Hewlett Packard Enterprise

Business white paper

Growing the Security Analyst

Hiring, training, and retention

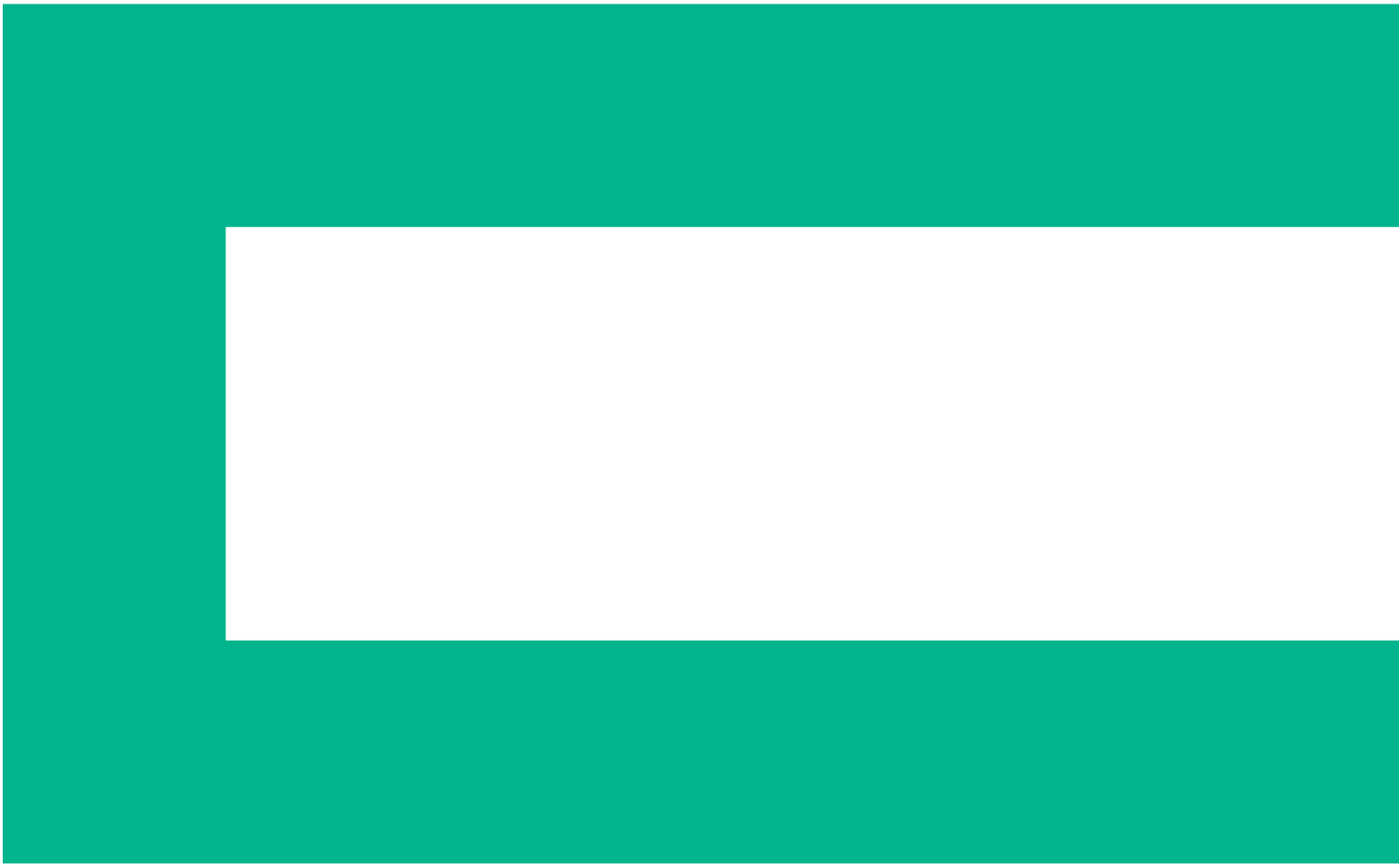

Table of contents

Introduction

The good guys at the front line of defense for many organizations are the Security Analysts within the Cyber Defense and Security Operation Centers (SOCs) of the world.

