Use offense to inform defense.
Find flaws before the bad guys do.

NOC/SOC Integration: Opportunities for Increased Efficiency in Incident Response within Cyber-Security

GIAC (GCIH) Gold Certification

Author: Nelson Hernandez, nelsonl.hernandez@gmail.com
Advisor: Stephen Northcutt
Accepted: January 26th, 2018

Abstract

Managing, monitoring and defending enterprise networks with siloed Network Operation Centers (NOC) and Security Operation Centers (SOC) is a challenge. Each team running 24/7 incident response, event monitoring/correlation, generating/escalating trouble tickets and up channeling communications which provide an opportunity to integrate NOC and SOC functions. Integrating both teams at the first tier through cross-training, rewriting Standard Operating Procedures (SOP's) with coordination points, standardizing shared and coordinated communications, sharing and integrating dashboards and other data tools as cybersecurity continues to evolve. Adoption of integration as an industry best practice can capitalize on federated data, improve communication, increase visibility and situational awareness, optimize resource sharing and increase efficiencies.

1. Introduction

1.1. What is a Network Operation Center NOC?

A Network Operation Center (NOC) is a command center designed to manage, control and monitor one or more network infrastructures.

- This includes all technology equipment such as servers, switches, routers, firewalls, device management systems, storage systems, database systems, wireless systems, telecommunication systems, Internet of Things (IoT) devices and any other terminal with an IP address. Typically, they are focused on Layer 1-4 technologies...i.e. on the OSI stack.

- A NOC is usually staffed 24x7x365 with personnel who continuously monitor for outages, faults, critical events, and abnormalities within the network.

- The NOC handles issues such as:
  - DDoS Attacks, power outages, network failures;
  - Remote hands support, the configuration of hardware (such as firewalls and routers) routing black-holes;
  - Port management (Opening and closing ports on the firewall to allow the network to communicate with outside servers);
  - Communications with network users when a major incident occurs, impacting network services; and
  - First level triage of network change requests; once validated, they then funnel to the correct team.

- A NOC may also be called IT Operations, Data Center Operations, Operation Management Center, Network Management Center or NetOps, depending on how an organization incorporates this resource.

- The Network Control Center was the first iteration of the current NOC. It has since evolved to encompass all network infrastructure, server and device management, computer operations, vendor management, outside contractor management, project management, deploying improvements and fixes to the network and applications infrastructure (Hertvik/Hertvik Business Services, 2015), ("History of the AT&T Network - History of Network Management| History| AT&T," n.d.), (Department of Defense, 2008).

One important note: A NOC is not a helpdesk. (Shields, B, personal communication, January 8, 2018)

1.2. What is a Security Operation Center SOC?

A (Cyber) Security Operation Center SOC is a team organized to detect, analyze, respond to, report on and prevent cybersecurity incidents within an enterprise network.

- A SOC may also be called Computer Security Incident Response Team (CSIRT), Computer Incident Response Team (CIRT), Computer Incident Response Center (CIRC), Computer Security Incident Response Center (CSIRC), Cybersecurity Operations Center (CSOC) or Cyber Defense Center.

- SOCs are either part of the organization they serve (internal) or (external) Managed Security Service Provider (MSSP) to the organization.

- As per an organization's needs, the SOC may be responsible for a wide variety of tasks, depending on the organization's size, complexity, NOC alignment and whether the SOC itself is insourced or outsourced.

These tasks may include:

- Real-time monitoring and triage;
- Cyber Intel collection, analysis;
- Distribution, creation and fusion;
- Trending, the long-term analysis of event feeds, collected malware, and incident data for evidence of malicious or anomalous activity;
- Threat assessment, incident analysis/response coordination;
- Tradecraft analysis which may include carefully coordinated adversary engagements, whereby SOC members perform a sustained "down-in-the-weeds" study and analysis of adversary Tactics, Technics, and Procedures (TTP), such as a honeypot;
- Countermeasure implementation including firewall blocks, DNS black holes, IP blocks, patch deployment and account deactivation; and
- Forensic artifact handling and analysis, malware and implant analysis also known as malware reverse engineering.

- Other SOC capabilities include:

  - Border protection device operation and maintenance
  - Network mapping to assist risk assessment exercises and exposure reviews;
  - Vulnerability scanning and assessment;
  - Product assessment (Zimmerman/MITRE, 2014);
  - Data leakage monitoring;
  - Reputation and brand protection monitoring – sometimes hand-in-hand with existing in-house compliance or social media monitoring team;
  - Domain/Typo squat monitoring and takedown services;

- IOC (Indicators of Compromise) collection, monitoring and dissemination/integration into existing security tools;
- Anti-DDoS configuration, monitoring and reporting;

1.3. Definition of an integrated NOC and SOC

Integrating a NOC/SOC involves convergence/integration at three levels:

1. Organizational level: (i.e., common first level response) – including triaging, collaborating, cross-correlating and identify common patterns from NOC/SOC respective tools. Combining tier 1 SOC and NOC analyst positions would result in forming one unified set of defenders;

2. System level: (integrate ticketing and workflow) - service level agreements, standard operating procedures, integrating processes and structures in place would allow operators to communicate and coordinate seamlessly; and

3. Asset level: (shared sensors and event criticality information) - utilizing a common information aggregator that collects all the data required and then distributes it using integrated tools and dashboards (Jenkins/IBM, n.d.).

