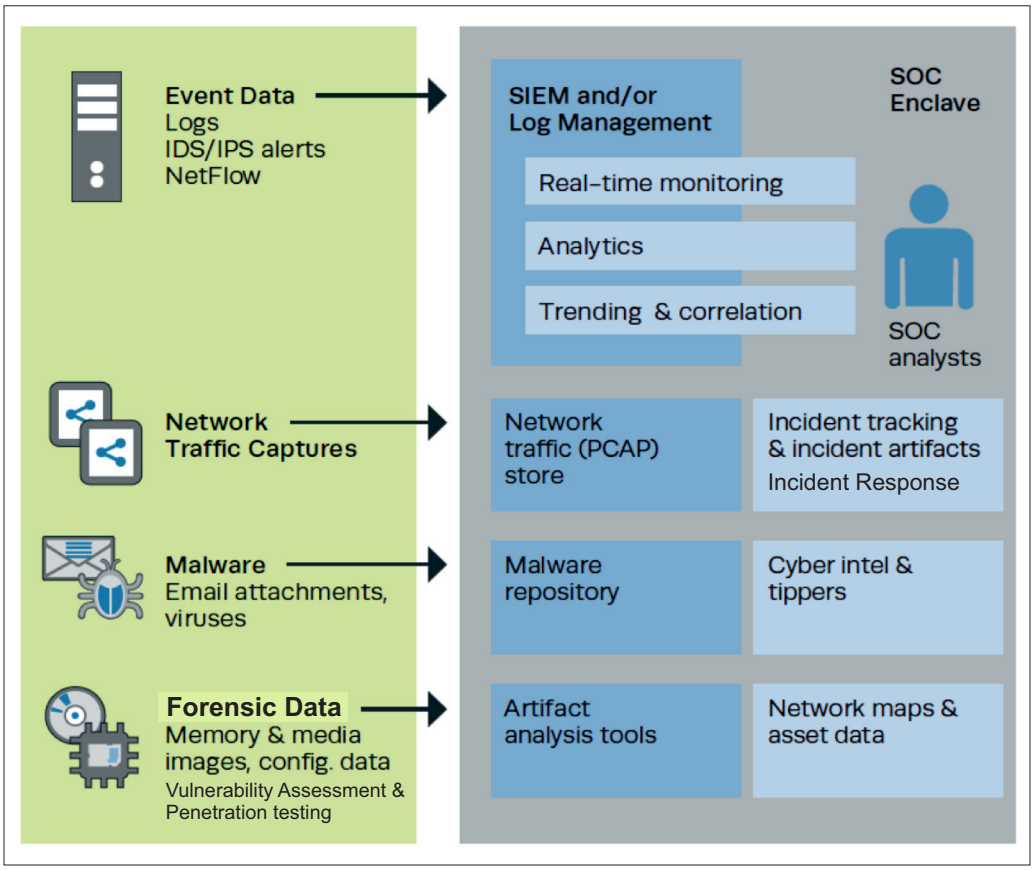
2.7.8 Identify the ISOC Technologies

The ISOC is a combination of technologies put together with seamless integration, in order to achieve a faster incident detection and response.

- Security information and event management (SIEM) tools are the core technical components of ISOC. SIEM technology supports threat detection and security incident response through real-time collection and historical analysis of security events from a wide variety of event and contextual data sources.
- It also supports compliance reporting and incident investigation through analysis of historical data from these sources. The main capabilities include event and log collection and management, data aggregation, normalization, correlation, analysis, reporting, alerting and dashboard facilities.
- Network monitoring tools provide insight into the state of the network within an organisation. Often referred to as Network Analysis and Visibility (NAV)/NBAD, these tools monitor critical network characteristics for a possible presence of threat in real time and alert/trigger the response mechanism.
- Situational awareness is an important component in ISOC, which aims to achieve a thorough understanding of attack vectors and the knowledge of what process/systems/people have access to which valuable information within an organisation. In order to counter the emerging threats, self-learning, predictive analysis and risk based decision systems are also being implemented as part of situational awareness.

2.7.9 Understand the ISOC Tool Architecture

ISOC Tool comprises of Log Analyser, Network Analyser, Malware Analysers and Forensic Analysers with incident response mechanism taking input from all these analysers. For carrying the process of security analysis, auditing, and compliance, data from various sources like event logs, network packets, network flows, etc., and in different formats need to be collected.



Typical SOC Tool Architecture

2.7.9.1 Log Collection

The following information will assist in acquiring relevant data and to perform useful analysis:

- Systems/ elements need to be monitored
- Data format
- Level of logging
- Protocols used to collect data from the various systems
- Log storage and retention period
- System and network overhead caused by data collection
- Capacity management in accordance with the data collection
- Optimize data collection capability.

The type of data to be collected and logging mechanisms/protocols supported by end devices, determine the collection mechanism for deployment. Majority of the systems and devices natively support the 'Syslog protocol' for event logging. In case of few non-Unix systems, one may need to install an agent. The Annex 2.4 provides recommendations on logging. They also help decide the logging model to be adopted: centralized, distributed, or semi-centralized.

2.7.9.2 Telemetry Data – Network Flows

To monitor network from a security perspective, capturing and transferring network packets is not always feasible. The storage costs of the data captured, lack of skillsets required to analyse the data and hardware costs of these data collection tools discourage capturing such data, especially in

case of multiple locations connected over a wide-area network (WAN). Collection of network flows, which gives contextual information about network connections, is much more feasible than capturing full packets.

The system's overall performance is dependent on capturing, maintaining, and exporting network flow information. Working through a capacity-planning exercise and consulting with network vendor on the impact of enabling the feature is the best practice.

Similar to syslog, one can implement a centralized, distributed, or semi-centralized model for collecting network flows.

2.7.9.3 Telemetry Data – Packet Capture

There are cases in which one need to go beyond collecting logs and network flows. Security point solutions like Intrusion Detection System (IDS), Deep Packet Inspection (DPI) and Forensic Analysis, etc., need network traffic containing actual data (payload) to be captured and forwarded. One may consider the following two techniques to capture network packets, in the case of Ethernet:

Port Mirroring: Network switches can be configured to mirror traffic seen on ports or VLANs to other local or remote ports. The network throughput of the source and destination ports needs to be considered while doing a port mirroring.

Network Taps: Connecting network taps (out-of-band devices) is another approach to monitor and capture packets from point-to-point links. Connecting taps to all network lines may not be feasible. Taps can be connected to the most important locations in the network, such as Internet Gateways and Data Centers. In larger complex organization, network taps may be implemented for packet capture, to reduce the overhead on the business network.

2.7.9.4 Parsing and Normalization

Data that has been collected must be first parsed and normalized for further analysis. Raw input data is processed and meaningful data from raw logs is extracted through the process of parsing. With normalization, similar extracted events from multiple sources are uniformly stored or consumed by subsequent processing steps.

2.7.9.5 Security Analysis

Security analysis involves researching collected data in order to uncover potential threats. This could vary from performing a basic incident mapping to advanced mathematical modelling, to discover known or unknown threats and to understand threat patterns.

Security event correlation is being offered by many SIEM Solutions as one of their core components. This involves identifying relationships between disparate events from various sources and collating and analysing these, to detect and report threats.

The correlation engine of SIEM has rules, which require regular updates. The default rules can be fine-tuned and custom rules created, based on the organizational environment, business requirements and the use cases identified. Out-of-box rules could include alerting excessive failed login attempts, malware detection, unauthorised outbound connection, DoS attacks, etc.

2.7.9.6 Data Enrichment

Adding additional context to the data collected is known as data enrichment. Data enrichment helps in making more informed decisions, thus improving the accuracy of threat-detection processes and tools. Following are few example of data enrichment:

- Geo information, mapping IP addresses to geographical locations
- WHOIS information, providing additional contextual information on IP addresses
- Reputation information on IP addresses, domain names, file hash values, e-mail senders, etc.
- Domain age information.

2.7.9.7 Storage Technology

During the planning phase, it is necessary to choose the right Storage Technology as well as do the sizing for storage, such that retrieval of data is faster and without impacting the performance of the system.

Network behavior data with or without packet is normally kept on online storage for very short duration, whereas event related data can be stored for longer periods like six months or more. Storage sizing and type should meet legal, compliance, organizational and performance related requirements with some buffer as well as scaling up options. The kind of online and archival storage (SAN, NAS or Device Attached Storage) may be OEM/ISOC solution specific.

2.7.9.8 Threat Intelligence

Threat intelligence or cyber threat intelligence (CTI) is organised, analysed and refined information about potential or current attacks that threaten an organisation. The primary purpose of threat intelligence is helping organisations understand the risks of the most common and severe external threats, such as zero-day threats, advanced persistent threats (APTs) and exploits. There are various service providers providing real-time global threat intelligence using feeds, e-mails, reports, etc. Annex. 2.3 provides information about information exchange on threat intelligence.

2.7.9.9 Compliance

For any successful security operation, it is necessary to have the compliance of systems monitored against the security best practices, regulatory requirements (RBI and various relevant Government Agencies), a global security standard like PCI DSS or maybe even a configuration template. Regular monitoring can help have a visibility into the changes in the system and existing configuration problems that could lead to a security breach. Automating the system compliance process and then linking it to risk management and incident response practices are key steps in any successful security operation.

2.7.9.10 Ticketing and Case Management

Any security incident or potential incidents reported by tools or by people need to be tracked until closure, to ensure that the incident is properly managed. For proper incident management, a ticketing system could be used, which would help in creating, assigning and tracking an incident. This activity should be supported with the right tools, authority, and integration with incident response and case management processes.

SIEM, vulnerability management, and other ISOC tools should either support built-in incident management modules or should have the facility to integrate with organisation's existing IT ticketing system, for central management and reporting of incident tickets.

2.7.10 Collaboration

The ISOC should have a strong collaborative system with IT and Business, which allows the ISOC team to centrally store, manage, and access documents, including system manuals, documented processes, incident response procedures, and so on.

2.7.11 ISOC Sizing

The sizing for ISOC should be planned based on the various parameters mentioned in the log collection section. The ISOC sizing would depend on the number of servers, applications, Events per Seconds (EPS) and Flows per Second (FPS) generated by the systems, type of system, etc. A sample sizing data sheet and a template has been provided at Annex 2.5 for reference.

2.7.12 Understand Deployment Models

Once the data collection steps like – deciding the data sources, calculating EPS, etc., have been completed– one has to decide, how the ISOC would be deployed. The major component of ISOC is SIEM. SIEM in turn consists of three major components called Event Collector, Event Processor and Event Correlation Analyser. (Terminology could vary between various

products). Collectors collect events from Syslog UDP, Syslog TCP, JDBC, Log File protocol, etc. Event Processors filter the events based on parsers and some rule sets. Event Analysers perform analysis on the events filtered by event processors and provide a dash board to the ISOC users. ISOC deployment models basically vary on how these three elements are best placed.

2.7.12.1 Centralised

In a centralised model, all the three components are placed at a central location. This deployment model is very simple and suits very small organisations, wherein the number of systems and events are very low. For larger organisation, this model would not be suitable, as shipping the event data to central location without filtering may exhaust the bandwidth on WAN links.

2.7.12.2 Distributed Processor and Central Analyser

In this model, the collectors and processors could be distributed. Each processor filters the events collected by a group of collectors and then hands them to analyser. This model suits larger organisation, wherein only the processed data is handed over to the central analyser, reducing the bandwidth requirement over the WAN, considerably.

2.7.13 Understand the ISOC Licensing Models

ISOC components are basically licensed depending on the number of EPS generated, number of data collectors and data processors deployed. During the data collection phase, the EPS estimation exercise needs to be done, which would help in deciding actual deployment model that in turn decides the licensing model. The specific products purchased should support scalability and also upgradation, based on the changing environment.

2.7.14 Understand Processes

Identify the core responsibilities and processes in an ISOC. There would be various day-to-day security tasks like patch management, server hardening, anti-virus signature update, fixing vulnerabilities, monitoring availability, etc., which needs to be handled by the IT Operations. Other monitoring tasks such as detecting a DoS attack, remote code execution attacks, SQL injection, unauthorised login attempt, etc., should be handled by ISOC.

It is important to identify the core responsibilities of the SOC and the IT operations center. Based on the identified responsibilities for each, come to an agreement on how responsibilities are to be divided between the two.

