Building Your Security Operations Center and Taking it to the Next Level

Abstract

IT threats continue to evolve and become more evasive, blended, and persistent, with attackers finding resourceful ways to avoid detection and breach security. The key to cyber defense is to develop Security Operations Centers (SOCs) that will evolve continuously to effectively counter such advanced attacks. This paper presents a comprehensive strategy for developing a next-gen SOC, along with a systematic approach to effective management.

Although most large enterprises have Security Operations Centers (SOCs), nearly 70% of security breaches are detected by external agencies[1].

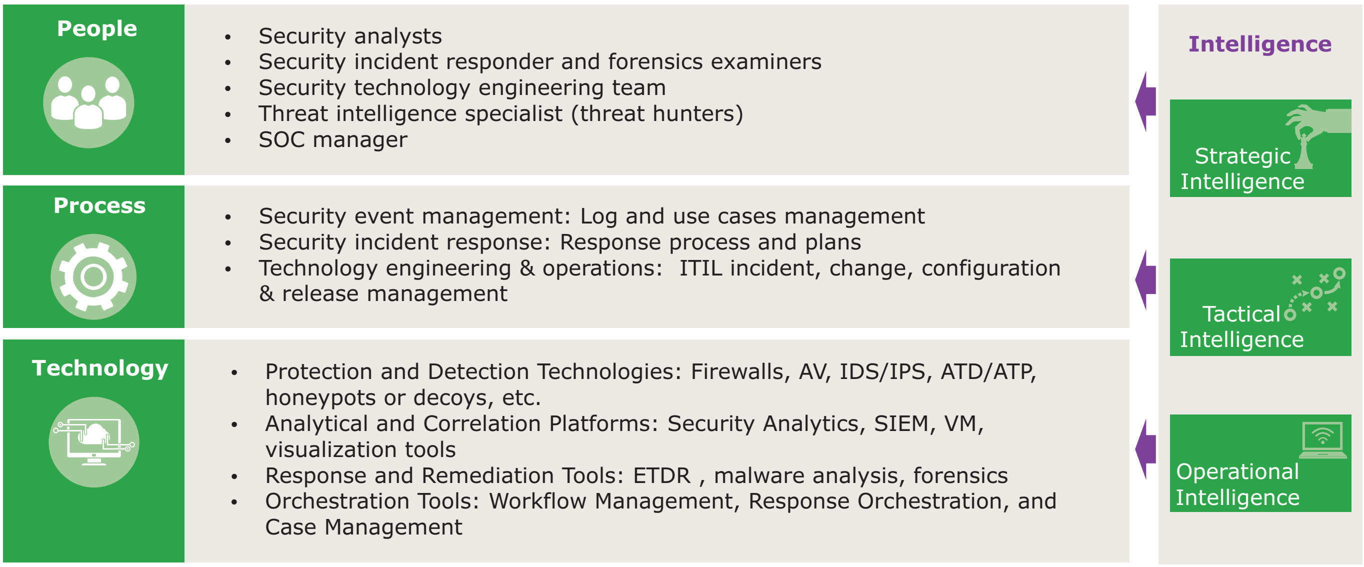
Evolving Security Threats

As 2015 saw several high-profile cyber security breaches involving JP Morgan Chase and Sony[2], among others, enterprises are increasingly focusing on developing and maintaining a robust Information Security Operations Center (SOC) to achieve that impeccable security. Most SOCs currently focus on perimeter and network threats, resulting in incomplete coverage and limited ability to address security requirements. This is compounded by:

- Impeded visibility into security issues due to multiple teams working in silos
- Lack of broader organizational participation and effective processes to support response management
- Shortage of skills and attrition

Three Steps to a Successful SOC

Four key elements go into building a world-class SOC: people, processes, technology, and intelligence (Figure 1). The wider the coverage of SOC across these four aspects, the more robust the security management.