This collaborative integration should result in over-arching company visibility and prioritized risk assessment and agreement, including the following initiatives:

- Event management;
- Security management (antivirus, intrusion detection/prevention systems);
- Endpoint management;
- Network management (firewalls, router, switches, servers);
- Fault management;
- Configuration management;
- Performance management; and
- Accounting (Administration and Identity Access management systems).

Complex issues are investigated by Level 2-3 SOC/NOC specialists to diagnose and pinpoint the nature of the infrastructure incidents more accurately. The integrated staff cross-trains to expand their range of skills, adjust their mindsets and tap each other's skillsets and experiences to identify, manage and resolve incidents effectively (Jenkins/IBM, n.d.).

When an incidence occurs regarding a NOC or SOC specific issue, there is shared accountability and authority between the SOC and the NOC managers on triaging, remediating, handling and making recommendations to stakeholders and system-owners of the respective impacted system.

1.4. NOC/SOC Integration

NOC/SOC integration provides an opportunity for improving communications, increasing visibility/efficiencies, optimizing resources and as such, the tiers and levels associated with this partnership are crucial for the analyst to understand. As stated in "Building a World-Class Security Operations Center: A Roadmap" SOC analysts are a "special group of security professionals" (Torres/SANS, 2015), SOC teams are organized into tiers. Tier 1 Alert analysts are the frontline defenders. "Tier 1 SOC Analysts do alert analysis and continuously monitor the alert queue; triage security alerts; monitor the health of security sensors and endpoints; collect data and context necessary to initiate Tier 2 work" (Torres/SANS, 2015). Integration begins at the first tiers due to their similarities. "Much like the Tier 1 SOC analyst are Level/Tier 1 NOC analyst/engineers who keep their eyes on the network infrastructure and do proactive alarm monitoring 24x7x365. Working issue via their ticket management system per service level agreements (SLA) and identify and work with system fault management." (sic) (Chavan, 2016).

A SOC and a NOC analyst at the tier 1 level have similar yet specialized capabilities. With the vast cost of running a NOC or a SOC and with overlapping (federated) data on network events, system events and endpoint events, there are

opportunities for cost/benefit analysis, case studies and innovations in reciprocal integration.

Additionally, as conveyed by Ministry of Defense (MINDEF) and the Singapore Armed Forces (SAF) technical teams, the rationale and benefits of combining the conventional (NOC) and (SOC) into an integrated Network and Security Operations Centre (NSOC) are as follows:

> According to Hae/SAF, Thong, Matthew, & How "As IT infrastructures grow in size and complexity to meet users increasing operational needs, NOCs and SOCs will need to work closely together to provide a holistic infrastructure and security view of the IT system. Integrating a NOC/SOC will enable better sensemaking and situational awareness which will allow the NOC and SOC to remain effective in addressing monitoring and service recovery challenges amid infrastructure growth and complexity" (Hae/SAF, Thong, Matthew, & How, 2016).

The partnership between NOC/SOC analyst could establish a deeper understanding of roles, risks, threats and security vulnerabilities.

This potential partnership is effective when using collaborative tools such as Splunk Enterprise Solutions with additional add-ons or other similar industry-leading enterprise tools that integrate and automate key Network Operations, and Security Operations functions. The need to lower costs, improve communications, increase visibility, increase efficiencies and optimize resources in both groups are of great value to organizations (Crowley/SANS, 2017).

Some key takeaways from the 2016 SANS Survey on Security Optimization help illustrate why integration is important for future optimization of SOC/NOC environments.

Why integration? Efficiencies that can be achieved by integrating the workflow and data feeds across functions include not re-inventing the wheel, increasing visibility and accountability and providing more accurate detection and reduced false positives. Taken together, successful integration circles back to improving prevention. Better data

integration means that it is easier to mine internal data for threat intelligence and indications of compromise, which also makes it easier to create and implement organizationally specific detections. A more integrated workflow makes it easier to deploy and implement detective capabilities and use them to prevent compromise going forward. As Davidson/SANS states "The same efficiencies can be gained when centralizing data and integrating workflow across these functions are, perversely, the most critical inhibitors to organizations achieving this integration, according to respondents" (Davidson/SANS, 2016).

Per the SANS survey 2016:

- 84% of respondents reported lack of skills and staffing for organizations of all sizes.
- 56% of respondents reported lack of funding and management buy-in, Are the top two impediments keeping organizations from achieving the full visibility needed to prevent, detect, respond to and remediate events on their networks.
- 34% of respondents reported the third overall inhibitor was lack of workflow among prevention, detection, response and remediation programs
- 33% of respondents reported problems resulting from lack of a centralized knowledge aggregation tool (Davidson/SANS, 2016).

Additionally, another reason is career progression as part of the shortage of skilled practitioners which can create a pipeline of talent. Pulling in skilled system administrators, network administrators and individual understanding the incident response process which are cross-trained into the Security Operation creates a much-needed cybersecurity pool of talent for an organization.

Although this portion of the report points out SOC specific integration concerns related to centralizing data and integrating workflow, it also relates to and can be applied to NOC/SOC optimizations/convergence in those areas.

1.5. Similarities and differences

It's important to discuss the similarities and differences because at the first tier the NOC and SOC analyst share similar responsibilities. Some similarities include monitoring events, escalating issues, providing triage on incidents and up channeling communications. As we move up the tiers, the differences in skillset are apparent with Tiers 2 and 3 analysts being expert in their respective fields. Both teams monitor events coming from various dashboards and sensors throughout the infrastructure, utilizing similar tools to maintain vigilance of the enterprise network. The NOC analyst may be using tools that are SNMP/Syslog based alerting system like Nagios, NetXMS, Netcool, HP Openview, Monolith, Zabbix or some other home-grown type tools for event correlation. Similarly, SOC teams receive alerts which may use a more advanced SIEM based on security logs from tools such as Sourcefire/Snort IDS, RSA Security Analytics and Splunk Enterprise Security consoles and dashboards. Additionally, a NOC and a SOC analyst need to have visibility to see systems involved in Fault Management, Configuration Management, Accounting (Administration), Performance Management as well as Security Management (Chavan, 2016).