2.7.15 Understand the level and depth of automation

The ISOC's job is to monitor and help respective team to remediate the threats across entire IT infrastructure as quickly as possible. To achieve this, it is necessary to integrate and automate functions and processes of ISOC. More the automation, faster would be the detection and mitigation capabilities, with minimal human resources. However, automating monitoring and remediating could be a costly process. Identify the core tasks and processes which needs to be automated.

2.7.16 ISOC Operating Models

Most organisations face the dilemma of whether to outsource the ISOC or have it built in-house. Organizations have varied business models, risk profiles, technology implemented and compliance and regulatory requirements to satisfy, with which ISOC must align. Based on these factors, the ISOC deployment methodology may be arrived at. The common ISOC Operating Models are:

2.7.16.1 In-house Captive ISOC

Captive or In-house ISOC is generally deployed by organisations who want to avoid outsourcing of ISOC, due to various reasons like risks of critical security data loss, misuse of security logs and analysis, policy and regulatory requirements, etc. The organisation can leverage on its own dedicated resources who

understand the environment and enable efficient correlations among different working groups. This also allows for customization as per organization's needs. The challenges include, high Capex investment, requirement of in-house skilled resources on long term, time to realize ROI and time and effort to setup infrastructure.

One method to implement in-house Captive ISOC is Build, Operate and Transfer Model (BOT). Organisations adopt this model with a vision to fully own and operate the ISOC at a later period, however wanting to leverage the expertise of a service provider in setting up and in attaining a faster maturity level, thus mitigating risks in the start-up stage. BOT, as a hybrid model, combines elements of the captive centre and outsourcing.

During the Build-phase, the service provider sets up the infrastructure and provides resources required for the activity. In the Operate-phase, the provider manages the ISOC providing security services and also personnel required for the same. During the Transfer-phase, the provider initiates activities like trainings, knowledge transfers, etc. to the in-house team.

2.7.16.2 Outsourced or MSSP Model

Organisations going for managed security operations can leverage on the service provider's already existing infrastructure and skilled resource pool. Immediate benefits of ISOC implementation is visible to the management. In addition, service providers, due to their various engagements with other organisations, can bring in the knowledge base, learnings, and best practices with respect to security incident and event handling and threat intelligence. The ability to scale up would be faster when compared to captive ISOC. Risks include loss / misuse of critical security data, sharing organisation's vulnerability details with third party, misuse of data after end of contract, etc. It is necessary to choose trusted partners based on their reputation, reference customers, level of security and experience of staff. Stringent contracts, NDA and SLA need to be in place with the service providers to address the risks involved.

2.7.16.3 Hybrid ISOC

This model is a hybrid of in-house and outsourced methods, wherein the organisation can leverage the best of both the worlds. The security logs may be maintained in-house and the analytics, specialized services and threat intelligence may be provided by the service providers. This provides organisations flexibility to develop expertise in specific areas, flexible deputation of organisation's resources, utilize expertise and infrastructure of the service provider for advanced analytics, scale up in times of need and also meet stringent regulatory requirements regarding security logs. Risks include loss/misuse of security data, which would need to be addressed by choosing trusted partners and having in place NDA, contracts and SLA with the service provider.

While choosing the model, organisations have to keep in mind the regulatory recommendations also.

2.7.17 Manpower Requirements

The ISOC requires workforce can be divided into five categories:

Leadership Roles: The responsibility of the official would be to lead the ISOC team to achieve the mission of the ISOC.

Analyst Roles: Responsibilities include security event monitoring, incident report investigation, incident handling, threat intelligence, vulnerability intelligence and reporting.

Engineering Roles: Engineers with specific in-depth knowledge about tools and technology on top of which ISOC is built, is required for expanding the ISOC functions and to handle and resolve any ISOC specific issues.

Operations Roles: While ISOC engineers focus on

expanding scope of coverage in terms of both ISOC functions and the devices to be monitored, operators basically concentrate on the upkeep of the current ISOC setup.

Other Support Roles: Other support roles like BCP and DRP support, compliance and audit support, incident and problem managers, process/procedure developers, training specialists, communication specialists, vendor and contract management support may be made part of ISOC, depending on the IT and Security Structure within an organisation.

Based on the data collected during the data collection phase, regarding scope of ISOC, number of servers, type of incidents, number of applications, type of systems, etc., a resource sizing activity for ISOC may be carried out.

Conclusion

This chapter highlighted all the measures, technologies, people, processes, etc. to be employed for planning and designing of ISOC before going in for actual implementation.

References

- Zimmerman, C., Ten Strategies of Word-class Cybersecurity Operations Center, Mitre corporation, 2014.
- A Design Model for a Security Operations Centre (SOC) https://www.deitauditor.nl/informatie beveiliging/a-design-model-for-a-security-operations-centre-soc/
- A Successful SOC Builds on the Basics, http://www.ey.com/Publication/vwLUAssets/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime/$FILE/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime.pdf
- SOC 2.0 Protecting Your Information Assets From Next Generation of Threats, http://www.dts-solution.com/wp-content/uploads/2014/04/Security-Operations-Center-v2.pdf
- Overview of Security Operations Center Technologies, http://www.ciscopress.com/articles/ article.asp?p=2455014
- Rishikesh Kamat, Security Operations Center To Build Or Outsource?, http://www.netmagicsolutions.com/data/article/Security Operations Center - Inhouse vs17-01-241485253065.pdf

Chapter 3

ISOC Integration and Implementation

EVENT generators, event collectors, message database, analysis engines and reaction management software are the five distinct modules of any typical ISOC. Built as autonomous parts, usually integrating all these modules keeping the integrity, security and availability of their data, is a major task.

The data gathered from log and event sources prior to and during the incident, helps ISOC analysts to use it as an investigative tool, look for suspicious activities that make up the present incident, and to manage the response to an incident or breach.

The incorporation of Threat intelligence, Asset, Identity and other context information aids the ISOC analyst's investigative process. Often, an alert is associated with network or host-based activity and, initially, may contain only the suspicious endpoint's IP address. Incorporating asset and identity information provides a huge advantage in time and effort to prioritize the security incident - higher-value business assets should be prioritized over lower-value assets.

3.1 Understand the Environment

The ISOC team must have the appropriate tools, processes, documents, diagrams and knowledge to plan, deploy, operationalize and manage ISOC in close coordination with each IT infrastructure and application team. It is important to have copies of the key network and application architecture diagrams. As a part of the ISOC's service functions, the security architecture will be defined and the ISOC team will have access to different components and tools within that architecture. These may include, but are not limited to:

- SIEM monitoring and correlation
- Antivirus monitoring and logging
- Network and host IDS/IPS monitoring and logging
- Network and host DLP monitoring and logging
- Centralized logging platforms (syslog, etc.)
- Email and spam gateway and filtering
- Web gateway and filtering
- Threat monitoring and intelligence
- Firewall monitoring and management
- Application whitelisting or file integrity monitoring
- Vulnerability assessment and monitoring.

3.2 High Level Execution Plan

Equipped with the details of IT environment, chalk out a high-level plan on how to integrate the critical assets with ISOC. The plan may include the following steps.

- Deciding core functions and core capabilities
- Phase-wise integration based on functions
- Phase-wise integration based on criticality of assets
- Phase-wise integration based on geographical coverage .

3.2.1 Deciding Core Functions and Capabilities

ISOC is made up of five core functions viz. Log analysis, Vulnerability Analysis, Network Behaviour Analysis, Malware Analysis and Forensic Analysis. Keeping these five functions at the core, the other layers like ticket management, incident response, risk management, governance, etc., are built around.

List down the prerequisites for implementing each of these functions. Asset Discovery is an important prerequisite for a majority of the ISOC functions, without which it would be difficult to identify and

attribute the logs from each asset. Start with basic ISOC functions like log analysis and vulnerability analysis. One needs to choose the capabilities that can be built based on the functions chosen.

3.2.2. Phase-wise Integration Based on Core Functions

It is suggested to go in for a phase-wise implementation as indicated below along with ticket management, incident response and risk management:

- Phase 1
  - Log Analysis – SIEM
  - Vulnerability Analysis
- Phase 2
  - DAM – Database Activity Monitoring
  - NBAD – Network Behaviour Anomaly Detection
- Phase 3
  - Malware Analysis – Advanced Persistent Threat Protection
- Phase 4
  - Forensic Analysis.

3.2.3 Phase-wise Integration Based on Criticality of Assets

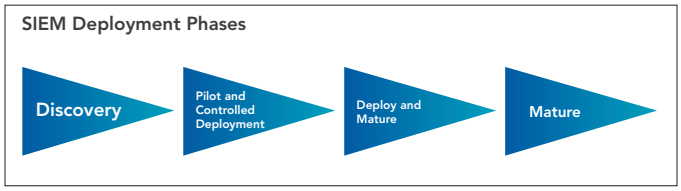
Integrating all assets with ISOC is a huge and time-consuming process. A plan needs to be in place to include all assets over a period of time. Initially, go with critical assets (Crown Jewels) that cover 90% of the business.

- Critical Security Point Solutions like Firewall, IPS, DAM, PIM, Anti-DDOS, etc located in DC/DR
- Critical application servers / equipments located in DC/DR
- Critical network equipments.

3.2.4 Phase-wise Integration Based on Geographical Coverage

Organisations' critical assets may be spread across a wide geographical area. Apart from DC and DR, certain business offices may also be critical. Integrate the assets of DC, DR, Central Offices, Regional offices, branches, etc., in a phase-wise approach.

3.3 ISOC Deployment



3.3.1 Discovery Phase – Laying the Groundwork

- Review the organisational security posture and the initial business case for a SIEM. Then prioritize the goals of the SIEM implementation from the most critical to the optional -taking into account the tasks that must be performed in order to support the effort
- Review in detail the organizational security policy and separate those policies from a priority standpoint. Determine what is critical, what's necessary for mandatory compliance and what policies are best practices to ensure a secure environment
- Identify current controls that are auditing those policies to determine compliance level
- Identify a smaller representative subset of the current policy and devices, where SIEM can be applied and enough data can be gathered.

3.3.2 Pilot Phase – Beginning the Implementation

The primary goal of this phase is to determine which specific SIEM project goals can be implemented in order to establish initial ROI while creating a baseline operational model:

- The lessons learned from the discovery phase are used to implement a larger subset of technology
- The assumptions developed during the discovery phase are tested in real-time
- The list of devices should be expanded to incorporate a wider set of technologies and numbers
- The information developed from this phase is used to determine the final steps of controlled deployment and maturity phase.

3.3.3 Controlled Deployment Phase – Capacity Building

The primary goal of this phase is to develop a deployment workflow that enables the organisation to build capacity as full deployment approaches. This phase also serves as the initial production test run and the completion of operational processes and procedures necessary to manage a full deployment.

3.3.4 Maturity Phase – Continuing to Evolve

Significant work must be performed in order to mature the organisation's security posture and implement the finer points of deployment. This phase never has an end since SIEM must continually evolve.

3.4 Asset Inventory

There should be a centralised asset inventory of the entire IT infrastructure and applications consisting of targeted systems/devices/applications/networks. The next step will be integration of log sources with the ISOC for situational awareness and in-depth visibility of the organisational IT setup. Classification of the assets on the basis of criticality is must and will be linked to the severity of incidents, its response and mitigation measures. Indicative asset collection template is in Annex. 3- A.

3.5 Time-Stamp

Logs must be time-stamped to trace back the events and correlate findings. The best practice to ensure that all systems are in the same time schedule is to use a time-stamp server (NTP).

3.6 Event Generation, Collection and Storage

Once the targeted systems are identified and inventoried, the next step is to collect the events through logs. The Event Generation should be set-up to generate as much raw information as possible. This information can be sent in "real-time" to collectors and/or can be stored locally for future collection.

Identify and place the log collectors in appropriate locations like DMZ, internal network, critical server segments, etc. The deployment and number of sensors/collectors for perimeter and internal components will be dependent upon the network architecture and the types of cyber security solutions deployed by the organization. The sensors/collectors will in turn forward the logs gathered to central processor/correlation engine for further processing and storage. The Log Analysis and Correlation engine will then apply the use cases to the data it receives to provide the required alerting and reporting actions by the SIEM.