People

- Security analysts
- Security incident responder and forensics examiners
- Security technology engineering team
- Threat intelligence specialist (threat hunters)
- SOC manager

Process

- Security event management: Log and use cases management
- Security incident response: Response process and plans
- Technology engineering & operations: ITIL incident, change, configuration & release management

Technology

- Protection and Detection Technologies: Firewalls, AV, IDS/IPS, ATD/ATP, honeypots or decoys, etc.
- Analytical and Correlation Platforms: Security Analytics, SIEM, VM, visualization tools
- Response and Remediation Tools: ETDR , malware analysis, forensics
- Orchestration Tools: Workflow Management, Response Orchestration, and Case Management

Intelligence

Strategic Intelligence

Tactical Intelligence

Operational Intelligence

SOC Building Blocks

Building a comprehensive SOC is a long-term initiative. The following three steps are critical to developing an effective SOC.

1. Define the strategy and implementation plan.

As security management requirements vary across organizations, it is imperative to first understand the enterprise’s requirements and drivers for an SOC. Therefore, you need to:

- Conduct an as-is assessment to gain insight about the current state, define the target state, and plan better to implement effective solutions.
- Plan a phase-wise implementation with key objectives for each phase, as well as details of activities you need to perform.

2. Define the key components.

Define the technologies to be used in the SOC and how they are to be integrated. Then, identify information and event sources, develop use cases, and decide on the reporting structure.

- **Technologies:** The key technologies needed for a SOC are listed in Table 1. These technologies can be adopted based on where you are on the maturity curve. For example, in terms of detection and protection, you can start with basic security controls such as antivirus, intrusion detection, proxies, and firewalls), and then move on to more enhanced techniques such as honey pots and endpoint threat detection and response. Similarly, in terms of security analytics, you can first ensure you are reviewing security event data, and later include forensic-level information. For service management, you can start with a simple workflow and later add response orchestration for automation.

Types	Technologies
Detection and Protection	• Next-generation firewalls • Email security gateway • Web security gateway • Intrusion detection/prevention system • Antivirus (network and endpoint) • Integrity monitoring and change detection • Advanced threat detection/prevention • Honeypots and decoys • Endpoint threat detection and incident response
Security analytics and incident response	• Security information and event management • Data analytics • Malware analysis (static and dynamic) • Host and network forensics • Visualization and analytics tools
Orchestration	• Workflow automation • Response orchestration • Case management

Table 1: Information Sources

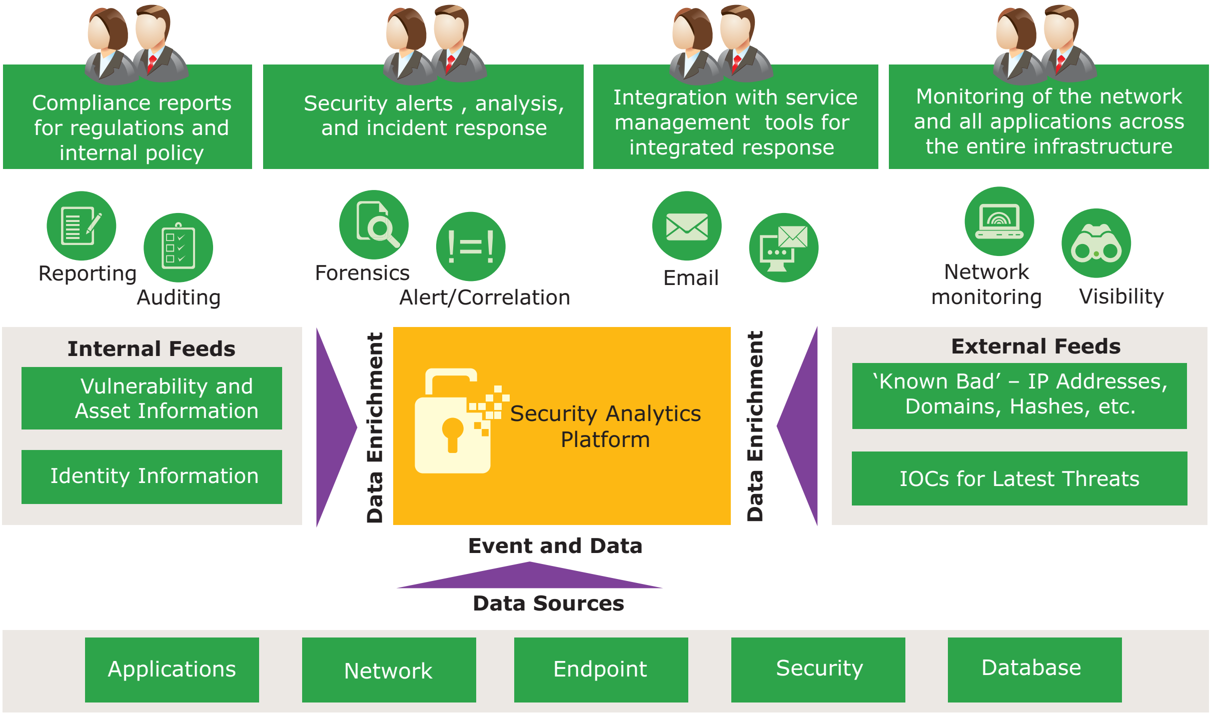
- **Information Sources:** Next, organizations should identify the most relevant information sources like:
  - Security tools or devices such as antivirus systems, firewalls, and web and email security that generate alerts and events for any security issue detected.
  - Identity and access management (IAM) systems including an active directory and IAM tools
  - Enrichment sources including internal and external data feeds that help understand the context and evaluate a security incident.
  - Platform and application related information
- **Reporting and Use Cases:** After selecting the technologies and information sources, define use cases and reports. To arrive at these use cases, you should:
  - Create a high-level threat profile of the environment
  - Set high-level detection objectives, including events of interest (e.g., brute force attacks, data exfiltration, etc.) and the threshold for each
  - Create reports that offer a view of overall traffic trends or attack patterns to facilitate informed decisions. To be effective, these reports should be
    - Targeted to the recipients
    - Provide actionable insights for each stakeholder
    - Have well-defined key performance indicators (KPIS) and key risk items (KRIS) for each line item