Some similarities and differences amongst the teams can be seen in the following chart:

NOC support structure	Duties	SOC support structure	Duties
Level 1 support Alert Analyst	Proactive alarm monitoring 24x7| triages network alerts; Issue ticket management per service level agreements (SLA)| Fault management - monitors health of network sensors;	Tier 1 Alert Analyst	Continuously monitors the alert queue; Triages security alerts; Monitors health of security sensors and endpoints; Collects data and context necessary to initiate Tier 2 work
Level 2 support Incident Responder	Higher level support for fault management| Change execution| Root cause analysis| Coordination with Network/Infrastruture Vendors TAC	Tier 2 Incident Responder	Performs deep-dive incident analysis by correlating data from various sources; Determines if a critical system or data set has been impacted; Advises on remediation; Provides support for new analytic methods for detecting threats
Level 3 support Subject Matter Expert	Change validation| Problem management| Coordination with Network/Infrastruture VendorsTAC| Performance Management| Performance monitoring and reporting| Analysis and improvement suggestions	Tier 3 Subject Matter Expert/ Hunter	Possesses in-depth knowledge on network, endpoint, threat intelligence, forensics and malware reverse engineering, as well as the functioning of specific applications or underlying IT infrastructure; Acts as an incident "hunter," not waiting for escalated incidents; Closely involved in developing, tuning and implementing threat detection analytics.
NOC Manager	Manages resources to include personnel, budget, shift scheduling and technology strategy to meet SLAs; Communicates with management; Serves as organizational point person for business-critical Infrastructure incidents; Provides overall direction for the NOC and input to the overall Network strategy.	SOC Manager	Manages resources to include personnel, budget, shift scheduling and technology strategy to meet SLAs; Communicates with management; Serves as organizational point person for business-critical incidents; Provides overall direction for the SOC and input to the overall security strategy.

Figure 1: Similarities and Differences (Torres/SANS, 2015)

As noted, there are numerous parallels between the two fields. In particular, the Tier 1 analyst in the SOC matches up closely with the Level 1 analysts in the NOC. Moving down to Tier 2 and Level 2 support tasks become specialized in both areas. Level 2 is where opportunities exist to differentiate and exclusively utilize the tier team's special skill sets. At Level 3, support personnel and the Tier 3, Subject Matter Experts (SME), these members are deeply involved in the specific subject matter and need to focus on specialized areas to effectively handle/triage/contain network and security incidences. They are the SME's of their particular fields in the NOC and SOC.

There are overlapping infrastructure faults and cyber threats. The lines between them are becoming increasingly unclear as more advance cyber-attacks tend to freely jump between attack surfaces of different IT equipment to cover their tracks and launch attacks. "The Stuxnet computer worm was an example of this type of attack. Having the NOC and SOC collaborate, cross-correlate and potentially identify the common patterns from their respective tools instead of the traditional approach of looking at IT equipment faults and security events monitoring in silos (sic). These anomalous patterns can then be further investigated by Level 2-3 SOC/NOC specialists to diagnose and pinpoint the nature of the infrastructure incidents more accurately" (Hae/Singapore Armed Forces (SAF), Thong, Matthew, & How, 2016).

1.6. Compliance concerns

There are varying concerns when it comes to compliance when a NOC/SOC are integrated because the SOC sometimes has to audit the NOCs activity or task.

The following is part of a discussion concerning compliance with Johanna Ullrich who makes some interesting points especially concerning the potential SOC auditing of NOC.

> "One concern with integrating a NOC and a SOC is there could be some compliance/auditing issues. Integrating the two functions makes a lot of sense, the teams should certainly talk to each other. But in the end, it can be part of the SOC's job to audit the NOC unless there is a specific audit function that is neither part of a

SOC or a NOC (e.g., if both SOC and NOC report to a CISO/CIO, but auditing report up to a legal counsel). In particular, if there is any CISO function or the "head of security" reports to a CTO, then integrating the two can make a lot of sense." (J. Ullrich, personal communication, October 30, 2017).

2. Industries NOC/SOC conversations

In researching this topic, thirty-one industry leaders were polled and ten responses (32 %) were received from various industries ranging from oil and gas, financial markets, cloud management services, real estate, technology services and cybersecurity.

(see Appendix A for conversations information)

2.1.1. Integrations and future considerations

The following is an example of a NOC partially integrated with their SOC and some survey information on potential issues integrating the two teams.

As stated in an article written by Todd Haselton, (2012, July). "A Look Inside AT&T's Global Network Operations Center (GNOC)":

> "At AT&T's global network operations center (GNOC) has always had a focus on security — that much is obvious. Otherwise, the GNOC probably wouldn't need to exist in the first place. But it's also paying closer attention to … security threats or malware that might be stemming from computers and phones, AT&T's executive director of security technology, explained. In a small room that sits inside the GNOC, the Director and other AT&T engineers are working daily to protect AT&T's network against these threats — often by creating custom algorithms that can predict and stop an attack as it happens" (Haselton, T., 2012).