3.6.1 Integration of Log Sources

The integration of log sources with the Collector/Sensor of the SIEM data may be carried out on the basis of the filtering and logging level as per suggestions given in Annex 2.

- **Initial Implementation:** It is a good practice to start with UAT or Test systems, observe the performance and then start with less critical log sources. The process of integration of log sources is mostly non-disruptive except for few systems where agent has to be installed for detailed log capture.

- **Connectors/Parsers:** Most of the standard SIEM solution will provide out-of-box connectors/parsers to integrate the IT infrastructure with SIEM. As a part of RFP or initial planning, the organization needs to get compliance matrix from System Integrator/OEM implementing the project. The compliance matrix will indicate compatibility of their SIEM solution vis-à-vis different flavors and versions of IT infrastructure (OS, DB, Middleware, Network and Security components, NOC solution tools, Ticketing, LDAP, etc.) and different applications/solutions deployed in the organization. In few cases, there may be requirement for customization and/or development of connectors and same has to be factored in the scope of work in RFP. It will be an on-going activity as more and more systems/devices/applications are added.
- **Integration and Scaling:** The indicative integration of systems/devices is provided in mentioned in Annex 3-B. Clear cut scope of work, customization/development of connectors/parsers, scope of scaling up the SIEM solution, need for new connector/parser, etc. has to be beforehand finalised.

3.6.2 Collection and Storage

The main operations performed by collectors are the reception of raw logs/events through different protocols and from varied source types and identification and parsing. Once a message is parsed, it is stored for a long term compliance purpose and for real-time alerting and reporting. Performances and availability requirements naturally influence the design of a scalable architecture.

3.7 Data Analysis

ISOC gives structural and behavior-led alerts. The main operations performed that generate alerts/incidents using well-defined use cases are the following:

- **Correlation –** A stand-alone operation used to detect an intrusion attempt by creating the contexts from captured data and matching them with specific intrusion characteristics.
- **Structural Analysis –** This is a kind of advanced pattern matching process, used to determine whether events of a certain context lead to a known intrusion path.
- **Intrusion Path Analysis –** This provides information about the exposure of the target system to the intrusion attempt detected.
- **Behaviour Analysis –** By taking information from the security policy and asset database this step determines whether the intrusion attempt is allowed or not. The idea here is to generate alerts by taking care of the security policy defined, as well as criticality of the target systems.

3.8 Developing Use Cases

Use Cases, the heart of any ISOC, is used to determine if any event is an incident or not. To ensure that the ISOC as cyber security system for monitoring, detection, prevention and mitigation is effective, a series of use cases must be defined. A use case may include the involvement of a Rule, Alarm, Mail alert or even a Dashboard. Use cases may be developed to meet the organisation's security policy requirements and detect policy violations.

A good way to start developing the use cases can be as mentioned below:

3.8.1 Attack based Use Case Model

Look at cyber security incidents that the organisation has experienced over the past few years. Identify anatomy of attack and model threat indicators for monitoring in SIEM to generate alert and help team to take mitigation steps. Examples of attack based use cases are SMTP from unauthorized host, failure of anti-virus to clean malware, excess inbound or outbound flow, etc.

3.8.2 Business based Use Case Model

Understand business process and linkage to IT Security and monitor logs for compliance violation. Use cases should be built to detect non-compliance of legal and regulatory requirements, taking cues from recent audit findings. Examples include use cases for PCI DSS compliance, etc.

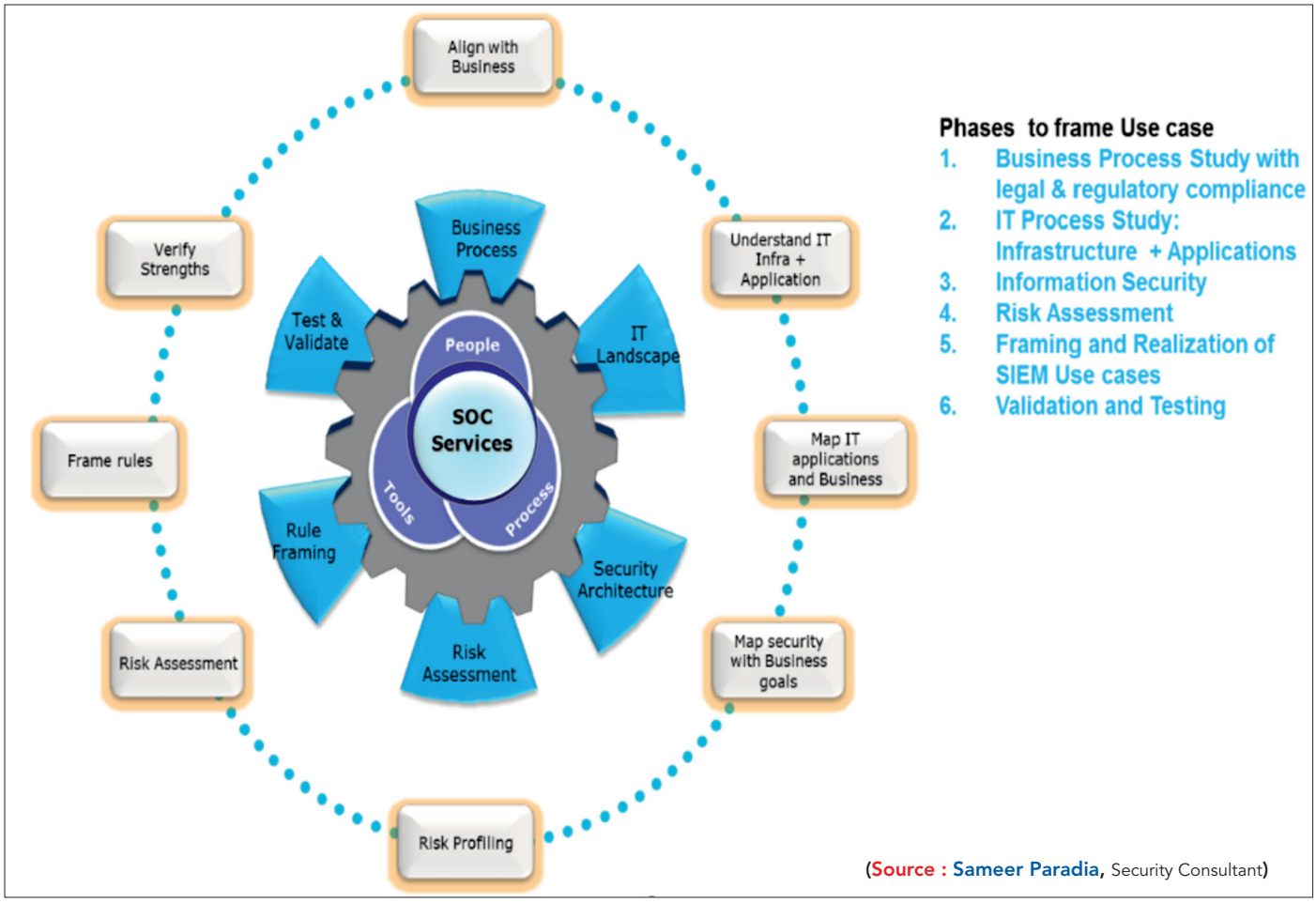
3.8.3 Asset based Use Case Model

Look at the organisational IT infrastructure set-up. Identify OS, Application, DNS, Web Server etc., and based on their threat exposures, the organisation can monitor logs and correlate events to generate required security alert. Examples of asset-based use cases include password cracking of OS, DDoS on Web servers, malicious probe on Firewall, etc.

3.8.4 Lifecycle Phases of ISOC Use Cases

Even though out-of-box use cases will be available, organization need to study and develop Use Cases to meet its cyber security requirements, which are highly contextual. Organisations can apply the Lifecycle Framework for development of use cases as depicted below:

A few examples of attack scenario is in Annex. 3-D and an example of a Use Case is in Annex.3-E.



(Source : Sameer Paradia, Security Consultant)

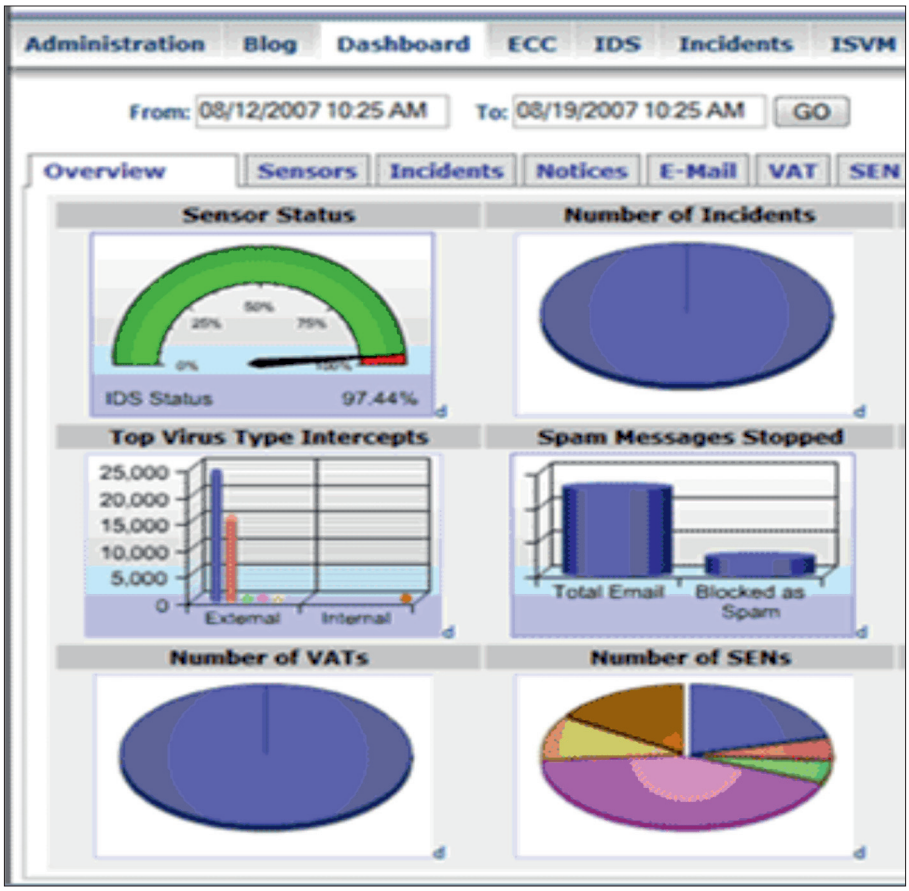
3.9 Reporting

ISOC should be capable of generating customised reports at regular intervals for the purposes of meeting compliance requirements, informing Top management, Audit requirements, and incident management. In general, the ISOC, may provide reports on the following:

- Security Event and Trend Statistics
- Firewall Traffic and Utilization Statistics
- Vulnerability Management
- Audit Compliancy
- Workload Prioritization
- Suspicious Host Detection
- IP Intelligence (Security Analytics)
- Compliance.

3.10 Developing Dashboards

Enterprise dashboards are the first points of contact in the area of Security Information Management. It provides a bird's eye-view to the top management on the security posture. Reporting of incidents and threats are commonly projected via the dashboard format. Dashboards act as frontends to ISOC tools by providing collaboration, workflow, publishing, reporting and tracking capabilities. The dashboard has to be customized to meet the requirements of set of stakeholders like Executives, CISOs, Operation team, etc. Below is an example dashboard:



The dashboard tab of the ISOC portal brings up the KPI dashboard. The Analyst can enter a range of dates, to see an overview of security metrics like IDS status, number of incidents, ISVM notices, top virus intercepts, spams messages stopped, number of vulnerabilities tracked, number of security event notifications and ISVM compliance. The graphically presented dashboard KPI should have drill-down capability.

