ArcSight™

Whitepaper

Building a Successful Security Operations Center

This paper outlines industry best practices for building and maturing a security operations center (SOC). For those organizations planning to build a SOC or those organizations hoping to improve their existing SOC this paper will outline the typical mission parameters, the business case, people considerations, processes and procedures, as well as, the technology involved.

Research 014-052809-09

ArcSight, Inc.
5 Results Way, Cupertino, CA 95014, USA
www.arcsight.com info@arcsight.com

Corporate Headquarters: 1-888-415-ARST
EMEA Headquarters: +44 870 351 6510
Asia Pac Headquarters: 852 2166 8302

Introduction

In order to prevent the myriad of modern attacks, comply with government and industry regulations, monitor deployed technology solutions, and verify the endless human interactions with technology, organizations turn to industry-leading security technology. They may go to IBM Internet Security Systems for their network intrusion prevention systems (IPS), Cisco for their firewall solutions, and McAfee for host-based protection. This heterogeneous approach to selecting security solutions provides organizations the best-of-breed technologies and offers inherent security by not relying on any single vendor or security platform.

The combination of technologies does, however, present a large challenge - there is no inherent way to normalize, aggregate, and correlate the security events across technologies. Further, one team may support the firewalls, another may support the network IPS devices, and yet another may support the host-based security tools. This leads to security monitoring that is performed using different tools and by different teams. Piecing together the details of an attack in real-time becomes incredibly difficult and even forensic analysis after an attack is slowed by the need to combine event streams. In reality, building and maintaining a strong security posture necessitates a centralized effort to monitor, analyze, and respond to security events across technologies as quickly as possible.

To meet this need, many organizations turn to Managed Security Services Providers (MSSPs) to outsource the bulk of security monitoring and testing. MSSPs offer a number of benefits because they can:

- Monitor security events around-the-clock and provide in-depth information security expertise.
- Spot patterns across a number of customers to provide advanced warning on new threats.
- Provide services to customers that do not have dedicated information security staff.

However, MSSPs also present a number of disadvantages. Namely, MSSPs do not:

- Have an in-depth knowledge of the customer's policies, procedures, or overall IT environment.
- Offer dedicated staff for every customer. Only large organizations that spend the most with the MSSP generally receive dedicated support.
- Offer customized services, processes, or procedures for the customer needs. MSSPs strive to standardize services in order to gain economies of scale in providing security services to many customers.
- Store security data only at the customer premise. Security data will be transmitted and stored at MSSP locations that may or may not be in the home country.

Weighing the considerations, many IT groups decide to build their own Security Operations Center (SOC) to correlate events and centralize the security monitoring, analysis, and response within a single team. For these organizations, the MSSP's disadvantages outweigh its benefits. There are unique business requirements that require a dedicated SOC, or there may be cost drivers that dictate the need for an in-house SOC. Building an in-house SOC does, however, present its own set of challenges and many groups struggle on how to best start. This paper will offer a clear understanding of how to build your own SOC and balance the triad of IT project components – people, processes, and technology - to jumpstart your efforts.

Mission and Business Case

Prior to building a security operations center, organizations need to take some time to plan. All too often this planning focuses only on the people, process, and technology components of the project and ignores outlining the fundamental drivers for why the SOC is needed and what business problems the SOC will solve. Prior to developing the project plan for building a SOC, project sponsors need to take a hard look at the overall mission and business case for the SOC.

Mission

All successful teams need a unifying sense of purpose to help motivate team members, prioritize work, and respond effectively to the changing needs of the business. Time spent in this phase of planning will benefit the SOC long-term. Prior to building a SOC, organizations must answer the following questions:

- What needs will the SOC meet for the organization?
- What are the specific tasks assigned to the SOC? (e.g., detecting attacks from the Internet, monitoring PCI compliance, detecting insider abuse on the financial systems, incident response and forensic analysis, vulnerability assessments, etc.)
- Who are the consumers of the information collected and analyzed by the SOC? What requirements do they hope to impose on the SOC?
- Who is the ultimate project sponsor for the SOC? Who will "sell" the SOC to the rest of the organization? What requirements will he or she levy on the SOC?
- What types of security events will eventually be fed into the SOC for monitoring?