AT&T's SOC sits within the GNOC, and it could be assumed works closely with their GNOC, although they do not appear to be fully integrated.

From a SANS 2017 Security Operations Center Survey: "Responses indicate that SOC's gather, analyze and react to tremendous amounts of information on a daily basis. The key is making it useful for all SOC-related functions and improving integration with network operations centers (NOCs). Right now, only 32% of respondents' report having close integration between their SOC and NOC, with 12% having strong technical integration." (Crowley/SANS-Survey,2017)

According to Jenkins/IBM, "Integrating a NOC/SOC requires convergence and integration at the organizational level (i.e., common first level response), system level (i.e., integrated ticketing and workflow) and asset level (i.e., shared sensors and criticality information)" (Jenkins/IBM, n.d.). These are the three pillars of successfully integrating a NOC and SOC team and covers the necessary levels within an organization.

2.1.2. NOC/SOC integration potential problems

If a network anomaly starts to occur which causes a network slow down or bottleneck on a specific node at a particular location the NOC and SOC will receive different but similar notifications related to the event. These events come in via their respective dashboards, event alert monitors or automated processes or procedures. At what time do the NOC/SOC analysts teams start correlating with each other if that particular event is a network incident or a possible indicator of compromise?

Additionally, if a SOC analyst receives an alert from the SIEM, forensic analyst tool, dashboard or another notification system, what triggers a call or notification to the NOC analyst and at what levels? As two teams that are on the frontlines of handling incidences do, they have processes, procedures and SLAs of when to communicate, what to communicate and how they are going to communicate. Additionally, the NOC is usually focused on getting the company back to operational levels for the business to function, while a SOC is focused on containment and eradication.

Another area of concern is disaster recovery. If the NOC notices a particular site has gone down due to some weather-related issues, a fiber cut or power line cut, what is the correlation or process for notification to the SOC team? The SOC analyst may notice different issues with his tools sensors on a particular node, how long is it going to take him to realize or know to ask the NOC analyst whether there's an issue in a particular location. A NOC analyst may interpret a device outage event as an indicator of equipment failure while a SOC analyst may interpret that same event as a compromised equipment indicator. Beyond the fundamental infrastructure and system technical skills, SOC skillsets are investigative while NOC skillsets are more focused on troubleshooting and recovery. These are all concerns related to the relationship most SOC and NOC have when not truly integrated.

2.1.3. NOC/SOC integration skills alignment/cross-training

Cross training is key to the NOC/SOC integration along with readjusting the first line of the network defenders focus and expanding their situational awareness to encompass a broader spectrum of the network.

As stated by Hae/SAF, Thong, Matthew, & How, 2016:

> "The NOC and SOC staff will need to cross train and adjust their mindsets and mental models. They will also need to expand their range of skills more rapidly and react faster to the increased number of technologies involved" (Hae/SAF, Thong, Matthew, & How, 2016)

(see Appendix B for cross-training information).

The chart below shows one way in which NOC/SOC convergence/integration can work:

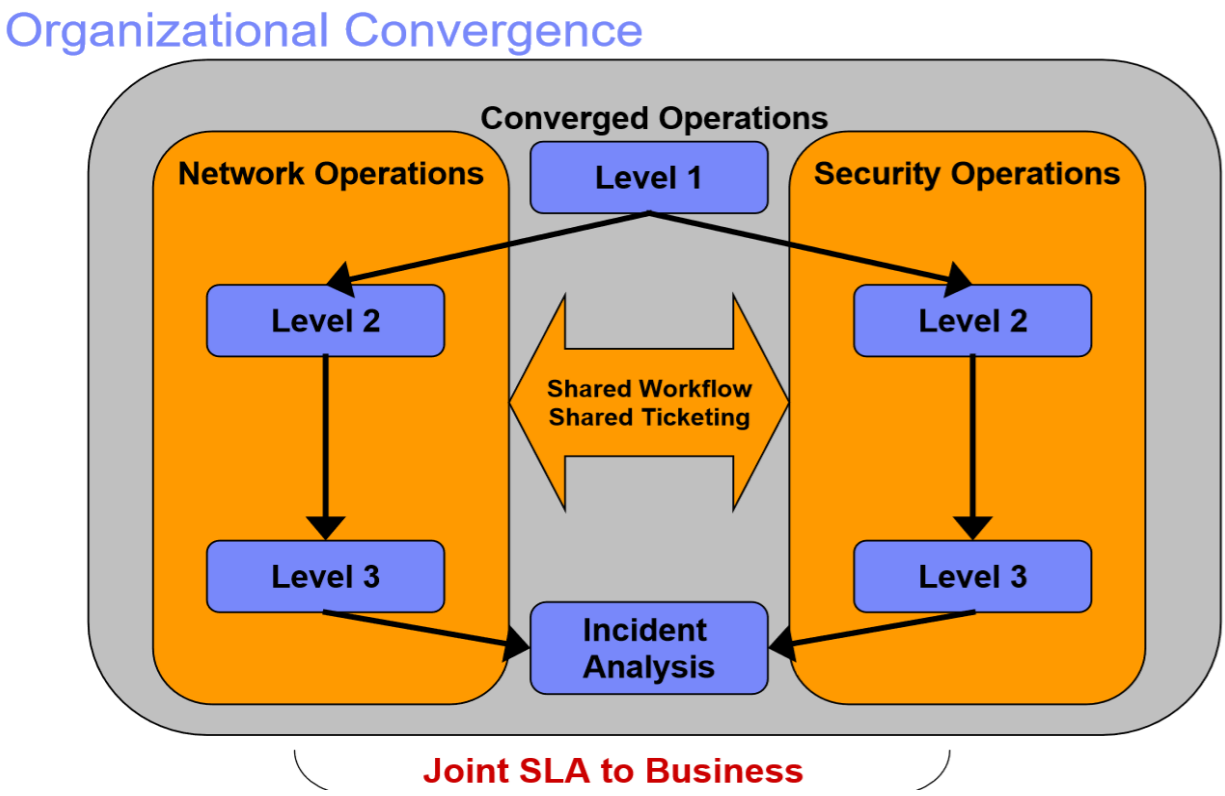

Figure 2: Organizational Convergence (Jenkins/IBM, n.d.)