At their best, these guys understand how the adversary thinks, what they are after, and what methods they use. They also understand their own networks, the assets on those networks, what matters to the business, and how systems and people behave. They understand how operating systems work, can disassemble a TCP-IP packet in its binary form and spot the bytes that are out of place. They understand the protocols and routing and services they are protecting, and the policies and standards they are enforcing.

Good guys are tireless problem solvers that rejoice in following symptoms to their cause, can communicate in written and verbal forms across all levels of the organization, are advanced in using a wide variety of tools and techniques, work well in a crisis and under stress, and are vigilant and consistent in the execution of their duties.

There are certain truths about Security Analysts:

- Nearly every business is trying to hire them.
- Any business who has one is trying desperately to keep them.
- There are many job seekers lacking the ability to execute as a security analyst.
- Many organizations have an incomplete understanding of what caliber of good guy they actually need.

In this paper, we will explore the aspects of recruiting, training, and retaining security analysts. A blueprint will be provided for how to find and assess candidates, how to nurture analysts during employment, and what sorts of opportunities should be granted to security analysts to help with job satisfaction and ultimately effectiveness and retention.

Industry-wide problem

As a provider of industry-standard software that powers the core of most of the world's SOCs and with the world's most accomplished SOC consulting practice, Hewlett Packard Enterprise has a keen understanding of the challenges that organizations face in staffing Security Analysts. For organizations attempting to build a SOC for the first time, or those expanding their SOC's capability or coverage, staffing the right people is arguably the most critical aspect of the people/process/technology puzzle. Hiring experienced analysts from the marketplace presents a number of challenges, especially for a new organization that has not yet established a critical mass of positive culture and established processes. There is a broad disparity in the quality of existing SOCs in the marketplace. While analysts coming from existing SOCs arrive with valuable experiences, they also come with baggage. If you build a full team of these individuals, the result is often conflict and inconsistency. While being a security analyst can be an exciting and flexible role, there is need for operational consistency and predictability, otherwise it can wreak havoc on the performance of the SOC. Also, experienced analysts in the market are seeking career progression and are not interested in another Level 1 Analyst role. Since we know organizations are working very hard to keep their top-performing analysts, there is a chance that those with SOC experience who are actively seeking Level 1 Security Analyst roles are not the top performers on their team.

Many successful SOCs cultivate their own analysts through rigorous development programs.

According to a white paper published in 2013 by $(ISC)_2$, Booz Allen, and Frost & Sullivan[1], when respondents were asked which job title was undergoing the most extensive workforce shortage, 47 percent chose the security analyst. Many companies are realizing that the need for this type of position, or even a SOC function, is mandatory. The current supply of skilled, analytical, interested, and curious analysts cannot meet that demand. There are few college programs that wrap a curriculum around detecting and handling security incidents, and commercially available training programs fail to link theory and knowledge to real-life experience in an organization. Many successful SOCs cultivate their own analysts through rigorous development programs that include a mixture of formal, on-the-job, and custom training.

[1]The 2013 (ISC)$_2$ Global Information Security Workforce Study, Frost & Sullivan, 2013

The US Federal Bureau of Investigation (FBI) may consider removing requirements for clean marijuana drug tests for cybercrime positions in an effort to not further diminish an already shallow talent pool. Read more.

IT systems are ubiquitous to modern organizations and IT transformation is constant. These transformation projects are notorious for leaving artifacts of the old shape of IT online—the result is an ever-expanding attack surface with increased complexity. The complexity of the attacks and time to resolve most cyber-attacks leaves companies struggling to find the resources to respond. While vendors are continuously creating tools and technologies to strengthen our defenses, the technology alone does not solve the problem. As companies become more aware of the threat landscape and the true risks of cyber-compromise, they are finding that they lack the experts to truly utilize the tools at their disposal. When it comes to finding indicators of compromise, they are unable to execute effective security analytics and manage the sheer volume of information involved. Hiring and retaining experienced security professionals is an ongoing challenge for most organizations.