Business Case

There are very few organizations that are going to approve the build-out of a SOC without a clear outline of the costs and strategies to recover those costs. In outlining the costs of the SOC, the following items will help start the discussion:

- **Facilities:** Furniture, computer equipment, special badging requirements, power, HVAC, telephony
- SOC Labor: Security analysts, shift leads, SOC managers
- Supporting Labor: Network support, system support, database support, telephony support, security device management (if not performed by the SOC)
- Education and Training: Classes, conferences, continuing education
- Threat intelligence subscriptions: Up-to-the-minute information on the latest threats
- Monitoring technology: Hardware, software, storage, and implementation services
- Additional technologies: Problem and change management, email, knowledge sharing

Recovering these costs is a much tougher problem to solve. The following list outlines some common approaches in justifying the expense of a SOC:

- Cost avoidance: Building the SOC will cost far less than not detecting, preventing, and responding to attacks.
- Cost efficiencies: Chances are that many of the SOC processes or technologies can help automate functions already taking place within the organization. By accepting a new data feed and producing automated reporting, a SOC can often save the organization money by reducing manual effort.
- Cost sharing: In many cases, other groups are currently tasked with the responsibilities outlined for the future SOC. Are those groups willing to "outsource" these responsibilities to the SOC? Having other organizations help to foot the bill can minimize the overall impact to all.
- Revenue / Cost Recovery: Can SOC services be offered to customers – either internal or external? There is more work in determining separation of information among customers, pricing models, and other business aspects, but actual revenue (or cost recovery in the case of internal customers) is a powerful argument where SOC services can be leveraged to perform security services for other organizations.

People

Once the SOC mission and business case are clearly outlined, project teams can then focus on the traditional IT project components of people, process, and technology. While no portion of the triad is more important than the other, organizations tend to fail more often in attracting and retaining the key people necessary to operate a SOC effectively.

Selection

The most common error in implementing an internal SOC is attracting people with the right skills. Companies tend to start with too low a skill set for the analyst. The SOC analyst is the infantry man of the information security community engaged in daily trench warfare with a tough and innovative opponent. This is an opponent who understands the rigors of monitoring a console for malicious events that are masked by thousands of nuisance events. The effective SOC analyst needs a good deal of trouble-shooting patience, the ability to research problems, and an unflappable ability to communicate during stressful times. It takes more than entry level IT skills to succeed.

While the exceptional candidate can go from a help-desk technician to being an effective SOC analyst, a better initial capability is found in system administration, desktop support, and network operations personnel. Personnel experienced in network, server, and desktop support tend to have the troubleshooting background to excel quickly in the typical analyst tasks involving the depths of the TCP/IP protocol suite and various intrusion detection signatures.

Career Progression

Monitoring and responding to an endless supply of security events is enough to tire even the most eager information security professional. As such, the typical tenure of a SOC analyst is between one to three years. This makes it imperative to continually identify candidates for the next generation of analysts and plan the career progression for existing analysts. The SOC Manager should develop strong relationships with other IT groups to help identify those candidates wanting to start a new information security career. Additionally, the SOC Manager should look toward Incident Response teams, Audit, and other advanced information security groups to help offer SOC personnel a career path after their SOC tenure.

Training

No SOC analyst can be effective without appropriate training; luckily, there are very good options for building an effective training program. When crafting training plans, SOC managers should include both formal training on standard information security skills and on-the-job training (OJT) to maximize the analysts' effectiveness within the organization.

Formal training should include the SANS (System Administration and Network Security) "Intrusion Detection in Depth" training module and the GCIA (GIAC Certified Intrusion Analyst) certification. This is the industry standard in training analysts in the fundamentals of TCP/IP, TCP/IP monitoring tools, and skills associated with advanced intrusion analysis. For those organizations standardizing their Security Information and Event Management (SIEM) program around ArcSight, the ArcSight Certified Security Analyst (ACSA) training is a must-have. ACSA trains analysts to properly identify, correlate, and filter critical security events using the ESM product.

On-the-job training programs should provide an overview of important information security concepts, training on specific intrusion detection tools in use, analytical processes and procedures, and effective communication techniques. The SOC analyst will be required to effectively communicate and brief all levels of engineers and senior management during times of extreme stress, thus training in managing combative communication is invaluable. This training should also include the hierarchy of communication methods. Learning when to page, call, e-mail or assign a ticket is a critical skill. Additionally, it is important that any analyst learn to communicate in concise well-written papers and e-mails. SOC managers should create a program that has aspiring analysts writing analytical papers and then presenting their findings to their peers to hone written and verbal communication skills.