The incorporation of a security blog allows the administrator to keep users advised of system news, help materials and other community-oriented material:

- A common feature list of a ISOC portal include: Security Event Notification Publishing & Tracking
- Comprehensive Incident Handling and Response Capabilities with Workflow
- Vulnerability Assessment Scan Scheduling and Tracking
- Vulnerability Management Publishing of Technical Alerts, Advisories, and Bulletins
- Vulnerability Management Compliance Tracking
- Dashboard View of Overall Security Posture of the organisation with drill-down capability
- Comprehensive Reporting Capabilities
- Facilitates Compliance with PCI DSS and other Regulatory Reporting
- Security Device Tracking
- Several Security Related RSS Feeds and Links to Security Vendors
- Source of information about the Organization's Security Policies and Directives
- Discussion Forum for Security Related Discussions
- Blog for Immediate ISOC Related Information to be posted
- Engineering Change Control for System Change Requests
- An Administrative Interface for Managing Users and Roles
- User role based with application role based access
- Ability to add data feed and generate dashboard graphs
- Ability to add third party software for integration to the portal such as Vulnerability Scanners and Ticketing Systems.

A sample list of dashboards is in Annex. 3-C.

3.10.1 Security Metrics Dashboard

Organisations need to communicate the operational results of ISOC to the top management. Today, communication is lacking in updating the decision-making executives of the organisations. Therefore, the organisation is unable to provide the necessary oversight to the security programme, which comes under the responsibility of the Security Operations Center, and runs the risk of not providing information to the organisation's regulatory bodies.

The security metrics dashboard can give a glimpse on the state of security to the top management. In terms of the metrics, this enterprise dashboard includes Privacy (reported incidents, resolved incidents), Threat Management (Forensic Investigations – active, new, closed, Intelligence – cyber threat incidents, Intrusion Detection – security tickets), Assessments (third party site assessments), Awareness & Education, and Issues Tracking (audits).

Security Metrics

2005 Metrics	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	YTD*
Privacy													
Reported Incidents	10	26	15	31	19	19	16	21	12	24	21	23	**237**
Resolved Incidents	12	22	9	20	22	16	21	20	21	14	7	10	**194**
Threat Management													
Forensic Investigations Active	48	63	62	56	68	58	65	48	46	37	31	32	32
Forensic Investigations New	26	26	26	25	17	22	18	20	9	17	20	22	**248**
Forensic Investigations Closed	11	27	32	13	27	15	35	22	18	23	19	27	**269**
Intelligence – Cyber Threat Incidents	281	85	172	83	79	53	45	183	44	34	40	82	**1181**
Intrusion Detection Security Tickets	2316	361	503	243	388	429	701	158	131	116	144	54	**5544**
Assessments													
Third Party Site Assessments Completed		1	3	7	11	3	2	0	0	8	1		**36**
Awareness & Education													
Percent Complete of the Tutorial 2005-2006										**64.47%**	**78.25%**	**80.58%**	**80.58%**
Issues Tracking													
Audit – Past Due Issues				11	19	11	10	7	5	5	6	4	4
Audit – Closed Issues	9	10	17	5	10	12	3	10	14	1	2	9	**102**
Risk Acceptances													
Risk Acceptances – Active						18	18	22	23	21	22	23	23
Risk Acceptances – Expired						7	7	3	3	2	4	4	4
Risk Acceptances – Closed						7	8	10	11	15	15	15	15

3.11 Testing the ISOC Deployment

There are different ways to test the ISOC deployment:

- Inject simulated test data into the ISOC database and see whether the incident response and ticketing mechanism along with dashboards are working fine
- Engage third-party pen-testers and check whether all the events are generated, data is collected by collectors and shipped to the central processor for analysis and alert is raised.

Develop attack cases and detection rules as given below, for few cases and test whether the ISOC is responding as expected.

Brute force attack to an administrative interface: This attack attempts to connect either to an exposed SSH server or to an exposed web administration page, through multiple connections with varying credentials. Using tools like Hydra, one can simply launch multiple connections to the server using different credentials every time until it succeeds to identify a valid account with its password. The rule of detection consists of a check of the number of connection attempts from a specific IP address over a period of three minutes. Use of TOR as a proxy for the brute force attack, resulting in a wide range of source addresses makes this rule practically useless. In order to be able to detect a successful attack, the SIEM needs a list of allowed IP address ranges that are entitled to access the associated administration interface. Successful connection from another IP address should generate an event “Remote Admin Access from Unknown Address”.

Conclusion

This chapter covered in detail the implementation and integration phases of ISOC, use case developments and dashboards.

Chapter 4

Operating ISOC: Governance, People and Processes

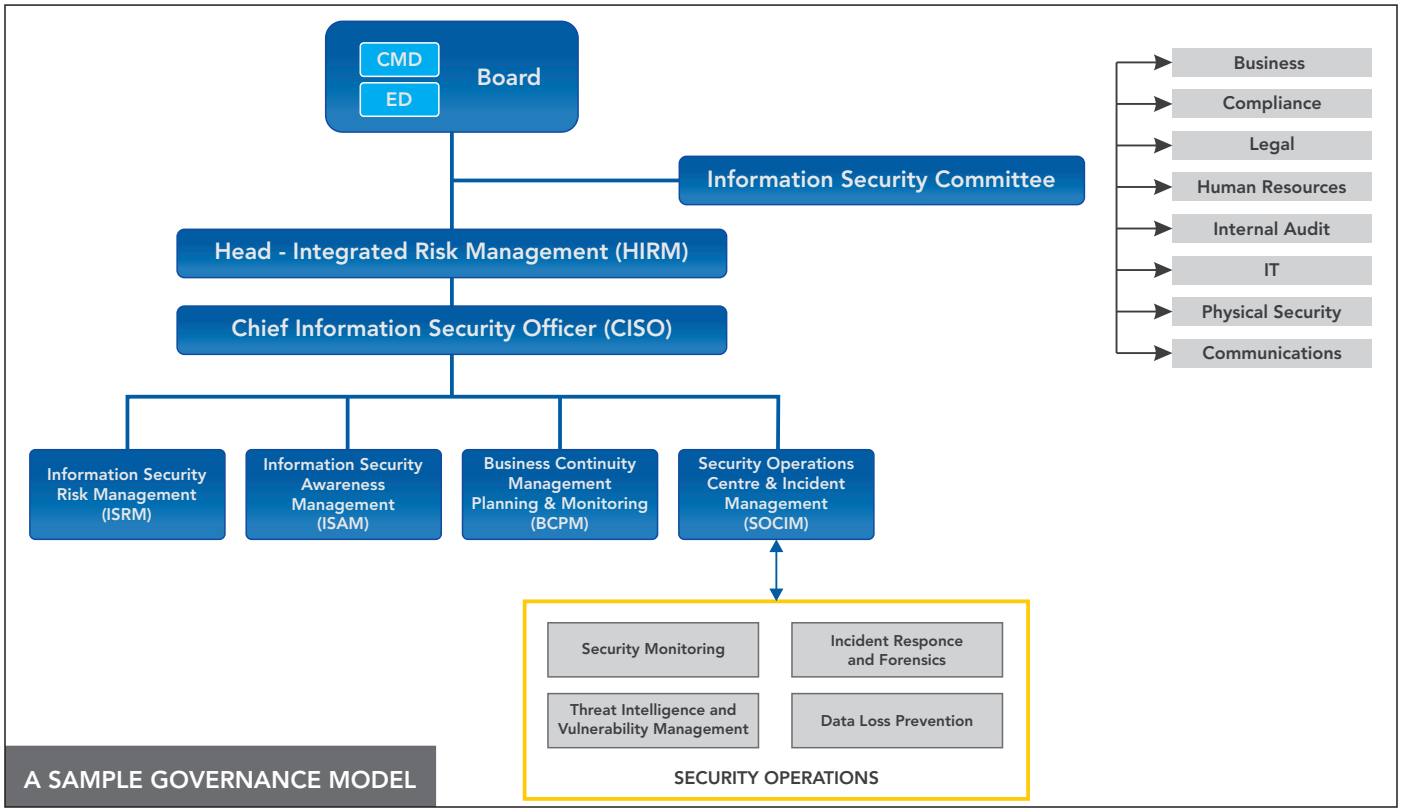
THE ISOC must align with and be integrated into the business process of an organisation with a strong Information Security principle that drives protection of valuable assets. The SOC operations must be integrated into the Risk Management, Business Continuity, Compliance and Governance processes. With Incident Response and Escalation procedures well-defined, Change Management, Alert and Notification policies need to be clearly communicated to business units from time to time.

4.1. ISOC Governance Model

Organisations need to develop a governance framework for escalating security issues and evaluating their impact on the business. The governance framework shall clearly define the place of ISOC in the organisational chart and describe the scope of ISOC authority, through policies and standards. The key aspects of governance include the following areas:

- Top Management/Board must be updated on the latest changes in the threat landscape
- Appropriate and insightful dashboards must be published
- There has to be a well-defined policy and procedure governing the security operations, which should be periodically reviewed
- There must an appropriate reporting structure/ escalation matrix, to be followed for critical incidents
- Key metrics must be defined to measure the efficiency of the overall ISOC team.

Lastly, all the stakeholders must be involved and a proper responsibility matrix must be defined so that everyone is aware of individual roles.



A SAMPLE GOVERNANCE MODEL

4.2 SOC Authority

The SOC Authority describes the amount of discretion the SOC has in directing actions that affect an organisation's assets, with or without permission from, or in co-ordination with other groups. The three levels of authority, an ISOC can exert are:

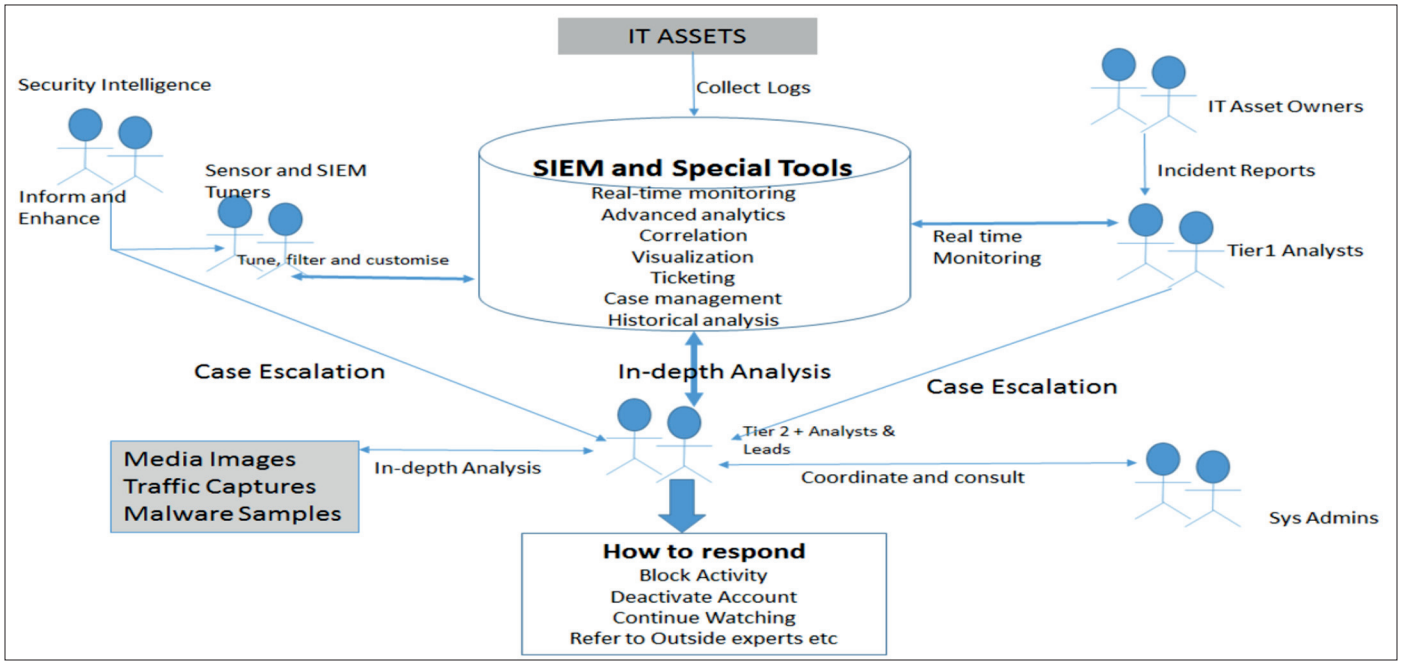
- **No Authority:** An ISOC can suggest to the IT asset owners, the actions they should take. However, the ISOC has no formal means to exert pressure. It is entirely up to the respective owners to heed or ignore the ISOC's recommendations.
- **Shared Authority:** An ISOC can make recommendations to executives (e.g., CIOs, CISOs, CEOs, system owners) who have various authorities to enact change. These recommendations are weighed against input from other stakeholders before a decision is made, giving the ISOC a right to vote, but not the final say.
- **Full Authority:** An ISOC can direct IT asset owners to take certain actions, without seeking or waiting for the approval or support from any higher-level executive.