There should be a clear definition of roles and responsibilities within the SOC and methods to hold individuals accountable for those responsibilities.

Job roles and skills definition

There should be a clear definition of roles and responsibilities within the SOC and methods to hold individuals accountable for those responsibilities. Security issues can become catastrophic when individuals assume that a task is someone else's responsibility. The most painful After Action Review (AAR) of security breaches often point back to failures in common understanding of roles and responsibilities for tasks associated with the incident response. To address this, document the roles and responsibilities of all positions involved in investigating and responding to a security incident. This can be a long list:

- Level 1 & 2 Security Analysts
- Incident Handlers
- Security Engineers
- SIEM Content Authors
- System Admins
- Network Admins
- Management of all levels
- Human Resources
- PR/Legal

Using a RACI matrix can help identify roles and responsibilities.

Description	Security Strategy & Architecture	SOC Manager	SOC Level 2	SOC Level 1	Threat Intelligence	SOC Business Office	Security Engineering	System Owner	System Administrator	Incident Responder	Human Resources	Public Relations	Legal	Compliance & Audit
Identify threats via monitoring and analysis of information	C	A	R	R	R	I	C	C	R	C	C	C	C	I
Actively searching historical logs for suspicious activity	C	A	C	C	R	I	C	C	C	C	C	C	C	I
Generating reports for audit purpose	C	I	R	R		I	R	Y	R	R				A
Creation of SIEM content	C	I	I	I	I	I	A	C	I	I	I	I	I	I

Figure 1. Example of a RACI matrix. R=Responsible, A=Accountable, C=Consulted, and I=Informed

Security analyst role attributes
- Description
- Required skills
- Feeder positions
- Assessment
- Development plan
- Career progression

Blogs on security
- KrebsOnSecurity
- PaulDotCom
- HPE Security Research Blog
- Contagio malware dump
- Tao Security
- Darknet
- Sans cyber defense
- ThreatPost

Once these job roles and responsibilities are defined for the SOC, they must be continually enforced.

Skills definitions need to be created for all roles in the organization, especially for security analysts. These skill definitions will set expectations and document the scope of a particular job role as well as skills required for an individual to be qualified to fulfill the role. Each skill definition should set a minimum skill threshold for the role which can be used in evaluation of entry-level candidates. In turn, regular skills competency assessments should be conducted and results used to create individual development plans and to measure growth against those plans.

Each role in the SOC should have both feeder positions as well as career progression positions identified and documented. This is necessary for goal-setting as well as retention purposes. The more an individual knows how they may progress from one role to another, the more likely they are to set and attain their career aspirations.

Grow your own analysts

When there is such a shortage of talent available to hire in the market, the best option is often to "grow your own" analysts. This is not a quick and simple endeavor – you need to start with candidates who have the right mindset and aptitude, make the necessary investments into the analyst, and provide an environment where the analyst can be successful and truly commit to a full analyst training program.

Your top candidates will have a strong foundation in at least a few of the desired end-state characteristics and gaps filled with training and education through the SOC development program to create a complete package. Keep in mind that certain characteristics are easier than others to develop. Above all, the most desirable candidates will have the right attitude and demonstrate the right aptitude for the job. When working with people who have the right mindset, teaching technical skills is relatively trivial. Developing a logical and curious mind, a strong work ethic, business acumen, or communication skills will likely take much more time. Don't start with people with no understanding of IT, but keep an open mind when interviewing analysts. The staffing of a Security Analysis team is like a puzzle, and each individual hired needs to fit with the team dynamic as well as have skills and experience that complement and augment those of the other team members. Each shift should have the necessary skills as a composite, even when the individuals alone might not have everything.