Author Name, email@address

The illustration below covers some of the relationships concerns current organizations have with SOCs and NOCs.

SOC and NOC

Respondents described the SOC relationship to the NOC in multiple ways. There was separation (43%), which included no NOC, no relationship to the NOC and little direct communication. And there was integration to various degrees: 21% work together during emergencies, 20% work together but are not technically integrated, and only 12% are integrated technically (see Figure 7).

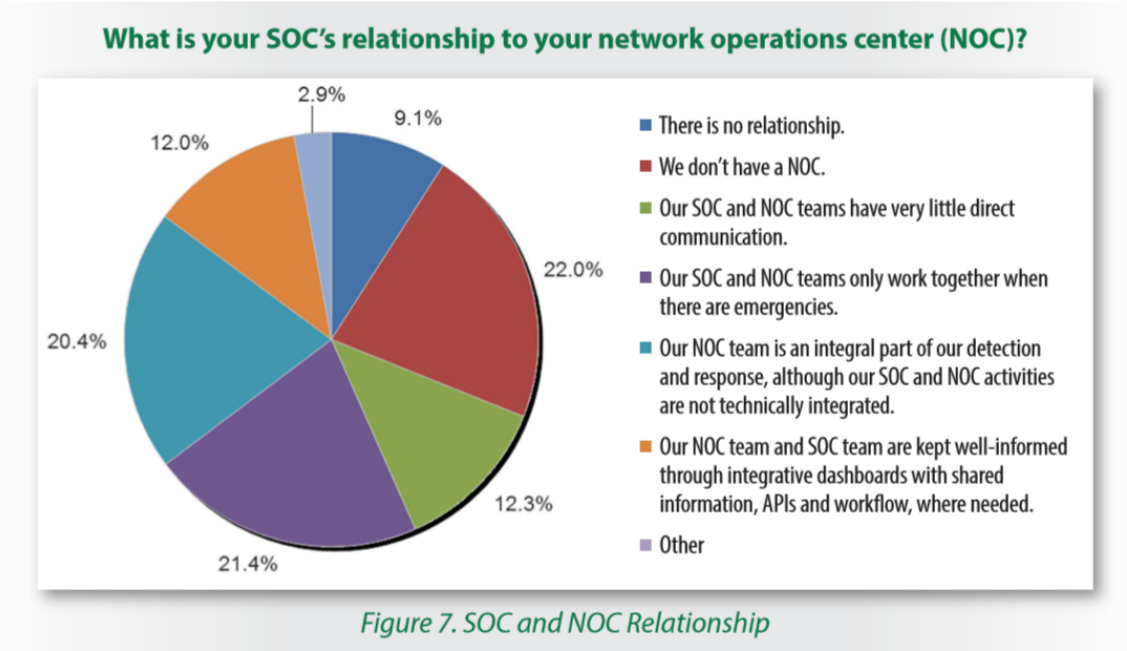

Figure 7. SOC and NOC Relationship

Figure 3: Relationship Concerns (Crowley/SANS, 2017)

The SOC and NOC relationship chart above shows that there are challenges with relationships, integration and possibly management buy-in to integration. The survey shows that 12% are integrated technically while 21% work together during emergencies. Showing that collaboration and integration are starting to gain traction as a way to successfully defend a network. The survey also illustrates that there are still concerns or misunderstanding on how to fully utilize and capitalize on an integrated NOC/SOC.

3. Conclusion

Understanding the complexities of combining/integrating a NOC and a SOC is an issue most Network Ops/Security Ops professionals and management haven't fully addressed. Integration of both groups at the frontlines of defense in many organizations could potentially be the best way to lower costs, increase efficiency and optimize resources. Compliance and auditing issues, as well as information overload (alert fatigue), may be a compelling reason to keep Legal/Compliance teams as well as Infrastructure management leadership involved in any integration discussions.

Integration of a NOC/SOC is starting to gain traction. Adoption of NOC/SOC integration as an industry best practice will likely be determined by factors such as the cost of running two separate teams, response time to initial incident response, collaboration on up channel communications and reporting. As the cybersecurity industry evolves factors such as time to resolution, centralization of workflow/data/dashboards, compliance and auditing concerns should be addressed.

With a phased approach Tier 1 NOC/SOC analyst should be integrated, but for more advanced threats, the SME would still be a Tier2/3 level support person joining forces into a CIRT team that integrates with the SOC.

However, CTO/CIO and Chief Information Security Officers(CISO) will be well served in understanding what a potential collaborative, efficient effort integration brings versus having two separate siloed teams with very little crossing of paths except for at a Lessons-Learned/After-action meeting. The exploration of integrating a NOC/SOC is something every organization should consider.