An organisation can apply ISOC's formal authorities up to a point, beyond which the ISOC must turn to influence rather than mandate. For aggressive countermeasures or response such as disabling a key corporate server, high-level agreement and understanding is needed.

Therefore, organisations need to establish clear-cut policies describing, when an ISOC can exercise full authority, shared authority and no authority.

4.3 People, Processes and Technology

Security is becoming more and more established in the corporate structure and it is no longer acceptable for it to be a secondary function of an IT department. Most of the organisations are investing in the development of an ISOC to enhance their security posture and provide rapid response to events throughout the network. Building an ISOC is a monumental task. There are three major components that every organisation must include – People, Process and Technology. These three exist in all elements of security and one should consider them as equally critical components. The following picture depicts the interaction of people, process and technology within ISOC.



4.3.1 People

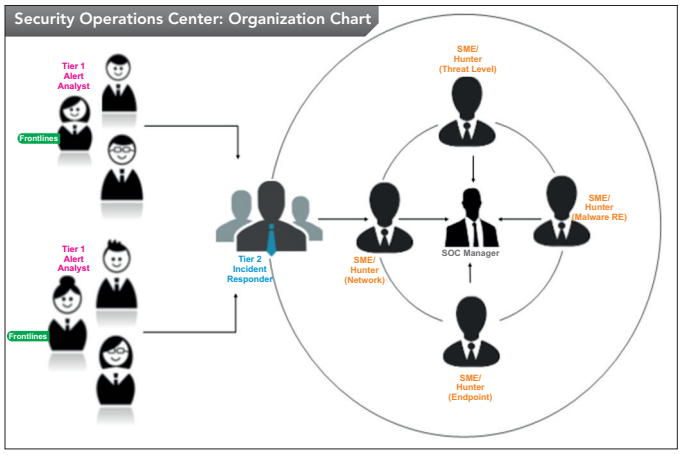
ISOC requires talented resources with deep technical knowledge, broad range of capabilities and diverse experience.

4.3.1.1 Tier 1 Alert Analyst

- Monitors the events queue
- Triages the security alerts
- Monitors the health of the security sensors and endpoints
- Collects data and is context necessary.

4.3.1.2 Tier 2 Incident Responder

- Performs deep dive by collating data from various sources
- Determines if a critical system or data has been impacted
- Advisory support
- Provides support for new analytic methods for detecting threats.



4.3.1.3 Tier 3 SME (Subject Matter Expert) or Hunter

- In-depth knowledge on network, endpoints, threat intelligence, forensics
- Acts as an incident 'Hunter', rather than waiting for escalated incidents
- Involves in developing, tuning and implementing threat detection analytics.

4.3.1.4 ISOC Manager

- Provides an overall direction for the ISOC
- Manages resources to include personnel, budget, shift scheduling
- Manages technology strategy to meet SLAs
- Communicates with management
- Organizational point of contact for business critical incidents
- Works with the ultimate goal of detecting, investigating and mitigating incidents that impacts business.

ISOC personnel must have the necessary training to deal with the constantly evolving and often quite challenging job of a security analyst, incident investigator, subject matter expert and ISOC Manager.

In addition to the ISOC analysts, the ISOC Manager plays a pivotal role. The ISOC Manager is responsible for prioritising work and organising resources with the ultimate goal of detecting, investigating and mitigating incidents effectively that could impact the business. The ISOC Manager should develop an incident workflow model and implement Standard Operating Procedures for the incident handling that helps the analysts guide through triage (order of treating security events) and response procedures.

4.3.2 Processes

ISOC processes and procedures can act as a buffer between the people and technology. Mature processes, procedures, and improving them constantly guarantee the success of ISOC. Capability Maturity Model® Integration (CMMI) is a process improvement approach that provides organisations with the essential elements of effective processes. Because ISOCs typically have a large number of processes and procedures, CMMI offers an architecture to help organise, maintain, and improve the processes and procedures. The ISOC processes are divided into four main categories:

Business Processes: Document all the administrative and management components that are required operate an ISOC efficiently.

Operational Processes: Document the mechanics of the daily operations, like shift schedules and turn-over procedures.

Analytical Processes: Encompass all activities designed to detect and better understand malicious events.

Technology Processes: Maintain all the information relating to system administration, configuration management and conceptual design.

The various processes that are necessary for an effective ISOC are depicted in following diagram:

4.3.3 Technology: ISOC Monitoring and Reporting

An enterprise wide data collection, aggregation, detection, analytic and management solution is the core technology of a successful ISOC. An effective monitoring system incorporates data gathered from the continuous monitoring of the log sources (network devices, servers, PCs, laptops, mobile devices).

Business	Operational	Analytical	Technology
BC/DR • Business continuity plan • Disaster recovery plan **Process improvement** • Maturity assessments • Project methodology • Knowledge management **Compliance** • Internal compliance • Compliance support **Metrics** • Reporting KPIs • SIEM performance • Operational efficiencies	**Event management** • Triage • Callouts • Case management • Crisis response **Daily operations** • Shift schedule • Monitoring • Problem and change • Shift turnover • Daily operations call **Training** • Training plans • Skills development tracking	**Subtle event detection** • Data visualization • Pattern analysis **Reporting** • Analyst comments • Incident summary • Threat reports **Incident management** • Incident research • Focused monitoring • Incident response **Intrusion analysis** • Event analysis • Threat intelligence • Information fusion	**Design** • Developing use cases • User and asset modeling **Configuration management** • SIEM architecture • Data Feed integration **System administration** • Access management • Maintenance and upgrades

SOURCE: HP

With the benefit of all the logs aggregated on the security monitoring system, ISOC analysts can leverage the monitoring system as an investigative tool from being just a detective tool; thereby reviewing the suspicious activities and to manage the response to an incident or a breach.

The ISOC is responsible for monitoring, detecting, analysing, investigating, isolating and responding to incidents. The ISOC technology is leveraged to carry the following ISOC operations on 24 × 7 basis.

4.3.3.1 Service Functions

Derive and document a list of service functions from the objective of the ISOC deployment. These may include:

- Status monitoring and Incident detection (Note: List is indicative, not exhaustive)
  - SIEM
  - AV
  - IPS/IDS
  - DLP
- Initial diagnostics and incident isolation

- Problem correction
- Work with OEMs
- Escalation to next tier level
- Closure of incidents in coordination with tier levels
- Persistent Threat Investigation.

The service functions will guide the ISOC personnel on the daily processes and procedures. Segregation of duties must exist between one tier to the other. For example, Status monitoring and Incident detection may be the service function of Tier 1 and working with OEMs may be the service function of Tier 2 or Tier 3 staff.

4.3.3.2 SIEM Health Check

The SIEM health status monitoring is designed to assist in increasing availability and uptime of SIEM. SIEM uptime monitoring consists of the following activities:

- Install monitoring software on eligible devices to monitor system health, system performance and report metrics to the authorized/concerned parties. For large organisations, this can be taken care by the Technology Team or NOC (Network Operations Centre) team
- Analyse and respond to key metrics such as:
  - Hard disk capacity
  - CPU and memory utilization
  - Process availability
  - Respond to alerts generated by the monitoring software.
- Where monitoring software installation is not possible on certain devices, the following activities can be performed:
  - Monitor the administrative interfaces of the devices
  - Monitor the event stream generated by the devices
  - Perform time based checks to verify any loss of connectivity to managed agents.
- If a security monitoring system (typically a SIEM) component is not functioning as expected or has a potential issue:
  - Tier 1 analysts shall create a ticket on the ticketing system
  - Perform preliminary investigation of the documented issue
  - Escalate to Tier 2/Tier 3 SIEM System administrators as appropriate
  - SIEM administrators shall further carry out the root cause analysis and track the incident to closure
  - Display the device health and outage ticket in the SIEM console and ticketing system.
- In the event where a SIEM system component becomes unreachable and that hampers log accounting on the SIEM console:
  - Notify the authorised contacts
  - Investigate the root cause related to the configuration and functionality of the system component
  - Display device health and outage tickets in the SIEM console and ticketing system
  - Provide troubleshooting and root cause analysis.

4.3.3.3 Event Monitoring and Investigation

SIEM Analysts shall perform event monitoring and analysis of security events and correlate events generated by the SIEM solution. They are responsible for analysing security events, determine if the events are considered an incident, then classify, prioritize and escalate as appropriate. Listed below are few of the activities of SIEM Analysts:

- Monitor SIEM events that result from real-time analysis and correlation of log data from sources identified

- Perform investigation and analysis of the events
- Assist in removing false positives and classify them as known events
- Create a ticket for effective tracking and closure
- Identify correlated events and classify them as security incidents upon investigation that include service levels, prioritisation based on SLAs, remediation and recommendations
- Analyse and respond to key health and availability monitoring metrics:
  - Correlation engine processing rate
  - Log manager processing rate
  - Backup of databases
  - Database utilization percentage.
- Examine SIEM configuration and its functionality for any potential issues that may result in malfunction of a particular component of SIEM or in entirety and escalate the matter.

Analysts must perform 24x7 security monitoring. Any qualified security event shall be reported to the concerned authorities based on the SLAs defined and agreed. Subsequent to the investigation of the alert and anomaly detection, the ISOC must provide a notification, typically containing the following information:

- Date of the alert triggered
- Time of the alert triggered
- Time zone of the customer location
- Log source
- Severity
- Classification
- Alarm ID
- Policy
- Source Host Name/Source IP address/Source Port
- Destination Host Name/Destination IP address/Destination Port
- User Account
- Event Count (Number of logs)
- Threat Description
- Impacted Host/Application
- Remediation/Recommended Action.

4.3.3.4 Alert Classification

The ISOC must follow a standard for severity level based on the classification of the alerts. The list of the identified classifications and associated severity with some example events can be found below. The ISOC Analysts must use this standard for tagging the severity while reporting legitimate alerts.

Classification	Description	Severity
Compromise	Logs reporting on a successful system or a network compromise.	High
Attack	Logs reporting on an activity indicating system or network attack. Attack is known to have originated from a "Bad Guy" source.	High
Denial of Service	Logs reporting on activity indicating denial of service where it is assumed to have succeeded to have failed.	High

Classification	Description	Severity
Malware	Logs reporting on activity indicative of malware installation, propagation or use which is specifically targeting the organisation and can be aligned with any Indicators of Compromise.	High
Suspicious	Logs reporting on an activity that is only suspicious but not known to be a legitimate attack.	Medium
Reconnaissance	Logs reporting on an activity indicative of or directly indicating system or network reconnaissance.	Medium
Misuse (Policy/Compliance violation)	Logs reporting on an activity indicating network or system misuse.	Medium
Activity	Logs reporting on general system or network activity.	Medium
Risk	Logs reporting on potential vulnerability weaknesses.	Medium
Authentication	Logs reporting on unusual authentication attempts and account modifications.	Medium
Access	Logs reporting on general system access activity.	Medium
Application	Logs reporting on application specific activity.	Medium
Failed Attack	Logs reporting on attack activity that was not successful, possibly due to preventive measures.	Low
Failed Denial of Service	Logs reporting on denial of service activity that was not successful, possibly due to preventative measures.	Low
Failed Malware	Logs reporting on malware activity that was not successful, possibly due to preventative measures.	Low
Failed Suspicious	Logs reporting on suspicious activity that was not successful, possibly due to preventative measures.	Low
Failed Activity	Logs reporting on general system or network activity that was not successful, possibly due to preventative measures.	Low
Other Security	Logs reporting on security activity not otherwise classifiable.	Low

4.3.3.5 Reporting Process

As a primary function, ISOC needs to generate regular reports to cater to different people or groups within the organisation. A report on incidents and another detailing the activity within the ISOC is usually generated every week. These reports can be delivered to the management and other members from the escalation matrix.

The ISOC manager must carry out regular review of all incident records for their resolution within the parameters of the defined severity levels. Proper review of incident records that exceeded standard resolution times needs to be validated to check whether they were handled appropriately. Based on the reviews and audits, the ISOC processes and procedures should be updated.