3. Implement the SOC.

The implementation phase includes deployment of the selected SOC tools and technologies, configuration of processes, and creation of an SOC team. Each technology has a different topology, as defined by the vendor. The most critical is the security analytics layer, which gathers information from various sources and brings additional context from external and internal sources to deliver efficient and actionable information to the SOC team. Figure 2 shows our suggested model for security analytics.

Key reports you should consider are:

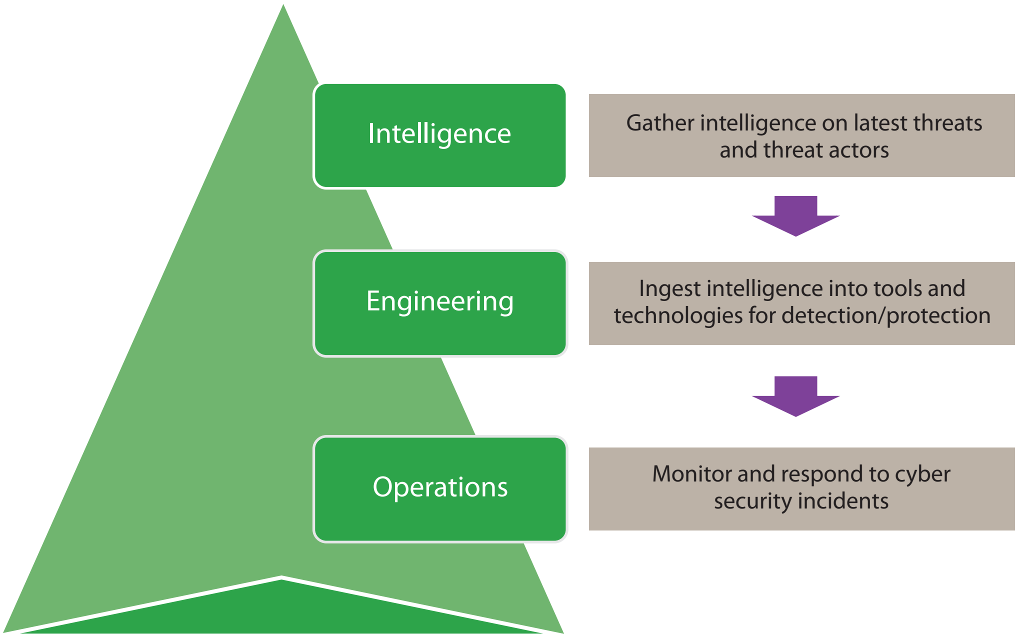
- A security risk dashboard that highlights big risk items, current open issues, and overall security health
- Security events trends, which cover issues related to access, vulnerabilities, malware, intrusions, etc.
- Compliance status, including top violators and actions required
- Service management reporting, including volumes handled and SLA performance