Author Name, email@address

References

Chavan, S. (2016). *Best practices for building Network Operation Center,* Retrieved October 2, 2017, from https://www.slideshare.net/SatishChavan4/best-practices-for-building-network-operations-center?qid=7b5da316-466d-4af4-8e21-5014a8d15346&v=&b=&from_search=2

Crowley/SANS, C. (2017). *SOCs Grow Up to Protect, Defend, Respond: Results of the 2017 SANS Survey on Security Operations Centers, Part 1*- SANS Institute. Retrieved October 20, 2017, from https://www.sans.org/webcasts/socs-grow-protect-defend-respond-results-2017-survey-security-operations-centers-1-103937/success

2017 SANS Survey on Security Operations Centers, Part 2- SANS Institute. Retrieved October 20, 2017, from https://www.sans.org/webcasts/103942?msc=PR

Crowley/SANS, C. (2017). *Future SOCs: Results of the 2017 SANS Survey on Security* Retrieved October 20, 2017, from https://www.sans.org/reading-room/whitepapers/incident/future-soc-2017-security-operations-center-survey-37785

Davidson/SANS, G. W. (2017, April). *Integrating Prevention, Detection, and Response WorkFlows: SANS Survey on Security Optimization*. Retrieved November 29, 2017, from https://www.sans.org/reading-room/whitepapers/analyst/integrating-prevention-detection-response-work-flows-survey-security-optimization-37730

Department of Defense. (2008). *NetOps for the Global Information Grid (GIG)*

Author Name, email@address

(8410.02). Retrieved December 9, 2017, from www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/841002p.pdf

Eldardiry, O. M., & Caldwell, B. S. (2015, January). *Improving Information and Task Coordination in Cyber Security Operation Centers.* In IIE Annual Conference. Proceedings (p. 1224). Institute of Industrial and Systems Engineers (IISE). Retrieved October 5, 2017, from https://search.proquest.com/openview/0f2f7f6f5ae63ebdfaa19bcd259c66a4/1?pq-origsite=gscholar&cbl=51908

Hae/Singapore Armed Forces (SAF), T. S., Thong, L. K., Matthew, S. N., & How, T. C. (2016). *SMART NETWORK AND SECURITY OPERATIONS CENTRE*. Retrieved November 28, 2017, from https://pdfs.semanticscholar.org/bdfe/b88732213ee20fdd10ebdb237af46f903f7d.pdf

Haselton, T. (2012, July 26). *A Look Inside AT&T's Global Network Operations Center (GNOC)*. Retrieved October 26, 2017, from https://www.technobuffalo.com/2012/07/26/a-look-inside-atts-global-network-operations-center-gnoc/

Hertvik/Hertvik Business Services, J. (2015, March 22). *What Does IT Operations Management Do (ITOps)?*. Retrieved December 12, 2017, from http://joehertvik.com/operations-management/

History of the AT&T Network - History of Network Management| History| AT&T. (n.d.). Retrieved December 12, 2017, from https://www.corp.att.com/history/nethistory/management.html

Author Name, email@address

Jenkins/IBM, D. (n.d.). *Secure Your Operations through NOC/SOC Integration - PDF*. Retrieved November 28, 2017, from http://docplayer.net/2408670-Secure-your-operations-through-noc-soc-integration.html

Karnam/HP, S., & Feldman/HP, A. (2014). *Top 10 tips for effective SOC/NOC collaboration or integration*. Retrieved October 5, 2017, from https://www.slideshare.net/sri747/top-10-tips-for-effective-socnoc-collaboration-or-integration

Kelley, D., & Moritz, R. (2006). *Best Practices for Building a Security Operations Center.* Information Systems Security, 14(6), (p. 27-32). Retrieved October 29, 2017, from http://www.tandfonline.com/doi/abs/10.1201/1086.1065898X/45782.14.6.20060101/91856.6

Meierdirk, A. (2012). *Best practices for developing and implementing the right monitoring framework: Next-generation network operations center*. Retrieved November 28, 2017, from http://www.remotemagazine.com/conferences/wp-content/uploads/2012/09/INOC.pdf

Metzler/Ashton, Metzler & Associates, J. (2008). *The next generation network operations center: How the focus on application delivery is redefining the NOC*. Retrieved November 28, 2017, from http://www.webtorials.com/main/resource/papers/NetQoS/paper13/NextGenerationNOC.pdf

Author Name, email@address

Rothke/Wyndham Worldwide Corp, B. (2012). *Building a Security Operations Center (SOC)*. Retrieved November 28, 2017, from http://www.rsaconference.com/writable/presentations/file_upload/tech-203.pdf https://search.proquest.com/openview/0f2f7f6f5ae63ebdfaa19bcd259c66a4/1?pq-origsite=gscholar&cbl=51908

Scarfone, K. A., Grance, T., & Masone, K. (2008). *Computer security incident handling guide.* NIST Special Publication, 800(61), p. 38. Retrieved October 23, 2017, from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Siponen, M. T. (1999, August). *Four Approaches to Construction of Information Security Guidelines.* In Seminar in Scandinavia (IRIS 22):" Enterprise Architectures for Virtual Organisations (p. 157). Retrieved October 5, 2017, from http://iris22.it.jyu.fi/iris22/pub/Siponen_R270.pdf

Torres/SANS, A. (2015). *Building a World-Class Security Operations Center: A Roadmap.* Retrieved Oct 1, 2017, from https://www.sans.org/reading-room/whitepapers/analyst/building-world-class-security-operations-center-roadmap-35907

Zimmerman/MITRE, C. (2014). *Ten Strategies of a World-Class Cybersecurity Operations Center*. Retrieved December 12, 2017, from https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf

Author Name, email@address

Appendix A

Industries NOC/SOC conversations

The three topics addressed were:

1. If NOC and SOC are integrated what are the effects on their enterprise?
2. If they're not integrated what are the issues or reservations enterprise leader have for not integrating?
3. Additionally, if not integrated are the reasons compliance or audit related?