The service levels must be reviewed once in a month at least. An example of the response time and resolution time SLA can be defined as below. All the numbers are indicative and should be aligned with individual organisation security policy/incident response plan.

Severity	Response Time	Resolution Time	SLA
High	20 mins	24 hours	98%
Medium	60 mins	48 hours	98%
High	180 mins	96 hours	98%

Response time is the time within which a security event upon detected, is investigated and reported to the concerned domains along with recommendation to the incident occurred. Resolution time is the time within which the recommendation is applied and helped towards incident closure.

When the SLA of High Severity incidents are set at 98%, the ISOC is bound to respond to those events within 20 mins and resolve the incidents within three hours 98% of the times.

4.3.3.6 Incident Management Process

As per Symantec, “an incident is a set of one or more security events or conditions that requires action and closure in order to maintain an acceptable risk profile. In the haystack of events, organisations must find the "needles" that are the security incidents. Events are isolated and disconnected, but incidents add the context that enables security administrators to gain understanding and take action”.

The Incident Management allows technicians need to understand:

- **Scope:** The number of systems affected
- **Impact:** The degree to which each system is affected in terms of confidentiality, integrity and availability
- **Business Criticality:** The importance of the incident based on the business value of the impacted systems relative to other systems
- **Priority:** The urgency of the required response relative to other incidents.

The SANS Institute has articulated a thorough framework for incident handling that lends consistency to an often muddled process. Between identification and closure, according to SANS, the following types of activities should occur:

- **Containment:** Limiting the scope and magnitude of the incident
- **Eradication:** Eliminating the source of the problem or avenue of entry
- **Recovery:** Returning affected systems to their fully operational state
- **Follow-up:** Documenting the root cause and impact of the incident; and implementing measures to avoid recurrences.

4.3.3.6.1 Case Management

An analyst performs multiple searches to understand the nature, intent and scope of a suspicious activity as part of the investigation process. Unless these searches and the resultant data are organised properly, it becomes difficult to interpret and may lead to an incorrect conclusion resulting an incident to slip.

Cases need to be created within ISOC platform, which can act as a central repository of evidence tied to ongoing investigations. They can include any existing forensic data within ISOC, as well as external evidence such as screen captures from third-party

products. Case Management ensures that threats are proactively identified, prioritised and rapidly investigated within the Security Intelligence Platform for streamlined incidence response.

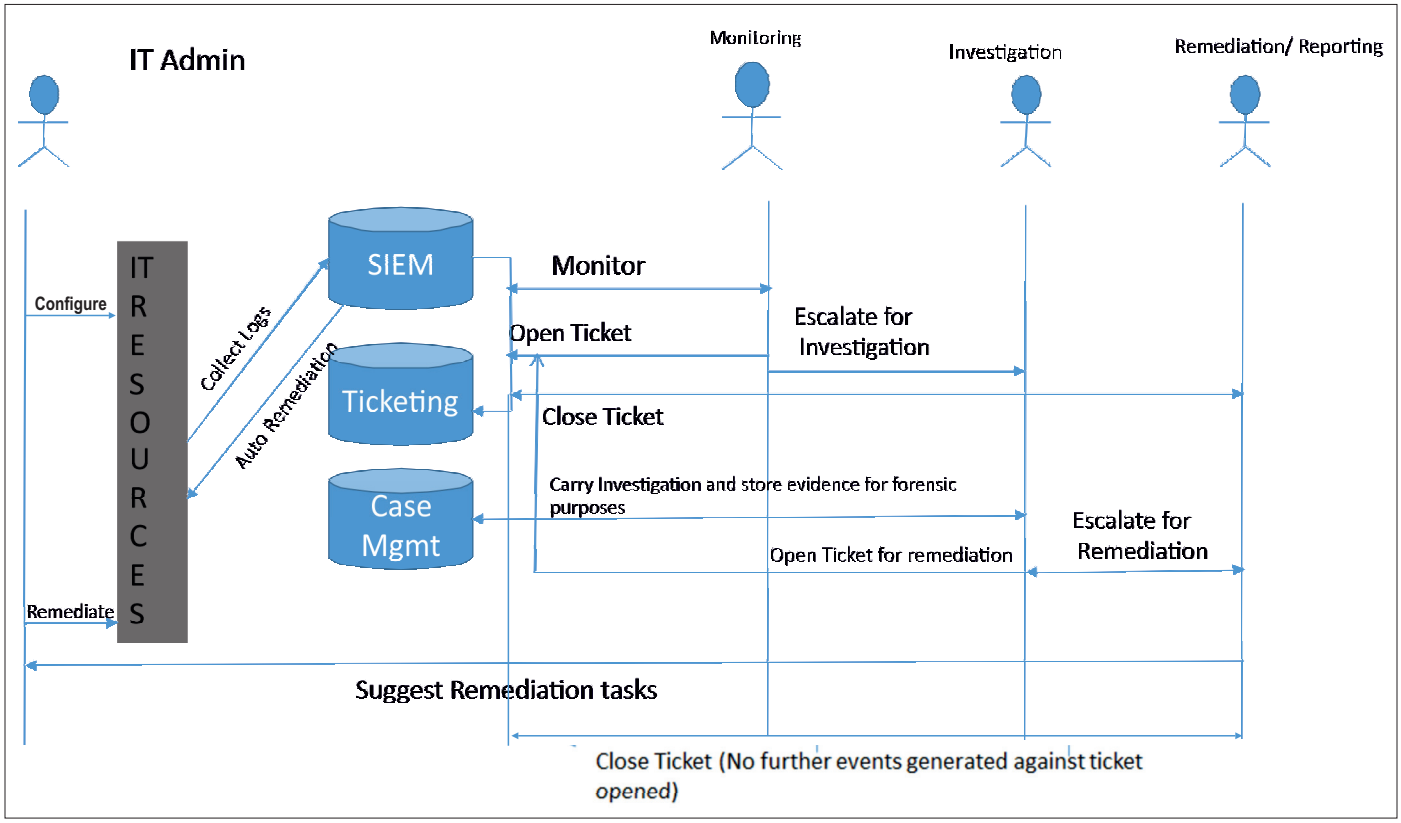
4.3.3.6.2 Incident Response Flow

Responding and managing an insider incident can be the most difficult phase. The ISOC should alert analysts via pager, e-mail, SMS, etc. and escalate those alerts. It can stop the progression of the threat/damage in real-time with or without human intervention.

Remediation too can take place with or without human intervention in the form of quarantining or blocking an IP address, disabling a MAC address port on a layer-2 switch and terminating a user's account. This limits their ability to login to the network or even physically access the building if the organisation has combined their physical and logical security solutions. The remediation capabilities need to follow industry best practices, organisational procedures, leverage change management parameters and provide full documentation of each change, change rollback and auditing capabilities.

One needs to decide what needs to be responded to automatically and what requires an analyst's intervention. When addressing insider threat scenarios that may have limited response windows, a growing number of organizations are now taking advantage of automatic remediation. This is a fundamental shift in how organisations have typically addressed remediation in the past, but a required change because the risks are now so great that there is often little to no time for a human response.

The following picture clearly illustrates the incident response process. In case of a security incident, the SIEM automatically opens a ticket in ticketing system or ticket opened by the Tier 1 monitoring people; Tier 2 personnel carry out investigation and assign resolution tasks to the remediation people.



4.3.3.7 Vulnerability Assessment and Penetration Testing

Another important component of the ISOC functions is Vulnerability Assessment and Penetration Testing. For large organisations, the same can be a part of a different team as per individual organisation security policy. The organisation's security policies must define the frequency at which the VAPT is performed at the minimum.

A standard approach is as follows:

- Define scope (devices that need to be scanned and their IP addresses)
- Set-up a virtual lab
- Install tools such as Nessus, NMAP
- Scan the IP addresses of the devices in scope
- Ensure to limit the number of concurrent connections so as to avoid a network crash
- Review the vulnerabilities detected
- Generate the report to publish the network assessment findings
- Each vulnerability will have a risk rating depending on the its severity
- Ensure to have all vulnerabilities closed per the timelines.

Conclusion

This chapter detailed how to operate ISOC with the help of a governance model, skilled proficient people and processes laid down by organisational policies.

References

- Addressing Insider Threats with ArcSight ESM, http://viewer.media.bitpipe.com/1120682139_877/1297107228_284/Addressing_Insider_Threats_With_ESM.pdf
- The SANS Institute, "Computer Security Incident Handling Step by Step," Version 1.5, May 1998
- Managing Security Incidents in the Enterprise http://www.symantec.com/avcenter/reference/incident.manager.pdf
- Intelligent Security Operations: A How-to Guide HP Enterprise Business White Paper, https://www.hpe.com/h20195/V2/getpdf.aspx/4AA6-6440ENW.pdf
- Case Management, https://logrhythm.com/products/features/case-management/
- Building a Successful Security Operations Centre, HP Enterprise Security Business Whitepaper.

Annex 1

ITIL Maturity Model

The Process Maturity Model for IT Asset Management proposed by Patricia Adams of Gartner (2003) is perhaps the most popularly cited model across ITAM literature. It has five levels of maturity: chaotic, reactive, proactive, service-oriented, and value creation.

Step	Attributes	Goals
1. Chaotic Uncontrolled environment *30% of enterprises*	• No processes, dedicated people or tools • No assigned accountability or accounting for changes • Unpredictable services, support and costs • Purchasing is ad hoc • Unused hardware and software are not controlled • Success depends on quality of people, not processes • Sub-optimization of efforts occurs.	• "Just want to know what we own, where it is, and who is using it" • One-time activity rather than systematic process.
2. Reactive Limited accountability *45% of enterprises*	• Focus is on asset counting • Employs physical inventory and some auto discovery recorded on spreadsheets or in a database • Accountability lies with IS organization but there is ineffective change accounting • Hardware and software viewed separately, not as single complex asset.	• Perform annual physical inventory and periodic spot audits • Report on asset counts, but cannot produce solid detail data to identify and resolve problems.
3. Proactive Life cycle focus *20% of enterprises*	• There is an IT Asset Program and manager with dedicated staff that reports to IS and finance organizations. • ITAM with auto discovery tools is integrated with service desk • Use of cross-functional teams for major asset management projects • Life cycle management process goes from requisition, to deployment, to retirement • Inventory system linked to financial and contractual data.	• "Clearly defined processes with accountability that detail the practical application of people, processes and tools that support the ITAM Program" • Effective change and configuration management processes • ITAM projects use repeatable processes that are well defined, adhered to, reviewed, and re-engineered when necessary. • ITAM operations manual with asset taxonomy produced and maintained.
4. Service Oriented Service level management *5% of enterprises*	• Metrics are available to measure program value • Services are delivered according to SLA-based plans • TCO processes in place • Automated requisition is integrated with purchasing and ERP systems • Just in time inventory practices used.	• Create SLAs for asset management and use them as a basis for planning • Conduct periodic reviews of service delivery quality • Institute an enterprise technology refresh plan for replacement and retirement of equipment.
5. Value Creation Cost recovery *< 1% of enterprises*	• There is a cost recovery process • Repository, auto discovery and asset-usage tools all in place • Seamless integration with strategic systems like HR, accounting, ERP, purchasing, network and systems management, IT service desk, problem and change management tools, and business continuity process • Decision support and analytic tools available for mining asset information.	• Continuous process improvement with improving metrics • ITAM data used for problem prevention • ITAM is a core business process and business enabler • Measurement of efficiency (employee productivity) and effectiveness (customer satisfaction) of business processes across all IT assets in the enterprise.