Staffing Plans

Staffing plans will evolve directly out of the needs of the mission. Is the SOC a virtual entity where events are collected, analyzed, alerted, and reported? Must the SOC have full-time personnel to monitor consoles, analyze, alert, and report? Or, does the SOC need full staffing twenty-four hours a day, 7 days a week, all year round? These mission needs will dictate the staffing models that must be implemented.

Despite the particulars of any giving staffing models, there are some guidelines to follow:

- One SOC analyst should never be alone in manning a shift. There are a myriad of safety and performance issues that can result.
- Each shift and role within the SOC should have clearly-defined responsibilities and deliverables.
- There should be no ambiguity in what is expected from each analyst at any given time during a SOC shift.
- There needs to be a clear "hand-off" between shifts. Each shift should keep a formal log of events documenting those issues that need additional or continual attention.
- There is a significant issue that always shows up on any night shift - the analysts feel ignored and uninformed. The SOC manager must work hard to ensure he/she constantly communicates with the night shift and even schedules time to work alongside.
- In order to staff a SOC 24x7x365, ten SOC Analysts are required. The shift schedule that best fits this staffing model is four twelve-hour shifts per week. Each analyst works three days on, four days off, followed by four days on, and three days off. This totals to 84 hours in two weeks. Additionally, two of the more experienced analysts (commonly referred to as Level-2 Analysts) work an 8x5 shift and are available to cover shifts for planned and unplanned absences. Figure 1 shows a sample schedule for a 24x7x365 shift schedule.

	DAILY SCHEDULE (8AM TO 8AM)			
Level 1 Analysts	Night Shift	Day Shifts 1 & 2 10AM to 10PM	Night Shifts 3 & 4 10PM to 10AM	
Level 2 Analysts	Day Shift 8AM to 5PM	Night Shift 5PM to 2AM	On-call Rotation	
Security Engineers	Day Shift 8AM to 5PM	On-call Rotation		
SOC Management	Day Shift 8AM to 5PM	On-call Rotation		

	WEEKLY SCHEDULE						
	SUN	**MON**	**TUES**	**WED**	**THURS**	**FRI**	**SAT**
Level 1 Analysts (Week 1)	Shift 1 (Days)				Shift 2 (Days)		
	Shift 3 (Nights)			Shift 4 (Nights)			Shift 3
Level 1 Analysts (Week 2)	Shift 1 (Days)			Shift 2 (Days)			
	Shift 3 (Nights)		Shift 4 (Nights)				Shift 3
Level 2 Analysts	On-call Rotation	Business Week					On-call Rotation
Security Engineers	On-call Rotation	Business Week					On-call Rotation
SOC Management	On-call Rotation	Business Week					On-call Rotation

Figure 1: Sample 24x7x365 SOC shift schedule

Processes and Procedures

SOC processes and procedures can act as a buffer between the people and technology. For example, new analysts will have very little idea how to start and it's likely that existing staff will not have a good deal of dedicated time to help train. Well-documented processes and procedures can clearly guide the new analysts' actions in those formative days. Additionally, the SOC technology may not have all the necessary features to accommodate a specific business need. Processes and procedures can pick up the slack by allowing people to follow guidelines to accomplish tasks manually.

To achieve an effectively operating SOC, the associated processes and procedures must not only exist but also be mature. Maturity in process management is first achieved by repeatability and then by continuous process improvement. The Carnegie Mellon® Software Engineering Institute (SEI) Capability Maturity Model® Integration (CMMI) offers a great approach to continuous process improvement. From the SEI web site:

> Capability Maturity Model® Integration (CMMI) is a process improvement approach that provides organizations with the essential elements of effective processes. It can be used to guide process improvement across a project, division, or an entire organization. CMMI helps integrate traditionally separate organizational functions, set process improvement goals and priorities, provide guidance for quality processes, and provide a point of reference for appraising current processes.