Here are some of their responses:

CIO/CTO, Oil and Gas industry

"... it was more cost effective for us to contract with a 3rd party SOC as a service model. There was little to no interaction with the NOC other than the occasional sharing of trouble tickets. There was a separate security incident response process and a separate ITIL based incident response process from the typical application and infrastructure incidents."

Analysis: MSSP is used as well as internal CIRT (Computer Incident Response Team) in place of NOC/SOC integration which works for this firm. This would indicate a small mature IT team with specialized skills in their particular field. With their SOC outsourced integration may not be needed.

Head of Infrastructure Services, Solutions provider to hedge funds, asset managers, brokerage firms and banks industry

"…I've not seen them integrated to date mostly due to the different skill sets of understanding break-fix alerts in the NOC and the trend analysis and anomaly detection

of the SOC. A NOC tech is more likely to ignore an alert that he frequently sees as a false alarm. The SOC has to analyze each occurrence to see if it's an intruder masquerading their activities as semi-normal things... i.e., a port scan is fairly common but if you detect a series of port scans that may require investigation." (sic)

Analysis: Cross training would bring a better understanding of their TTPs. Use of shared dashboard would increase their situational awareness. The teams are siloed, so visibility is limited.

Director of Engineers and Security, Cloud Services provider industry

"...a year ago, our SOC team was completely siloed. We had experienced a major virus attack, and things did not go so well. In a nutshell, the SOC team failed to coordinate and communicate with the NOC. This delayed the team 24 hours in remediating the issue. Our customers were not happy with the delays caused by the disruptions. We have since begun an integration process between both teams and moved the SOC within the NOC." (sic)

Analysis: This organization is capitalizing on their teams NOC/SOC SMEs at the tier 2-3 levels which are integrated. There tier 1, NOC and SOC analyst are not integrated. This is an option, but they may need assistance at the tier 1 level with SOPs and up channel trouble tickets.

Chief Information Security Officer, Global Financial (alternative asset managers and market makers) services industry

"…Tradition SOCs looked at layer 3 / 4 events like DDoS and Firewall blocks, etc…so they were embedded since they were the same team as the SOC.

With more sophisticated attacks, the last 2 companies I worked for decoupled the SOC/NOC. The SOC is more rebranded as a "Cyber Defense" or as you mentioned an "IR" team…since SOC is a bit dated turn that people still think is more operationally

focused. Most IR teams now also may have hunting components and Intel as you mentioned below.

Typically, you will still see the NOC do some triage on the L3/L4 events, but pass it off to the security folks beyond that.

In both roles I see a dedicated security team doing the engineering, but on the L3/L4 platforms (firewalls/proxy, etc.) they pass that off to NOC/SOC type function.

Issues: I see some issues with escalation times. Sometimes you see a gap in the time to escalated. Also since the teams may not be under the same hierarchy, you see instances of finger pointing or where a team may choose a solution that another team just has to accept without pushback."

Analysis: Integrating at the 1st tiers SOC/NOC and with management by in for both teams in SOPs and SLAs would help the two past firms mentioned above. Using the model listed in this paper with tier 2 and 3 breaking out and doing a more specialized analysis of incidences would optimize their respective skillsets.

CIO & Partner, Technology Leadership-as-a-Service (TLaaS) industry

"... In my experience, they generally are integrated. Mostly due to the management of a lot of false positives and dialing in the security and the alarms. Also, the NOC are the only ones who can translate what's happening most of the time. Also, if the organization is going through a lot of change or has a lot of change, this can result in the alarms. There's also the question of integration with change management and the ability to deal with how tight security is on various systems when changes do occur. All this, of course, boils down to the kinds of security that's in place, the tools, the procedures, processes, and people (culture). The one exception that I would say that is kept outside the SOC or NOC is using external auditors/consultants for PEN testing, etc. That's something I usually keep outside for a clean perspective and testing." (sic)

Analysis: The change management process is one of the important reasons to integrate or a least have the visibility into infrastructure moves, adds and changes.

Especially if there is a lack of security review in new or updated technologies, hardware and software.

Information Security Manager, Network Security industry

"…depending on organizational culture can benefit from the integration of Level 1 of NOC and SOC. Highlighting that success for integration is needed at all levels as well as defining roles and responsibilities, making sure the NSOC has a voice in the tools used as well as how they are configured. Even processes such as incident response can benefit from individuals with a NOC and SOC background checking the various tools since they look at things from different perspectives.

As for auditing/compliance, I would look at the reporting the Information Security team provides, such as metrics, as well as internal and external audit teams to validate what is in place and help suggest improvement/growth with people, processes, and technology.

For me, the ultimate criteria for success are trust in the people to be open and honest on communications as well as a thirst for knowledge between the positions.

Analysis: These comments are right in line with the concept of NOC/SOC integration at the Tier 1 level. Using metrics to validate auditing/compliance is a compelling suggestion for improvement of the integration process.

So, the question as to whether to utilize an integrated NOC/SOC comes down to the following. "The need for increased collaboration on event management, situational awareness of Security Management (antivirus, intrusion detection/prevention systems), Network Management (firewalls, router, switches, servers), Fault Management, Configuration Management, Accounting (Administration- identity access management systems) as well as Performance Management." (sic) (Chavan, 2016) Additionally, there is a need to align or address regulatory compliance or auditing concerns (i.e., ISO2700, NIST, COBit, PCI DSS, Sarbanes-Oxley (SOX), FISMA or SOC 2) and discretionary alignment issues with management.