Annex 2

2.1 Logging Levels

Log Collection

In general, Syslog is the mechanism used for logging events. Microsoft Windows platforms need an agent to forward events in syslog format. The minimum parameters that need to be configured are:

- **Logging Destinations:** The collector, relay IP addresses, or hostnames. To how many destinations the syslog messages from originator need to be forwarded, is dependent on the implementation.
- **Protocol and Port:** By default UDP and port 514 are used. The option of changing to some other port and protocol is implementation specific.
- **Logging Severity Level:** It can be a value ranging from 0 to 7, as shown in the adjacent table:

Logging Severity Levels

Level	Severity Levels
0	Emergency: System is unusable
1	Alert: Action must be taken immediately
2	Critical: Critical conditions
3	Error: Error conditions
4	Warning: Warning conditions
5	Notice: Normal but significant condition
6	Informational: Informational messages
7	Debug: Debug-level messages

Logging Recommendations

Enabling logging is associated with cost on performance and functionality. Implement Time synchronization for timeline events. Enable local logging to act as a backup repository when the centralised logging solution fails. Before enabling logging, consider the following:

- Log events that are of business, technical, or compliance value
- Configure clients and servers for NTP
- Time stamp log messages and include the time zone in each message
- Configure the client with the minimum log collectors. Use Syslog relays to replicate and forward the same message to multiple destinations. The destinations could be like monitoring platforms such as security, problem management, and system and network health monitoring
- Baseline and monitor the CPU, memory, and network usage overhead introduced by the Syslog service
- Have a limited local logging facility, in file or memory, so that logs are not completely lost if the Syslog collector is unavailable, such as in the case of network failure
- On a regular basis, test that logging is functioning properly
- Protect Syslog implementation by providing confidentiality, integrity and authenticity
- The log rotation and retention policies be set properly
- Protect files where logs are stored:
  - Restrict access to the system by assigning proper files access permissions and enabling file encryption.
  - Grant read access to log files only to authorised users and processes
  - Grant write access to log files only to the Syslog service or any such collection service
  - Apply standard system hardening procedures to operating systems that host the logging server.

Logging Infrastructure

While designing a logging infrastructure, pay special attention to the type of data being received, expected storage, security requirements, and so on. Here are some factors that may influence the design of logging infrastructure:

- Higher severity levels generate more logging messages. For example, configuring a firewall for severity level 6 (information) results in logging multiple events per permitted connection: connection establishment, termination, and possibly network address translation.
- Allocate sufficient system resources to the syslog client and server based on the number of logging messages being generated and collected. One may need multiple logging servers to handle a large amount of logging data.
- The per-device and aggregate events per second (EPS) rates. This depends on the device type, available resources, logging level, security conditions, and its place in the network.
- The average size (in bytes) of logging messages.
- Network bandwidth available between the logging client and the logging server.
- Consider the load introduced by protecting syslog messages using secure network protocols such as TLS and DTLS.
- Consider the scalability requirements of the logging infrastructure as part of capacity planning.
- Collect logging messages using an out-of-band physical or logical network.

Having a separate management plane by way of virtual LAN (VLAN) or a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) is a good network and system management practice. One has no other option but to forward logging messages in-band if a system does not support having a separate physical or logical management interface.

2.2 Best Practices for Calculating EPS Rates

Speed of hardware, NICs (network interface cards), operating systems, logging configurations, network bandwidth, load balancing and many other factors must also go into benchmark requirements. One may have two identical server environments with two very different EPS requirements due to any or all of these and other variables. With consideration of these variables, EPS can be established for normal and peak usage times. The equations included here, therefore, determine Peak Events (PE) per second and to establish normal usage swap the PEx by NEx (Normal Events per second) in the equations.

List all of the devices in the environment are expected to report to the SIEM. Be sure to consider any planned changes, such as adding new equipment, consolidating devices, or removing end of life equipment.

First, determine the PE (or NE) for each device with these steps:

- Carefully select only the security events intended to be collected by the SIEM. Make sure those are the only events included in the sample being used for the formula
- Select reasonable timeframes of known activity: Normal and Peak (under attack, if possible). This may be any period from minutes to days. A longer period of time, such as a minimum of 90 days, will give a more accurate average, especially for “normal” activity. Total the number of Normal or Peak events during the chosen period. (It will also be helpful to consider computing a “low” activity set of numbers, because fewer events may be interesting as well.)
- Determine the number of seconds within the timeframe selected
- Divide the number of events by the number of seconds to determine PE or NE for the selected device.

Formula 1:

Number of Security Events / Time Period in Seconds = EPS

The resulting EPS is the PE or NE depending upon whether it began with peak activity or normal activity. Once completed this computation for every device, insert the resulting numbers in the formula below to determine Normal EPS and Peak EPS totals for a benchmark requirement.

Formula 2:

- From the production environment determine the peak number of security events (PEx) created by each device that requires logging using Formula 1. (for identical devices with identical hardware, configurations, load, traffic, etc., use this formula to avoid having to determine PE for every device): [PEx (# of identical devices)]
- Arrive at a grand total by summing up all PE numbers for the environment
- Add at least 10% to the grand total for headroom and another 10% for growth. The resulting formula becomes:

  Step 1: (PE1 +PE2 +PE3 ...+ (PE4 x D4) + (PE5 x D5)...) = SUM1 [baseline PE]

  Step 2: SUM1 + (SUM1 x 10%) = SUM2 [adds 10% headroom]

  Step 3: SUM2 + (SUM2 x 10%) = Total PE benchmark requirement [adds 10% growth potential].

The Peak EPS is arrived at once these computations are complete. Consult SMEs and the system engineers provided by the vendor in order to establish a realistic Peak EPS that the SIEM system must be able to handle.

Use this list along with peers' experience and other references as resources to set benchmarks for the infrastructure. Sample templates are provided below.

Qty	Type	Description	Avg EPS	Total Peak EPS	Average Peak EPS
750	Employees/Endpoints (Windows XP)	Desktops & Laptops at 5 locations	Included at domain severs	Included at domain servers	Included at domain servers
7	Cisco Catalyst Switches	One at each loaction, one in DMZ and one in the Trusted network	5.09	51.88	26.35
7	Cisco Gateway/Routers	One at each location	0.6	380.5	154.2
5	Windows 2003 Domain Servers	One at each location	40	404.38	121.75
3	Windows 2003 Application Severs	In high availability duster at Data Center	1.38	460.14	230.07
3	MS SQL Database Servers Running on Windows 2003 Server	High availability cluster at Data Center	1.83	654.9	327.45
6	Microsoft Exchange Servers	One at each location with two (duster) at the Data Center	3.24	1121.5	448.6
3	MS IIS Web Servers on Windows 2003	High availability cluster at Data Center	1.17	2235.1	1117.55

Qty	Type	Description	Avg EPS	Total Peak EPS	Average Peak EPS
2	Windows DNS Servers	At Data Center - failover	0.72	110.8	110.8
2	Linux Legacy Application Servers	At Data Center	0.12	43.6	21.8
1	Linux MySQL Database Server	One in trusted network for legacy application	0.12	21.8	21.8
7	NitroGuard IPS	One at each location, one in DMZ and one in the trusted network	40.53	5627.82	1607.95
1	Netscreen Firewall	Netscreen facing th Internet	0.58	2414	2414
3	Cisco Pix Firewalls	Between the Data Center and the other four sites, in front of trusted network between trusted and the DMZ	39	1734	1178
1	Cisco VPN Concentrator	Located at Data Center facing the Internet	0.83	69.45	69.45
1	Squid Proxy	Located at Data Center	14.58	269.03	269.03
		Totals	**149.79**	**15598.9**	**8118.8**

Feature	Benchmark	Settings	Explanation	Avg.	Peak	Avg. Peak
System Logs Collected	Relevant and Critical logs are Collected. Should be able to handle peak threshold.					
Network Devices ▪ Fire Walls ▪ VPNs/SSL ▪ IAM.Switches ▪ Routers ▪ Web Process	Source destination, calls connections, access, traffic and other security-related log data can be collected and normalized at specified rate..					
EndPoints ▪ Servers ▪ O/S's ▪ Security ▪ Mac ▪ MCs	Collection from endpoint security-related data at specified EPS.					
Commercial Apps ▪ HR/Workflow ▪ Business Critical ▪ Contain P1 Data	Security- related data from commercial applications is collected as needed.					

Feature	Benchmark	Settings	Explanation	Avg.	Peak	Avg. Peak
Custom Apps ▪ Legacy apps ▪ Mainframe ▪ Midrange	Security-related data from custom/legacy applications and systems are collected as needed.					
Databases ▪ Third Party DB ▪ Monitoring tools ▪ Database Session logs	Access logs and other security-related data from databases collected.					
Backup Systems	Backup Systems log data is collected.					
Virtual System Logs (applies to any of the Above systems that are virtualized)	Virtual Machines(VMs) and VM managers are held to the same performance and monitoring standards as physical devices.					

2.3 Threat Information Sharing

A number of standards of schemas are being developed for disseminating threat intelligence information, including the following:

- **Structured Threat Information eXpression (STIX):** An express language designed for sharing of cyberattack information. STIX details can contain data such as the IP address of command-and-control servers (CnC), malware hashes, and so on. Learn more at http://stix.mitre.org/
- **Open Indicators Of Compromise (OpenIOC):** Open framework for sharing threat intelligence in a machine-digestible format. Learn more at http://www.openioc.org/
- **Cyber Observable eXpression (CybOX):** A free standardized schema for specification, capture, characterization, and communication of events of stateful properties that are observable in the operational domain. Learn more at https://cybox.mitre.org/

Transport mechanisms, such as Trusted Automated eXchange of Indicator Information (TAXII), are used to exchange cyberthreat information represented by the previously discussed schemas.

2.4 ISOC Budget

People Cost

The following table shows a sample cost for ISOC personnel. The annual salary and benefits may vary from state to state (or countries). The number of people are estimated for running a 24×7 ISOC with three analysts in first shift and two analysts in second and third shifts.

Annual Personnel Cost Estimates Template

Job	Quantity	Unit Annual Cost	Total Annual Cost
Tier 1 Analysts			
Tier 2 Analysts			
Tier 3 Analysts/ Threat Hunters			
Forensic Specialist			
Malware Engineer			

(Estimate for a 24x7 ISOC will depend upon number of shifts and actual number of analysts required for an organisation)

Job	Quantity	Unit Annual Cost	Total Annual Cost
ISOC Manager			
Total Annual Cost			

(Estimate for a 24x7 ISOC will depend upon number of shifts and actual number of analysts required for an organisation)

Capital Cost for Technology

The following table shows estimated cost of technology. This may vary depending upon size of organisation but this template tried to cover major expenses. As an example, the cost of SIEM may be much smaller or quite large depending upon geographical locations, amount of data collected, applications, and so on. This is to give a starting point.

Capital Cost Template

Description	Quantity	Unit Cost	Total Cost
SIEM Solution			
NBAD			
PIM			
DAM			
Server Hardware			
Laptops			
Forensic Software			
Secure Cabinets/Locks			
Log Storage and backup			
Office, Furniture, etc.			
Miscellaneous			
Professional Consulting/design/ setup			
Total Annual Cost			

(The list is indicative. Other S/W and H/W costs to be added as per requirement)

Other Annual Recurring Costs

Example of other recurring costs are given in the table below. First two rows are left empty. A simple rule is to take 20% of capital expenses as annual depreciation and maintenance cost. Accounts personnel may have to be consulted for a better estimate.