Compliance reports for regulations and internal policy
Security alerts , analysis, and incident response
Integration with service management tools for integrated response
Monitoring of the network and all applications across the entire infrastructure
Reporting
Auditing
Forensics
Alert/Correlation
Email
Network monitoring
Visibility
Internal Feeds
Vulnerability and Asset Information
Identity Information
Data Enrichment
Security Analytics Platform
Data Enrichment
External Feeds
'Known Bad' – IP Addresses, Domains, Hashes, etc.
IOCs for Latest Threats
Event and Data
Data Sources
Applications
Network
Endpoint
Security
Database

Security Analytics Model

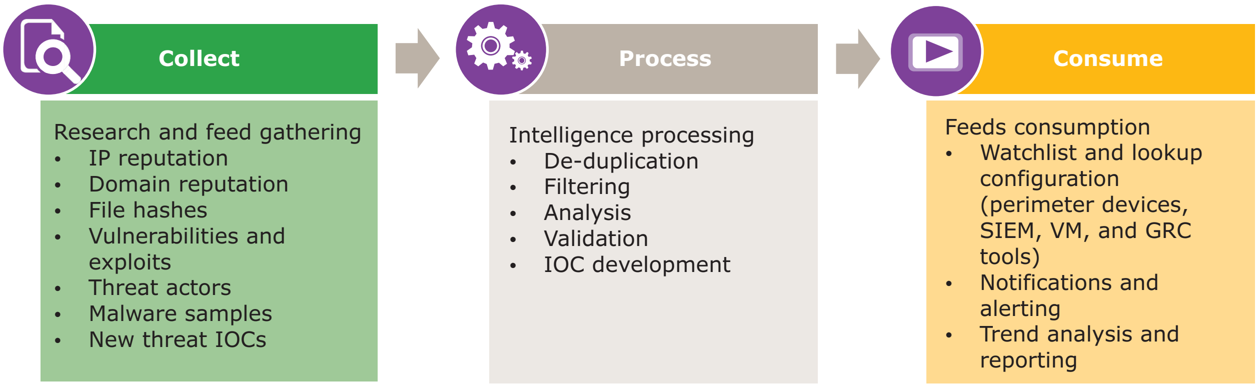
Role of Intelligence, Technology, and Operations Units

The core reason why SOC is different from other IT support functions is the ever-changing nature of vulnerabilities. The key aspects of SOC service operations are depicted in Figure 3.


Intelligence
Gather intelligence on latest threats and threat actors
Engineering
Ingest intelligence into tools and technologies for detection/protection
Operations
Monitor and respond to cyber security incidents

SOC Operational Pyramid

- The research and intelligence unit: This unit should continuously research the latest threats and vulnerabilities and define the indicators of new threats. Threat intelligence involves collection, processing, and consumption of information (Figure 4). Rather than rely solely on threat feeds, which generally help in malware-specific use cases only, organizations should ensure continuous development of use cases or new alerts to detect potential threats.



Collect

Research and feed gathering
- IP reputation
- Domain reputation
- File hashes
- Vulnerabilities and exploits
- Threat actors
- Malware samples
- New threat IOCs

Process

Intelligence processing
- De-duplication
- Filtering
- Analysis
- Validation
- IOC development

Consume

Feeds consumption
- Watchlist and lookup configuration (perimeter devices, SIEM, VM, and GRC tools)
- Notifications and alerting
- Trend analysis and reporting

Threat Intelligence Processing

- The technology and engineering unit: This unit implements the use cases in production. To ensure the right use of security intelligence, organizations need to implement ways to detect indicators of compromises (IOCs) within the security tools.