Because SOCs typically have a large number of processes and procedures, CMMI offers a great architecture to help organize, maintain, and improve this body of work. For most organizations, CMMI Level 3 is a sufficient goal. This maturity level ensures the processes and procedures are documented and subjected to demonstrable improvement over time. In practical terms, this means that any given analyst on any shift will execute a procedure in exactly the same manner. Additionally, if an analyst finds an error or change needed in a procedure they can make an on-the-spot correction and all subsequent analysts will benefit immediately from the improvement.

Note: This type of dynamic process and procedure maintenance is best achieved by the use of a wiki collaboration environment (e.g., Twiki or MediaWiki). A wiki documentation system is a collection of web pages that allows visitors to contribute and modify content on the fly. While other knowledgebase tools can effectively store documentation and offer adequate version control, not many tools can keep up with the dynamic needs of constant documentation updates like a wiki. (Note: A common use for dual monitors at SOC operations pods is to use one for console monitoring and the other for procedural reference and research.)

Process Hierarchy

Generally speaking, a process defines who is responsible for doing which tasks, and a procedure tells them in detail how to accomplish the task. For a SOC, there are generally fourteen main processes and around thirty-six subordinate procedures as shown in Figure 2. These are arrayed in a pyramid to demonstrate that each process and accompanying procedures rely on the processes below them. Thus, metrics support process improvement, technology design and event management support intrusion analysis, etc.

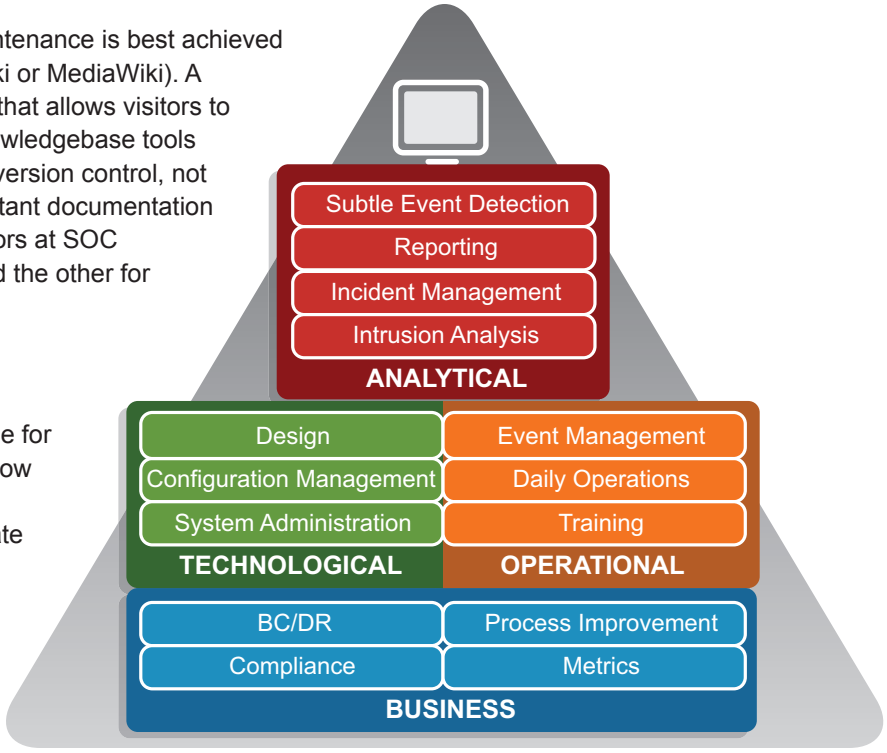

Figure 2: Process hierarchy that shows the various SOC processes and how they build on each other.

SOC processes are broken up into the four main categories:

- Business processes: Document all the administrative and management components that are required to effectively operate a SOC.
- Technology processes: Maintain all the information relating to system administration, configuration management and conceptual design.
- 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.

Organizational Relationships

In addition to documenting the processes and procedures necessary to operate the SOC effectively, the SOC must have a large number of external relationships to effectively manage a crisis situation. These relationships can include internal teams, such as: Incident Response, Security Management, Security Engineering, Legal, Human Resources, Public Relations, and Lines of Business. Relationships will also include external teams like: CERT/CC, Information Sharing and Analysis Centers (ISAC), local and national law enforcement, supporting product vendors, etc. All the various points of contact (POCs) should be well-documented along with how and when the SOC should involve them in a developing situation.