Annual Recurring Cost Estimates

Description	Quantity	Unit Cost	Total Cost
Depreciation of office equipments			
Software/Hardware Maintenance			
Staff Training , Skills update			
Incident Response Exercises			
Threat Intelligence Feeds			
Vulnerability Scanning (Network)			
Vulnerability Scanning (Applications)			
Total Annual Cost			

(The list is only indicative. Other similar costs to be added as per the setup)

References

- Benchmarking Security Information Event Management (SIEM) by J. Michael Butler https://www.sans.org/reading-room/whitepapers/analyst/benchmarking-security-information-event-management-siem-34755
- Building a Successful Security Operations Center Part 3: SOC Budget Calculator by Rafeeq Rehman http://rafeeqrehman.com/2017/02/05/soc_budget_calculator/

Annex 3

3 - A : Log Collection Format

S. No.	Operating System/ IOS	Version	Application (AV, ADS/LDAP, DHCP, Mail, Custom applications, etc.)	Hostname	IP Address	No. of devices	Log Collection Method	Owner	Location	Remarks

3 - B: Indicative List of Assets

S. No.	Asset	Quantity	Vendor/Brand and Version
1	Unix Servers (Linux, AIX, HP-UX, etc.)		
2	Windows General Purpose Servers		
3	Windows Active Directory Servers		
4	Windows IIS and Exchange Servers		
5	Proxy Servers		
6	DNS and DHCP Servers		
7	AS 400/iSeries		
8	Mainframe/LPARs		
9	Routers and Switches		
10	Firewalls – Internal		
11	Firewalls – External		
12	VPN devices		
13	Network IDS/IPS		
14	Host IDS/IPS		
15	Database Activity Monitoring Systems		
16	Antivirus Servers		
17	Endpoint DLP		
18	Network DLP		
19	Database Servers		
20	Applications		
21	Ticketing Systems (for example BMC Remedy)		

S. No.	Asset	Quantity	Vendor/Brand and Version
22	Custom Applications/Additional Log Sources (insert rows below and describe)		
23	<insert rows here>		
24	<insert rows here>		
25	Total Event/Log Sources		
26	Do you want to capture netflows? If so, please answer a and b below.		
27	a. How many total end user workstations/laptops are on the network?		
28	b. How many total servers are on the network?		
29	Total Flow Sources		

3 - C: Indicative list of Dashboards

Dashboard Type	Dashboard Name	Value to Graph	Chart Type	Display Top	Capture Time Series Data	Time Range
Threat & Security Monitoring	Default - IDS/IPS-All:Top Alarm Signatures (Event Count)	Event Count (Sum)	Pie Chart	10	Yes	24 hours
	Top Systems Attacked (IDS/IDP/IPS) (Event Count)	Event Count (Sum)	Table	10	yes	24 hours
	Most Recent Offenses	Default	Default	Default	No	1 minute
	Most Severe Offenses	Default	Default	Default	No	1 minute
	Top Category Types	Default	Default	Default	No	1 minute
	Top Sources	Default	Default	Default	No	1 minute
	Top Local Destination	Default	Default	Default	No	1 minute
Network Overview	Firewall Deny by DST IP (Event Count)	Event Count (Sum)	Bar Chart	5	Yes	24 hours
	Firewall Deny by DST Port (Event Count)	Event Count (Sum)	Table	5	Yes	24 hours
	Top Talkers (Total Bytes)	Total Bytes (Sum)	Bar Chart	5	Yes	24 hours
	Top Log Sources (Event Count)	Event Count (Sum)	Table	5	Yes	24 hours
	Firewall Deny by Source IP (Event Count)	Event Count (Sum)	Bar Chart	5	Yes	24 hours

Dashboard Type	Dashboard Name	Value to Graph	Chart Type	Display Top	Capture Time Series Data	Time Range
Application Overview	Outbound Traffic by Country/Region (Total Bytes)	Total Bytes (Sum)	Bar Chart	10	Yes	24 hours
	Top Applications Outbound to the Internet (Total Bytes)	Total Bytes (Sum)	Bar Chart	10	Yes	24 hours
	Total Applications (Total Bytes)	Total Bytes (Sum)	Bar Chart	10	Yes	24 hours
Vulnerability Management and Intelligence	Security News	Default	Default	5	No	1 minute
	Security Advisories	Default	Default	5	No	1 minute
	Internet Threat Information Center	Default	Default	Default	No	1 minute
	Scans In Progress	Default	Default	5	No	1 minute
	New Vulnerabilities in the last 7 days	Vulnerability Count / Network	Bar Chart	10	No	1 minute

3 - D: Sample Attack Scenarios

Brute force attack to an administrative interface (SSH, application interface)

This scenario is straight forward. Multiple connection attempts either to an exposed SSH server or to an exposed web administration page. The attack scenario includes two variants, one – resulting in a successful connection after some requests and another with no success.

Vulnerability Exploitation of Critical Server

- **Authentication bypass of an SQL server:** Attempt to bypass the authentication procedure of an SQL server by exploiting known vulnerabilities
- **Abuse of misconfigured DNS server (open relay):** Exploitation of a DNS server which permits openly (from any host, not restricted to its own network) recursive queries in order to conduct a reflected attack
- **Abuse of misconfigured SMTP server:** Exploitation of an SMTP server which permits everyone (from any host, not restricted to its own network) to send e-mails to any destination in order to contribute to spam campaign
- Application level attack to web server (SQL injection): Exploitation of an application level vulnerability on a web page allowing the attacker to dump the database.

Virus/Trojan Infection in the Internal Network

Malware infection through e-mail attachment, spreading itself throughout the internal network.

Covert Channels of Communication

This kind of attack involves the use of a side channel in order to circumvent monitoring and bypass control. As an example, an attack including a DNS server abuse from an internal user in order to establish a DNS tunnel and circumvent data traffic policies regarding data ex-filtration was used.

Detection of Advanced Persistent Threat

Advanced persistent threat (APT) includes a variety of attacks and techniques sharing a common factor, the

advanced level of sophistication and complexity of the attack in order to avoid detection and treatment. As an example of such attack, we used the infection and compromise of the critical infrastructure (Web Server) without identification of the entry point/procedure (in our case, phising e-mail leading to trapped web page distributing malware).

3 - E: Use Case Development

Use Case Development

Look at cybersecurity incidents that the organisation has experienced over the past few years. Look for common occurring scenarios in those incidents.

Look at the recent audit findings. See if the findings can be addressed by being able to detect and respond to particular threats to particular assets more effectively.

Look at the SIEM selected by the organisation. See whether there are any use-cases that can be relatively deployed using easy to integrate event and data sources with the off-the-shelf correlation rules within SIEM.

Here is an example of a simple use case. (Source: CISCO SOC Book)

Background

As a result of recent audit, all administrative access to critical systems has been given through PIM (Privileged Identity Module) servers. Admins need to log in to PIM, before proceeding for accessing any critical server. The advantage of this kind of system is that all admin activities can get recorded. However, organisation suspected that some direct admin access continued to happen avoiding the PIM. Management requested a use case that could be used to flag potential policy violations for further investigation.

Document the Use Case

Use Case ID: Critical Systems – Admin Access 1

Scope: Critical Systems

Use Case Category and subcategory: Policy Violations – Inappropriate administrative Access.

Use Case Objective: Aimed at generating an alert the moment it is noticed that a critical server is accessed without going through PIM.

Use Case Logical Flow: When an administrative access to a critical system happened, check whether that access was granted from PIM. If not, generate an alert.

Correlation Rules and Data Analysis: Capture the current set of critical systems through the asset management feed. Correlate administrative access success events on all critical systems with administrative access success on PIM. Where an administrative access on critical systems is successful without a matching event on PIM; (or) where IP address of host logging into critical system is not PIM, generate a high priority alert to the main channel.

Data Collection Points:

- CMDB – Configuration Management Database for asset criticality
- Event log and Syslog associated with all critical systems
- Event logs and Syslog associated with PIM.

Damage Potential: High, due to risk associated with inappropriate administrative access.

Implementation and Ongoing Operational Effort: Simple, no additional advanced parser or customization required.

Views and Visualisations: Alerted as high priority with in main channel and compliance channel. Relevant alerts to be reported via ad hoc and regular compliance reporting.

Compliance Mapping: Administrative Access Policy

Standard Responses and Escalations: Alerts need to be investigated by analysts, see whether the alert is false positive, if false positive, report it as false and close. Otherwise, if this appears to be inappropriate behaviour by an authorised admin, alert admin's direct supervisor or manager.

Glossary

1	AIX	An Unix Flavour Operating System sold by IBM
2	APT	Advanced Persistent Threats
3	BCP	Business Continuity Planning
4	BOT	Build Operate and Transfer Model
5	CISO	Chief Information Security Officer
6	CMDB	Configuration Management Database
7	CMMI	Capability Maturity Model® Integration
8	CnC	Command-and-Control
9	CSOC	Cyber Security Operations Center
10	CTI	Cyber Threat Intelligence
11	CybOX	Cyber Observable Expression
12	DAM	Database Activity Monitoring
13	DB	Database
14	DBA	Database Administrator
15	DBMS	Database Management Systems
16	DC	Data Center
17	DCL	Data Control Language
18	DDL	Data Definition Language
19	DDOS	Distributed Denial of Service
20	DHCP	Dynamic Host Configuration Protocol
21	DLP	Data Leakage Prevention
22	DML	Data Manipulation Language
23	DMZ	Demilitarized Zone
24	DNS	Domain Name System
25	DOS	Denial of Service
26	DPI	Deep Packet Inspection
27	DR	Disaster Recovery

28	DRP	Disaster Recovery Plan
29	DSS	Data Security Standard
30	DST	Destination
31	DTLS	Datagram Transport Layer Security
32	EPS	Events per Seconds
33	ERP	Enterprise Resource Planning
34	FPS	Flows per Second
35	HP-UX	An Unix Flavour Operating System sold by HP
36	ICT	Information and Communication Technology
37	IDAM	Identity Access Management
38	IDS	Intrusion Detection System
39	IP	Internet Protocol
40	IPS	Intrusion Prevention System
41	ISOC	Information Security Operations Center
42	ISO	International Organisation for Standardisation
43	ISP	Internet Service Providers
44	ISVM	Information Security Vulnerability Management
45	ITAM	Information Technology Asset Management
46	ITIL	Information Technology Infrastructure Library
47	ITSM	IT Service Management
48	JDBC	Java Database Connector
49	KPI	Key Performance Indicator
50	LDAP	Lightweight Directory Access Protocol
51	MDM	Mobile Device Management
52	MPLS	Multiprotocol Label Switching
53	NAC	Network Access Control
54	NAS	Network Attached Storage
55	NAV	Network Analysis and Visibility

56	NBAD	Network Behaviour Anomaly Detection
57	NDA	Non-Disclosure Agreements
58	NE_x	Normal Events per Second
59	NICs	Network Interface Cards
60	NMAP	Network Map
61	NOC	Network Operations Center
62	NTP	Network Time Protocol
63	OEM	Original Equipment Manufacturer
64	OpenIOC	Open Indicators of Compromise
65	OS	Operating System
66	OTP	One-Time Password
67	OWASP	Open Web Application Security Project
68	PCI	Payment Card Industry
69	PE	Peak Events
70	PIA	Privacy Impact Assessment
71	PIM	Privilege Identity Management
72	PKI	Public Key Infrastructure
73	RFP	Request For Proposal
74	ROI	Return On Investment
75	SACM	Service Asset Configuration and Management
76	SAN	Storage Area Network
77	SDN	Software Defined Network
78	SEN	Security Event Notifications
79	SIEM	Security Incident and Event Management
80	SLA	Service Level Agreement
81	SMTP	Simple Mail Transfer Protocol
82	SNMP	Simple Network Management Protocol

83	SOP	Standard Operating Procedures
84	SQL	Structured Query Language
85	SSO	Single Sign-on
86	STIX	Structured Threat Information Expression
87	TAXII	Trusted Automated Exchange of Indicator Information
88	TCL	Transaction Control Language
89	TCO	Total Cost of Ownership
90	TCP	Transmission Control Protocol
91	TLS	Transport Layer Security
92	TOR	The Onion Router (used for Accessing Internet anonymously)
93	UAT	User Acceptance Test
94	UDP	User Datagram Protocol
95	VAPT	Vulnerability Assessment Penetration Testing
96	VPM	Vulnerability and Patch Management
97	VPN	Virtual Private Network
98	WAF	Web Application Firewall
99	WAN	Wide-Area Network

CONTRIBUTORS

Mentor

DR. A.S. RAMASASTRI, Director, IDRBT

Members

Shri Y. V. Ramana Murthy, CISO, State Bank of India

Shri Sachin Y Shende, General Manager ,RBI

Mrs. B. Aparna, Manager (Systems), State Bank of India

Shri. Nabojyoti Sarkar, Manager, ICICI Bank

Shri Murtaza Bhatia, Practice Head (Data Centre & Security), Dimension Data

Shri B. Kuldeep, Manager, Deloitte

Shri P. Parthasarathi, Chief Technology Officer, IDRBT

Shri. G. Raghuraj, General Manager, IDRBT

Dr. V. Radha, Assistant Professor, IDRBT

Dr. Rajarshi Pal, Assistant Professor, IDRBT

Shri. V. S. Mahesh, Assistant General Manager, IDRBT

Institute for Development and Research in Banking Technology
(Established by Reserve Bank of India)

Castle Hills, Road No.1, Masab Tank, Hyderabad - 57.
EPABX: +91 40 2329 4999, Fax: +91 40 2353 5157
Web: www.idrbt.ac.in, e-mail: publisher@idrbt.ac.in