Appendix B

NOC/SOC integration skills alignment/cross-training

The NOC analysts will need to cross train on SOC topics that encompass the following procedures, which can be gained via various training (on-site, online or conference) including some On the Job Training (OJT) experiences:

1. **Cyber-Security Alert Triage procedures.**
2. N**etwork Intrusion Detection and Prevention.**
3. **Host-based investigative training.**

The NOC analyst will also need to think outside the box and think like the adversary hunt for anomalous and malicious activity while learning the SOCs TTPs. Additionally, according to (Zimmerman/MITRE, 2014), SOC/NOC analyst should have a "passion for the job, regardless of the position. Intrusion monitoring and the response is not just "a job" where people put in their eight- or 12-hour shift, collect a paycheck, and then leave. When it comes to "cyber," we're looking for enthusiasm, curiosity, and a thirst for knowledge. This passion is what will keep them coming back to the job, day after day, despite the stress and challenges inherent in operations. This passion, along with intellect and other soft skills, is what propels fresh recruits into becoming what we will call "rock-star analysts." This sums up some very specific qualities the NOC analyst must strive to attain while wearing both hats at the helm of monitoring (Torres/SANS, 2015) (Zimmerman/MITRE, 2014).

The SOC analysts will need to cross train on NOC topics that encompass to some degree the follow, which can be gained via various training (on-site, online or conference) with a majority coming from On the Job Training (OJT) experiences:

1. **Monitoring network health**
2. **Server Management**
3. **System Admin Operations**
4. **Communications with network users** when a major incident occurs impacting network services.
5. **Disaster recovery procedures**
6. **Change Management**

The SOC analyst will also need to correlate network faults/events with change management activities and understand the ramifications for the impacted business groups when communicating issues. They will also need to work hand in hand with on-call technical leads from various sysadmin teams to adjust erroneous configuration or failing devices while learning the NOCs TTPs.

After both teams receive cross-training in SOC and NOC specific topic, the teams will need to confer with one another and discuss specific methods and TTPs each team uses to meet their objectives. This will fortify what they have learned and help bond the tier 1 analyst (Hertvik/Hertvik Business Services, 2015).

Last Updated: July 22nd, 2018

Upcoming SANS Penetration Testing

SANS Pen Test Berlin 2018	Berlin, Germany	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS vLive - SEC560: Network Penetration Testing and Ethical Hacking	SEC560 - 201807,	Jul 24, 2018 - Aug 30, 2018	vLive
SANS Pittsburgh 2018	Pittsburgh, PA	Jul 30, 2018 - Aug 04, 2018	Live Event
San Antonio 2018 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	vLive
SANS Boston Summer 2018	Boston, MA	Aug 06, 2018 - Aug 11, 2018	Live Event
Security Awareness Summit & Training 2018	Charleston, SC	Aug 06, 2018 - Aug 15, 2018	Live Event
SANS San Antonio 2018	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	Live Event
Mentor Session - AW SEC560	Austin, TX	Aug 08, 2018 - Oct 10, 2018	Mentor
SANS Northern Virginia- Alexandria 2018	Alexandria, VA	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS New York City Summer 2018	New York City, NY	Aug 13, 2018 - Aug 18, 2018	Live Event
Northern Virginia- Alexandria 2018 - SEC542: Web App Penetration Testing and Ethical Hacking	Alexandria, VA	Aug 13, 2018 - Aug 18, 2018	vLive
Northern Virginia- Alexandria 2018 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	Alexandria, VA	Aug 13, 2018 - Aug 18, 2018	vLive
SANS Krakow 2018	Krakow, Poland	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Chicago 2018	Chicago, IL	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Prague 2018	Prague, Czech Republic	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VA	Aug 20, 2018 - Aug 31, 2018	Live Event
Mentor Session - SEC504	Cincinnati, OH	Aug 21, 2018 - Oct 02, 2018	Mentor
Mentor Session - SEC542	Denver, CO	Aug 23, 2018 - Oct 25, 2018	Mentor
SANS San Francisco Summer 2018	San Francisco, CA	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS SEC504 @ Bangalore 2018	Bangalore, India	Aug 27, 2018 - Sep 01, 2018	Live Event
Mentor Session AW - SEC504	New York, NY	Aug 27, 2018 - Sep 17, 2018	Mentor
SANS Copenhagen August 2018	Copenhagen, Denmark	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, Japan	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Wellington 2018	Wellington, New Zealand	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FL	Sep 04, 2018 - Sep 09, 2018	Live Event
Mentor Session AW - SEC560	Chantilly, VA	Sep 05, 2018 - Sep 12, 2018	Mentor
Threat Hunting & Incident Response Summit & Training 2018	New Orleans, LA	Sep 06, 2018 - Sep 13, 2018	Live Event
SANS Baltimore Fall 2018	Baltimore, MD	Sep 08, 2018 - Sep 15, 2018	Live Event
Threat Hunting & IR Summit - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	New Orleans, LA	Sep 08, 2018 - Sep 13, 2018	vLive
Community SANS Toronto SEC504	Toronto, ON	Sep 10, 2018 - Sep 15, 2018	Community SANS
SANS Alaska Summit & Training 2018	Anchorage, AK	Sep 10, 2018 - Sep 15, 2018	Live Event