Detection vs. Analysis

There is a key distinction to use in developing SOC processes and procedures. Detection time is defined as the period of time from when an event is identified within the SOC to when the analyst makes a decision as to how to act on it. For example, an analyst detects a SQL injection attack against a monitored web server. She will then conduct initial research using intelligence about the various threats to better understand whether the event points to a true attack. After research, the analyst will determine the priority of the event and annotate the event. For example, a misconfiguration of the security device, a false positive event due to a faulty web app, worthy of additional monitoring attention, worthy of additional research, or a confirmed intrusion attempt to be escalated.

The analytical time frame begins once operational time is past and continues for up to 90 days. After initial research, an analyst will typically annotate an event for further analysis. At this point, the processes within the analytical time frame take over. More senior personnel will continue researching the events, notify the necessary constituents, report the event, and perform forensic analysis as needed. Analysis continues as trends and long-term patterns are analyzed by visual data mining and other advanced analytical techniques. This distinction in timeframes, as shown in Figure 3, will help to organize SOC processes and clearly delineate roles among the associated actions.

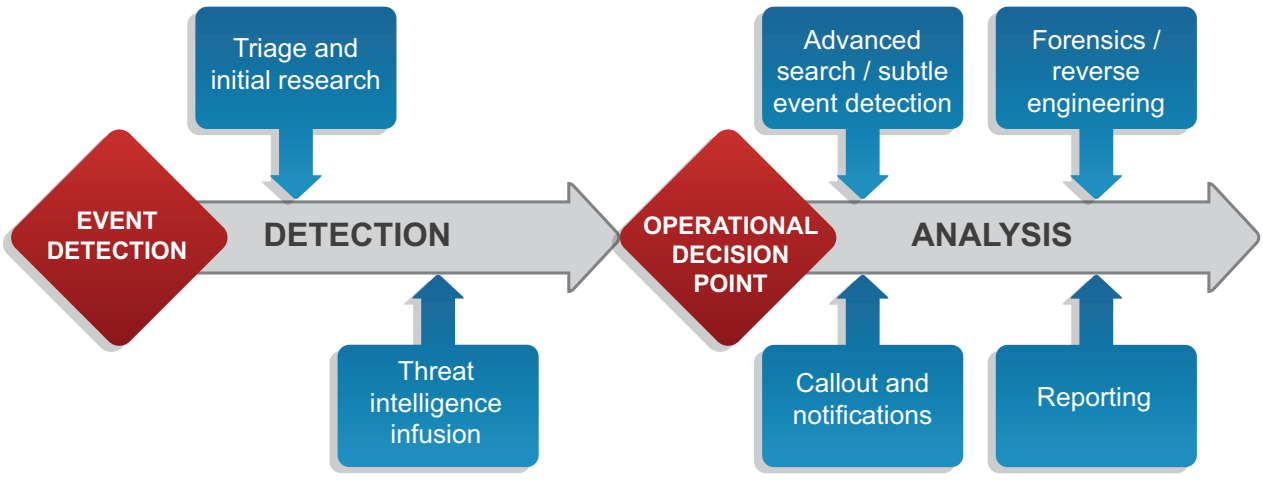

Figure 3: Timeline for event detection through analysis

Procedure Flow

Once SOC processes have been defined, the organization needs to take the next step in outlining the various procedures associated with each process. Each major area of process will have its own procedures. Here is an example from each area:

PROCESS CATEGORY	SOC PROCESS	PROCEDURE	PROCEDURE DESCRIPTION
BUSINESS	Metrics Reporting	KPI Reporting	Outlines the steps involved in reporting the key performance indicators (KPIs) of the SOC.
TECHNOLOGY	System Administration	User Access Management	Details the steps necessary to request, approve, and grant access to the various SOC tools.
OPERATIONAL	Daily Operations	Shift Turnover	Outlines information to be shared and reviewed in shift logs to ensure no information gaps occur at shift change.
ANALYTICAL	Intrusion Analysis	Threat Intelligence	Enumerates the steps the level-2 analysts perform to gather up-to-date cyber intelligence information, analyze it for relevance, and produce a daily report for the analysts to read and leverage in their monitoring role.