Interest levels must also be assessed. In order for an analyst to be successful, they must have the ability to continually improve themselves both on and off the job. The more effective security analysts will persistently immerse themselves in the security ecosystem. For example, they will keep up with current cyber-security news, will have favorite security blogs or feeds, will read security related books on the side, pursue certifications, and most likely have a lab environment at home in which they experiment with technology and offensive and defensive tactics. These levels of interest can be assessed at the time of the interview. Simple questions such as, "What are some of your favorite security blogs or feeds?" or, "What kind of setup do you have at home?" can reveal their overall level of interest outside of the job.

Organizations are finding these future analysts in a variety of places—and recruiting from multiple pools is necessary. Here are some common places to find security analyst candidates:

Consider looking at your internal IT organizations first

People within your own organization often have a solid IT background to build upon as well as an understanding of your organization or infrastructure. This includes network operations, IT support, and system admin roles.

Desktop support/PC support

These candidates have experience troubleshooting multi-faceted problems, often while under stress, and dealing with "customers" directly.

Recent college graduates
Often these individuals will have a good foundation of IT understanding and, perhaps more importantly, they will have a hunger and ambition to start their professional career. Be cautious not to staff too many of your positions with these new hires. They often need mentoring from more experienced professionals to grow and thrive appropriately.

Military veterans
The discipline and reliability of veterans is hard to match. In addition, many fields within the military, from signals and intelligence to field IT, teach very relevant skills and thought patterns.

Law enforcement
Similar to the above, these individuals will have the right mindset to solve problems and a familiarity with the concept and importance of protection.

Local user groups
ISSA and FIRST groups are examples of industry communities where skilled and motivated individuals will collect.

LinkedIn groups
There are SOC and cyber defense communities in LinkedIn that have hundreds of members, and if you're reading this paper, there's a good chance that your forward-thinking can inspire a few of the good ones to join you.

Work with your vendors
Sales account managers for IT security products and Enterprise Security services are networked to the hilt. It's a key part of their job. Let them know what you are looking for and there is a good chance that they can help you make solid connections.

Get help
Consider reaching out to your IT partners to explore expert staff augmentation or job placement services. Many of HPE's SIOC customers have had significant success taking advantage of a contract-to-hire model for analyst staffing.

The skills assessment is typically a self, peer, or third-party assessment and is driven by a combination of questionnaires or tests.

Skills assessments

In order to accurately measure an analyst's skills, both before and after hire, skills assessments must be performed. This will enable SOC personnel to correctly gauge individual strengths and deficits in relation to the needs of their role.

The skills assessment is typically a self, peer, or third-party assessment and is driven by a combination of questionnaires or tests, resulting in the output of a detailed score for competency of each skill. This score places the individual into a category, which will in turn let the SOC personnel know the level of expectation. For instance, a Level 1 Analyst will have a lesser overall score than a Level 2 Analyst.

After the skills assessment is performed and the individual is ranked, identified weaknesses should translate into action items for development. Preparing action items out of the areas that the analyst displayed lower competency allows the items to be inserted into annual goals and development programs. The analyst's current competency status is measured through the skills assessment and thus, can be used to define where the analyst needs to be at the same time the following year. Another facet of knowing the competency level is that training needs can be assessed. Combining the annual goals and training based on the current competency levels encourages a steady and guaranteed growth in the analyst. When review time comes again the following year, another skills assessment is performed along with an assessment of the goal achievements from the previous year. By assessing the goal achievement, both the analyst and the SOC management can visualize the amount of growth seen from the analyst. Accurately measuring the amount of growth and allowing the analyst to grow as a professional has immensely beneficial side effects. These side effects include higher levels of performance, better employee engagement, and more accurate and intuitive analysis.