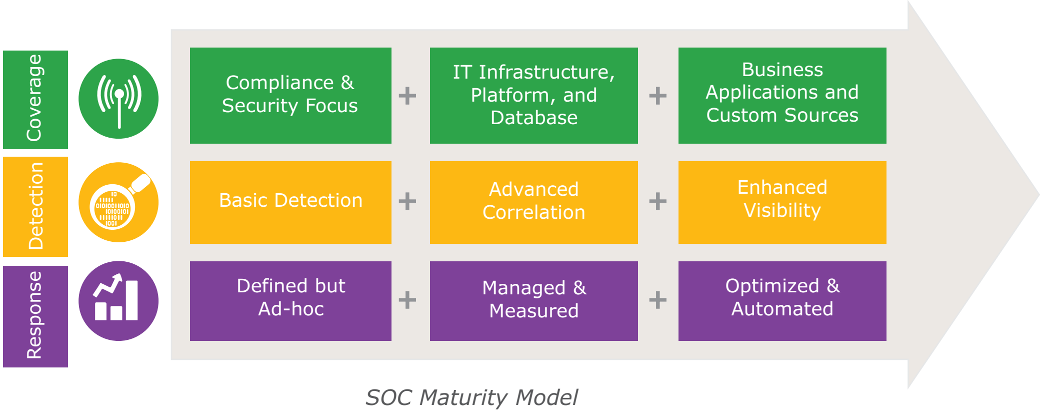
- The operations and response unit: Even a well-defined and designed SOC may fail to operate effectively in the event of too many false positives or false negatives. For efficient operations, use a customized version of the incident response framework defined by the National Institute of Standards and Technology (NIST)[3], which advocates four steps to incident response: detection, containment, eradication, and restoration. The SOC team should take control in the detection, containment, and eradication phases for efficient threat detection and faster incident response.

Around 35% of detection comes from threat intelligence information.

Implementing Continuous Improvement and Transformative Initiatives

Increasing maturity in coverage, detection, and response capabilities is the goal of an SOC. Figure 5 depicts a mature, effective SOC.

To ensure that security coverage is not limited to perimeter and security devices, organizations need to ensure wider coverage that includes a number of geographies, business units, use cases, and technologies.



Coverage	Compliance & Security Focus +	IT Infrastructure, Platform, and Database +	Business Applications and Custom Sources
Detection	Basic Detection +	Advanced Correlation +	Enhanced Visibility
Response	Defined but Ad-hoc +	Managed & Measured +	Optimized & Automated

SOC Maturity Model

Security requires holistic visibility. To deliver modern use cases in a next-generation SOC, the platform should support Big Data analytics and workflow-based response capabilities. Analysis of information from various sources will eventually improve endpoint and network visibility and enable enterprises to facilitate advanced malware solutions.

To improve response management, the first phase is to define the response strategy and document the same for security analysts. Then measure responses and move to automated response management for higher quality and operational efficiency.

Conclusion

Having a comprehensive SOC can enhance your ability to proactively detect, prevent, and respond to security threats and incidents. Given the rapidly evolving digital landscape and nature of threats, technologies used in SOCs should be scalable and interoperable to ensure effective and efficient operations. The process should be designed with stakeholder accountability and communications, and associated mechanisms should be defined as part of the processes.

While it is imperative to build an SOC with the right mix of talent and functional attributes, infrastructure, processes, and technologies, continuous improvement to achieve operational maturity should also be ensured.

References

[1] FireEye, Mandiant 2015 Threat Report, accessed August 2016, https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf

[2] Forbes, The Top 10 Security Breaches Of 2015 (Dec 31, 2015), accessed on Aug 3, 2016, http://www.forbes.com/sites/quora/2015/12/31/the-top-10-security-breaches-of-2015/#30afc4694ff0

[3] NIST, Computer Security Incident Handling Guide (Aug 2012), accessed Nov 2015, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

About The Authors

Tirath Singh

Tirath Singh is part of the Managed Security Services team within the Enterprise Security and Risk Management (ESRM) business unit at Tata Consultancy Services (TCS). Singh has 12 years of experience in building and managing Security Operations Centers.

Contact

Visit TCS’ Enterprise Security and Risk Management services unit page for more information

Email: Global.esrm@tcs.com

Subscribe to TCS White Papers

TCS.com RSS: http://www.tcs.com/rss_feeds/Pages/feed.aspx?f=w
Feedburner: http://feeds2.feedburner.com/tcswhitepapers

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model^{TM}, recognized as the benchmark of excellence in software development. A part of the Tata Group, India’s largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

Experience certainty.

IT Services
Business Solutions
Consulting

TCS Design Services I M I 12 I 16