Figure 4 gives an example of the relationships among the subordinate procedures. The core procedures documented in the circle should be areas of particular emphasis as these define the basic actions to recognize and respond appropriately to detected malicious events. This also shows how all the supporting business and technology procedures support effective daily security operations.

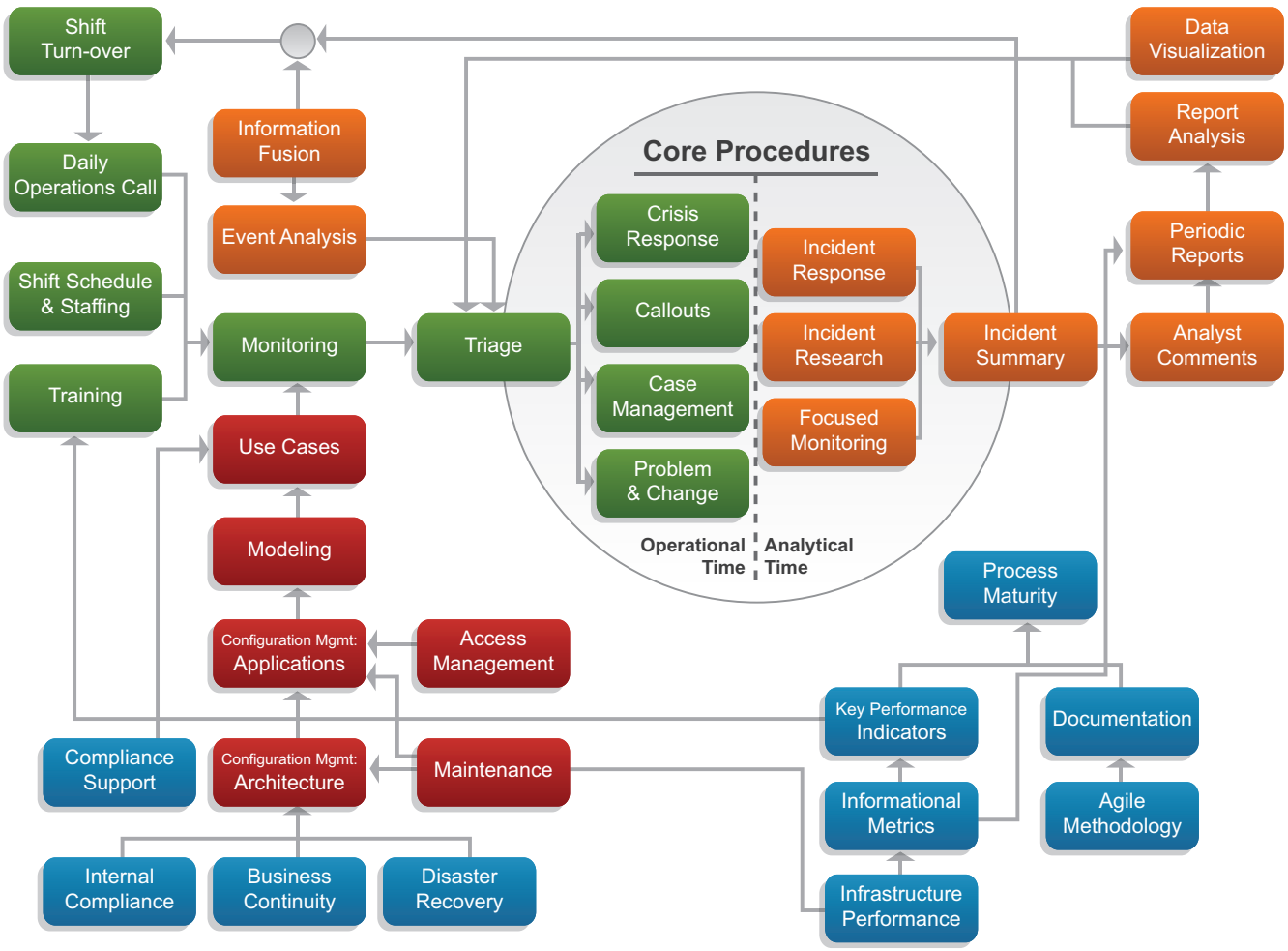

Figure 4: SOC procedure flow

Exercise

A key item on the path to a fully mature SOC is to conduct a full-scale exercise that includes the range of process and procedures and leverages all the internal and external relationships that have been built. There are a number of challenges that can be introduced to see how the SOC functions under considerable organizational and situational stress, such as: Degradation of communications, unavailability of various SOC tools, and condensation of the available time. Once this exercise is complete all involved teams should conduct a group “lessons learned” review and address all identified weaknesses with more training or improved process and technology.