The HPE Security Intelligence & Operations Consulting (SIOC) team has developed this framework for performing security analyst skills assessments:

Skill levels:

0	**No practical knowledge or experience within the defined area.**
1	**Beginner.** Basic foundational knowledge with no experience. Can perform limited tasks using pre-defined procedures.
2	**Intermediate.** Working knowledge with 1-2 years' experience. Power user. Can perform daily responsibilities but relies on expert for more advanced tasks.
3	**Expert.** Advanced knowledge with 3+ years' experience. Practical administrative experience. Can manage architecture, configuration, health and availability issues, and lead others to perform those tasks.
*****	**Certification completed.** Completion verifiable via public website, certificate, or other mechanism.

Sample analyst skill descriptions:

Skill	Skill level 1	Skill level 2
Anomaly detection	Basic understanding of baseline data sets and identification of non-conforming data.	Able to apply anomaly detection concepts utilizing thresholds and statistics derived by more advanced analysis.
Data loss prevention (DLP)	Familiar with basic DLP concepts and popular products. Able to recognize priority alerts and escalate.	Understanding of DLP engine, rule sets, and operations. Can perform basic DLP tuning procedures based on findings.
Data Integrity/File Integrity/Host intrusion prevention service (HIPS)	Knowledge of system security and data integrity concepts used to monitor and alert on data, file, and system changes.	Experience configuring OS specific host policies to identify, monitor, and alert on data, file, and system changes.
Digital forensics	Basic understanding of forensics concepts as they apply to digital attacks and evidence handling.	Demonstrated knowledge and experience conducting forensic investigations and solid understanding of evidence, chain of custody, and its application to security operations.

Analyst development

Once you have found the candidates with potential, and you know the skills that they need to fill their job role, you need to have a plan to fill in the missing pieces. While there are a number of great commercially available training programs and certifications for different aspects of IT security, it takes a custom and focused effort to make a great security analyst for **your** organization.

The HPE SIOC practice has created an Analyst Development Framework to develop highly effective analysts. This framework brings a robust syllabus of topics and a structure for lecture, study, exercises, and on-the-job mentoring and is adapted to meet a specific company's needs.

High level topics for this Analyst development program are below:

- Organizational introduction
- Analytical thinking (Psychology)
- Boolean logic
- Communications (written, verbal, and presentation)
- Intrusion analysis
- Packet analysis

- Information security principles
- UNIX® fluency
- Windows® fluency
- Network fluency
- Basic scripting
- Research skills
- Tools (Wiki, SIEM, etc.)
- Use cases and business context
- SANS GCIA boot camp and certification preparation

The HPE SIOC team uses a Wiki platform to store training materials and track progression through the program by analyst.

Measuring the work is not as important as the work itself.

Operational metrics

Skills assessments will help tell you how well equipped security analysts are for the job, but how do you know if they're putting that to good use? This can be done through the use of operational metrics. Operational metrics give management a view into the effectiveness and efficiency of the operation. The information that is gleaned from these metrics is a key portion of the continual measurement and improvement process that a healthy SOC needs to maintain. Assessing analysts in this fashion can be a tricky and cumbersome task. Operational metrics can be used as a gauge to drive behavior or measure analyst contribution, or they may be hazardous destructive to the culture and productivity of the SOC. A SOC needs to collect sufficient operational metrics to assemble a reasonably complete picture—focusing on too small a set of metrics creates a distorted view of operations. SOC managers should be careful to not allow the metrics collection process to become overly cumbersome—measuring the work is not as important as the work itself. Also be cautious to not waste time chasing down normal variance in your metrics.[2]

Metrics-Team Dashboard

ID	Metric	Current Period			Trend	Status
		Daily Mean	Daily High	Daily Low		
TM-002	Tickets containing adequate investigative data	86%	100%	75%	▲	2
	Labor (hours) impact on ineffective data acquisition	8.2	9.1	0	▼	2
TM-003	Events per Analyst Hour	11.1	132.1	2.1	▲	1
TM-004	Tickets with unique annotations	83%	95%	76%	—	2
TM-005	Use cases that require analysis change to impact	17%	19%	7%	▼	3
TM-006	Use cases that have false positives reported	11%	15%	0%	▼	3
TM-007	Alerts requiring escalation to level 2	15%	30%	10%	▼	1
	Alerts requiring escalation to level 3	7%	10%	0%	▼	2

Figure 2. Sample SOC operational metrics dashboard

[2] "Understanding Variation: The Key to Managing Chaos", Donald J. Wheeler.

An example of operational metrics being destructive is SOC management using the number of cases opened each week as the primary measure of analyst contribution. This measure is highly contingent on dynamic content: The number of events presented to an analyst may influence the number of cases opened by that analyst. And the number of events presented can vary greatly based on factors that are outside of the analyst's control. For this example, if SOC management looks at the number of cases opened each week by analyst and any time the number of cases opened deviates below the baseline, the contribution of that particular analyst is perceived as low and additional administrative tasks are assigned. The analyst then has to handle those additional tasks along with their regular monitoring and incident detection duties. The time that the analyst spends performing the additional tasks assigned by management is time that is not spent performing monitoring duties, which in turn means that the number of cases that are created for that week will again be less than normal. This situation then becomes a vicious circle for both SOC management and the analyst. This is greatly destructive for the analyst's morale and can destroy the overall productivity of a SOC.

Instead of assigning the analyst additional administrative tasks, encourage the analyst to dig deeper.

Metrics such as events per analyst hour (EPAH), number of events annotated, number of events vs. events of interest, case open time or time to close, and even the number of cases opened each week can be helpful if used appropriately. Take the previous example of gauging an analyst by the number of cases opened each week. Instead of assigning the analyst additional administrative tasks because of low numbers, encourage the analyst to dig deeper, explore the existing events further, mine the available data in different ways, and satisfy the curiosity that is native to the field. This type of encouragement almost always leads to innovation. By mining the available data in a different way, an analyst might discover a different path in which to detect possible attacks.

Retention

Whether you hired your security analysts or grew your own, you want to keep them. Analyst retention issues can stem from several sources: SOCs are high stress environments; shift work is demanding and inconvenient; the wrong SOC work format may be repetitive and boring; there may be a perceived lack of upward mobility; the pay may not be competitive enough; there may be insufficient opportunity for development; or there may be low team morale and a poor work culture. Several retention tools need to be utilized to remedy high turnover, starting with team culture, individual development, and progression planning. SOC management must realize the nature of an analyst's job require ongoing skills development, appropriate freedom to apply those skills, and recognition when deserved. The security field is very broad and dynamic and you have the wrong SIEM. While security analysts are performing "real-time" analysis, they should be actively engaged and constantly working out the context and connections of the information they are presented. If they ever say that they are "clearing the console", then they are doing it wrong. This indicates a focus on getting events off the screen instead of analyzing them for attacks. analysts must stay apprised of everything from new technologies and vectors of attack to the impact of emerging regulations.

Coaching and mentoring analysts is an obligation of the SOC leadership.

Coaching and mentoring analysts is an obligation of SOC leadership. Early career professionals require a more interactive management style and focus as they learn how to be both an analyst and a professional. Good career development overall, for both junior and senior professionals is a must. The junior analysts need to perceive that a clear path exists for progression into more senior roles. Also, the senior analysts need to be able to understand that the senior analyst roles aren't the ceiling. Management can work directly with HR to clearly define these progression paths, requirements, timelines involved, and should perform an annual market survey to keep compensation competitive. Regular (i.e., weekly or biweekly) one-on-one meetings between employees and management have a profound impact on the retention and engagement of employees, and feedback and coaching should be a regular part of these conversations. 24x7 environments require extra effort from management to interact with employees of all shifts, and this should be a consideration when designing shift schedules.