Technology

One of the challenges for security operations is identifying significant events from a large number of heterogeneous security devices and systems, correlating those event feeds, and reducing the overall event volume to a level manageable by the analytical staff. Analysts may have to log in to a number of management consoles to investigate events while the sheer volume of events (e.g., firewall logs) may make it impossible to perform sensible analysis. In order to automate event collection and correlation, SOCs must deploy a Security Information and Event Management (SIEM) solution.

The ArcSight SIEM solution is the premier solution for monitoring, investigating, and responding to malicious events. ESM takes the step beyond storage and alerting to provide real-time monitoring and correlation, historical analysis, and the automated response necessary to manage the higher level of risk associated with doing business in today’s digital world. ArcSight delivers real-time event management and “forensics on the fly,” the ability to drill down from an alert to the source events that triggered the alert.

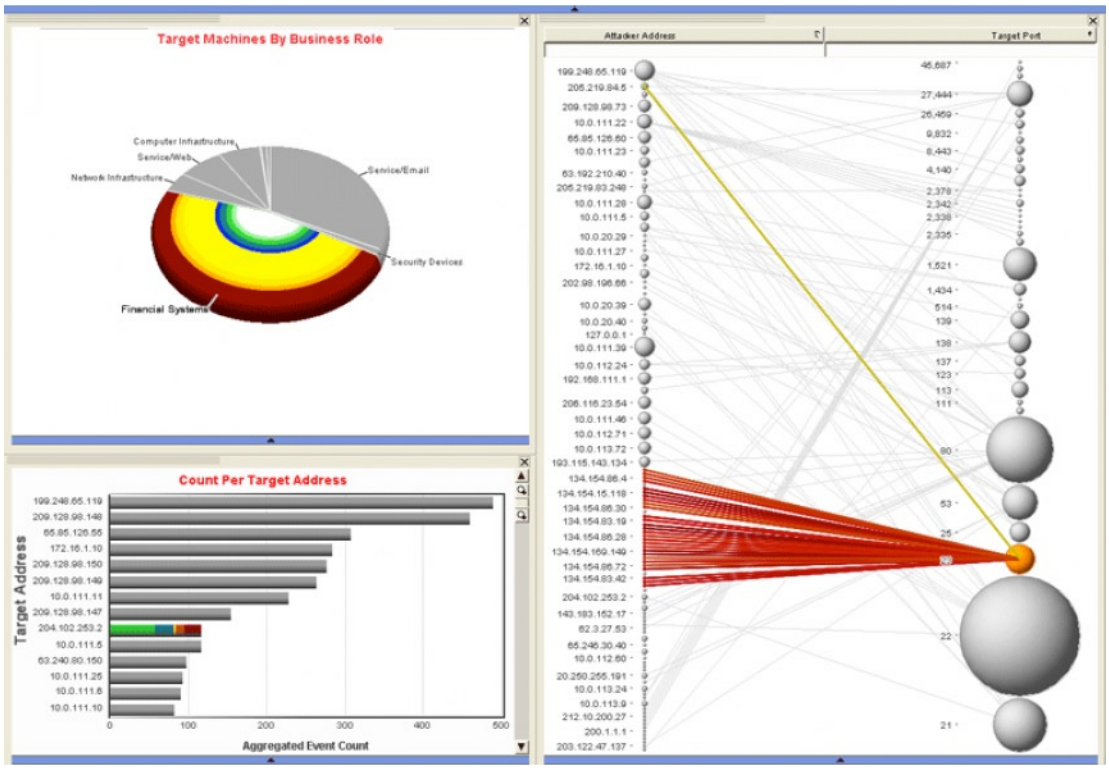

Figure 5: Target analysis using ESM Interactive Discovery

Data Aggregation

ArcSight ESM can collect thousands of events per second, which are stored in a relational database for analysis, display, investigation, and reporting. Data can be collected and aggregated in an agentless fashion by using the ArcSight Manager and deploying various devices and concentrators throughout the network using ArcSight SmartConnectors. This results in several benefits:

- Easy deployment to existing infrastructure without adding additional hardware or re-architecting existing devices and protocols.
- Distributed data collection can utilize a variety of protocols (e.g., Checkpoint, Cisco SecureIDS, any SNMP, any syslog) while working from a central ArcSight ESM platform.
- Secure communication occurs securely over existing IP or IPsec protocols and through firewalls conforming to standard security policies.
- Ability to scale to handle increasingly wider deployments that bring additional sources of information into the system without incremental installation and maintenance.

An important element of the ArcSight ESM data aggregation strategy is a complete capture of the status, alarms and alerts from the various firewalls, intrusion detection systems, and other relevant sources that are being monitored, no matter what topology of agents and centralized collectors is used. This means that every field from every event is available for real-time correlation, display, investigation, and reporting. ArcSight SmartConnectors support hundreds of products and can also:

- Normalize every alarm and alert into a common security schema
- Filter out unwanted traffic
- Set severity according to a common taxonomy
- Intelligently manage bandwidth to minimize network traffic

Data Correlation

While ensuring that the necessary data can be collected and centralized, a successful SIEM technology should also be able to normalize, categorize, and correlate the data across many technologies. In particular a SIEM must be able to accomplish these eight tasks:

- Normalization: A SIEM solution must have a robust data schema. In order to normalize data across many different devices, the solution must provide enough data fields to add all of the necessary information from these devices so it can correlate against them. Without this data capability, a SIEM could not add or integrate with multiple devices from disparate parts of the organization—such as from network devices, security systems, servers, applications, physical access, video analytic systems and environmental controls.
- Categorization: The SIEM should provide an extensible taxonomy to describe events in an easily understandable format, easily group events by writing vendor-independent rules, and the ability to seamlessly integrate new devices.
- Simple Event Correlation: The solution should be able to easily perform event aggregation and look at multiple events to detect something that would otherwise go unnoticed. This basic functionality allows several events to be correlated, producing an outcome that is then re-evaluated against other events in the flow. For example, five attempts to login to a system within one minute using the same user account could be indicative of a brute force login attempt.
- Multi-Stage Event Correlation: The SIEM solution should be able to analyze information from a variety of disparate events—sometimes three or more different events—to determine if they are all related to the same incident. For example, the SIEM should be able to find the relationship between the firewall accepting the attack traffic and the attacked system communicating back out to the attacker. This combination must be picked out of the haystack of millions of events passing through the correlation engine.

- Prioritization: The solution should have the ability to identify the business relevance of the target in question as it relates to the organization's business imperatives. If the target is a revenue-generating system or contains classified data, it should be given the highest priority. If it is a seldom-used system in a lab, it can be placed further down the list to be addressed when the event management team has time.
- Statistical Analysis: A SEIM should have the ability to detect events of significance by identifying mathematical deviations as anomalies from normal traffic such as sharp increases in activity on a particular port, protocol, or event type.
- Historical Analysis: The solution should be able to provide historical or forensic information to help the SOC figure out what might have been missed. This is impossible in solutions without an advanced correlation engine capable of reevaluating past data to look for compromises that may have gone undetected. The potential attacker might also be doing organizational reconnaissance, slowly mapping out the network in preparation for launching a full-scale calculated attack at later time. The SOC needs the ability to detect unusual activity levels for long periods of time before an attack is launched.
- Physical and Logical Analysis/Location Correlation: The solution should be able to perform both physical and logical correlation. The SOC needs the ability to correlate between physical access systems and logical security devices—such as operating system logs or VPN data. This will provide the ability to detect incidents such as account sharing physical plus VPN access violation, a geographic access violation or suspicious physical activity like after hours building access.

Summary

Designing, building, and managing an internal security operations center can dramatically improve an organization's ability to rapidly recognize and respond to malicious information security events. A SOC can also assist in ensuring organizations leverage the full value of the often expensive investment in security technology and meet a myriad of regulatory compliance requirements. Approaching the challenge across the full scope of People, Process and Technology will ensure the SOC is up to the task of effectively and efficiently recognizing and responding to malicious events.