Good Guys hate Bad Guys, but they hate being bored even more. Do not insult your security analysts by focusing on the operations over the analytics. The last thing that you should ever expect of a security analyst is for them to spend most of their time doing tasks that could easily be automated. If a procedure can remove the need for human analysis and decision, then that procedure should be automated using the power of the SIEM. If your SIEM can't do it, then you have the wrong SIEM. While security analysts are performing "real-time" analysis, they should be actively engaged and constantly working out the context and connections of the information they are presented. If they ever say that they are "clearing the console", then they are doing it wrong. This indicates a focus on getting events off the screen instead of analyzing them for attacks.

Console burn-out is one of the largest risks to job performance and satisfaction.

Schedule

Your Good Guys, however heroic, are still humans. You should have reasonable expectations of how long they can effectively perform an intensive task like "real-time" analysis. Console burn-out—the effect of spending too much concurrent time performing analysis is one of the largest threats to job performance and satisfaction. An analyst can perform effective analysis for no more than three concurrent hours, so task rotation is crucial in retaining your analysts and helping them to succeed in their job.

Analysts that truly make a difference contribute to the team in a number of ways:

- They must be able to suggest and create SIEM content.
- They improve or create SOC procedural documentation.
- They perform research that reveals threat intelligence.
- They optimize operations by creating automation.
- They tune and optimize the configuration of security devices.
- They may even manage some portion of the SOC infrastructure.

These types of jobs are complementary to the traditional task of analyzing security information and are necessary for a highly functional SOC.

	Level 1 Security Analysts		Level 2 Security Analysts	
Time	**Analyst 1**	**Analyst 2**	**Analyst 3**	**Analyst 4**
6:00	On Console	Escalation/OOB	Daily Ops Meeting	
7:00	On Console	Unstructured Analysis	Escalation/OOB	
8:00	QA & AAR	On Console	Escalation/OOB	
9:00	Escalation/OOB	On Console	Break	
10:00	Break	On Console	Escalation/OOB	
11:00	On Console	Break	Escalation/OOB	
12:00	On Console	Escalation/OOB	Meetings	Unstructured Analysis
13:00	On Console	Escalation/OOB	Meetings	Meetings
14:00	Break	On Console	Meetings	Escalation/OOB
15:00	Escalation/OOB	On Console		Meetings
16:00	On Console	Escalation/OOB		Unstructured Analysis
17:00	On Console	Break		Escalation/OOB
18:00	Unstructured Analysis	On Console		Break
19:00	Escalation/OOB	On Console		Escalation/OOB
20:00	Break	On Console		QA & AAR
21:00	On Console	Break		Escalation/OOB
22:00	On Console	Escalation/OOB		
23:00	On Console	Unstructured Analysis		
0:00	QA & AAR	On Console		

Figure 3. Example task rotation schedule.

Shift scheduling can have a profound impact on your ability to retain talent, especially in 24x7 environments. Below are some guiding principles on creating 24/7 schedules:

- Make the schedule predictable. An overly complex schedule can be frustrating and hard to follow.
- Do not rotate shifts too frequently. It takes time for people to adapt to working certain shifts and the stress of moving from a day shift to a night shift can have rippling impacts on health, productivity, and personal life. If your schedule has rotation in it, consider doing such rotations on at most a quarterly basis.
- Do not schedule analysts to work alone. You need depth in your shifts to perform successful task rotation and to prepare for absences. There may also be safety issues if analysts are working in isolated and secured areas.
- Build in overlap for your shifts. Most errors in a SOC occur during shift transitions. There are also negative cultural challenges for environments where individuals in the same operation do not ever see one another. Overlap periods also ease the facilitation of team meetings and training activities.
- Make considerations for commute times—in a 24x7 environment, it is easy to miss rush hour traffic.
- While 12-hour shifts can minimize headcount requirements, these shifts are very long and productivity and quality of work will diminish after 8-10 hours. Also, shifts with four concurrent 12-hour days can result in a very ineffective and unhappy analyst by the 48th hour in 4 days.

The HPE Cyber Defense Center (CDC) operates on a schedule similar to the following, which allows for high levels of overlap between shifts as well as a depth on Wednesdays where team meetings and training activities can be easily performed without sacrificing real-time monitoring or requiring repetition across each shift.

	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
early 4×10h	L1 Analyst 1						
				L1 Analyst 3			
	L1 Analyst 2						
				L1 Analyst 4			
day 5×8h		L2 Analyst 1					
	L1 Analyst 5						
				L1 Analyst 7			
	L1 Analyst 6						
				L1 Analyst 8			
afternoon 5×8h		L2 Analyst 2					
late 4×10h	L1 Analyst 9						
				L1 Analyst 11			
	L1 Analyst 10						
				L1 Analyst 12			

Figure 4. Sample SOC shift schedule.

Local labor laws and company policies may dictate your scheduling options.

The security field is not static and analysts should be encouraged to stay on top of new and upcoming threats.

Ongoing Training

Consistent and ongoing training is another facet influencing analyst retention. As mentioned before, the security field is not static and analysts should be encouraged to stay on top of new and upcoming threats. Analyst experience can be grown through training as well as real-world experience. A formal training program should be leveraged to ensure that analysts are always learning.

Formal training programs should be executed both during the on-boarding process and during employment. A training program during the on-boarding process is priceless to a new analyst as it should contain information on the network they will be monitoring, re-enforce technical skills, and acclimate them to the environment. Training after the on-boarding process should re-enforce and grow baseline technical skills and introduce new skills. Formal training should be leveraged along with informal training for these purposes. Formal training would be along the lines of either vendor specific or instructor-led/web-based training—anything that can result in obtaining a certification is a plus. Lunch and learns, webinars, on-the-job training, and technology deep dives can be utilized as informal, yet productive training.

Allowing analysts to work on complex problems, such as automating a repetitive task or addressing an ongoing issue that has eluded resolution, can greatly increase job satisfaction and engagement. Allow the analysts to propose projects as part of their annual growth plan. The analyst will be able to get away from the mundane and utilize their own problem-solving skills in different ways.

Another way to allow them to utilize their skills would be to temporarily rotate them to other security teams. This allows the analyst to be exposed to different tools, processes, and people. In turn, this exposure permits them to utilize this newfound knowledge in their analysis.

Summary

Bad Guys are everywhere and our attackable surface is expanding at an alarming rate. Technology alone cannot combat this challenge. We need good guys in the form of Security Analysts in our SOCs and Cyber Defense Centers to protect and defend our organizations, our customers, and our assets. Security Analysts are in short supply in the industry, far short of meeting the demand. Existing commercial training programs and certifications are not producing the volume and quality of professionals that are needed and successful organizations are investing in programs to grow their own security analysts.

The HPE SIOC team has the experience and best practices to help address this industry-wide problem through a combination of staff augmentation, job design, skills assessment, program development, analyst development, and expert mentoring. They have with over 100 organizations in building or optimizing their Security Operations Capability. The result is unparalleled expertise and a Security Analyst Training program including a proven methodology to finding, hiring, training, and retaining these Security Analyst good guys.

About HPE Enterprise Security

Hewlett Packard Enterprise is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading products from HPE ArcSight, HPE Fortify, and HPE TippingPoint, the HPE Security Intelligence Platform uniquely delivers the advanced correlation, application protection, and network defenses to protect today's hybrid IT infrastructure from sophisticated cyber threats.

Hewlett Packard Enterprise Services

HPE Security Intelligence and Operations Consulting (SIOC) Services take a holistic approach to building and operating cyber security and response solutions and capabilities that support the cyber threat management and regulatory compliance needs of the world's largest enterprises. We use a combination of operational expertise—yours and ours—and proven methodologies to deliver fast, effective results, and demonstrate ROI. Our proven, use-case driven solutions combine market-leading technology together with sustainable business and technical process executed by trained and organized people.

Learn more at

hpe.com/software/sioc

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA5-3982ENW, November 2015, Rev. 2