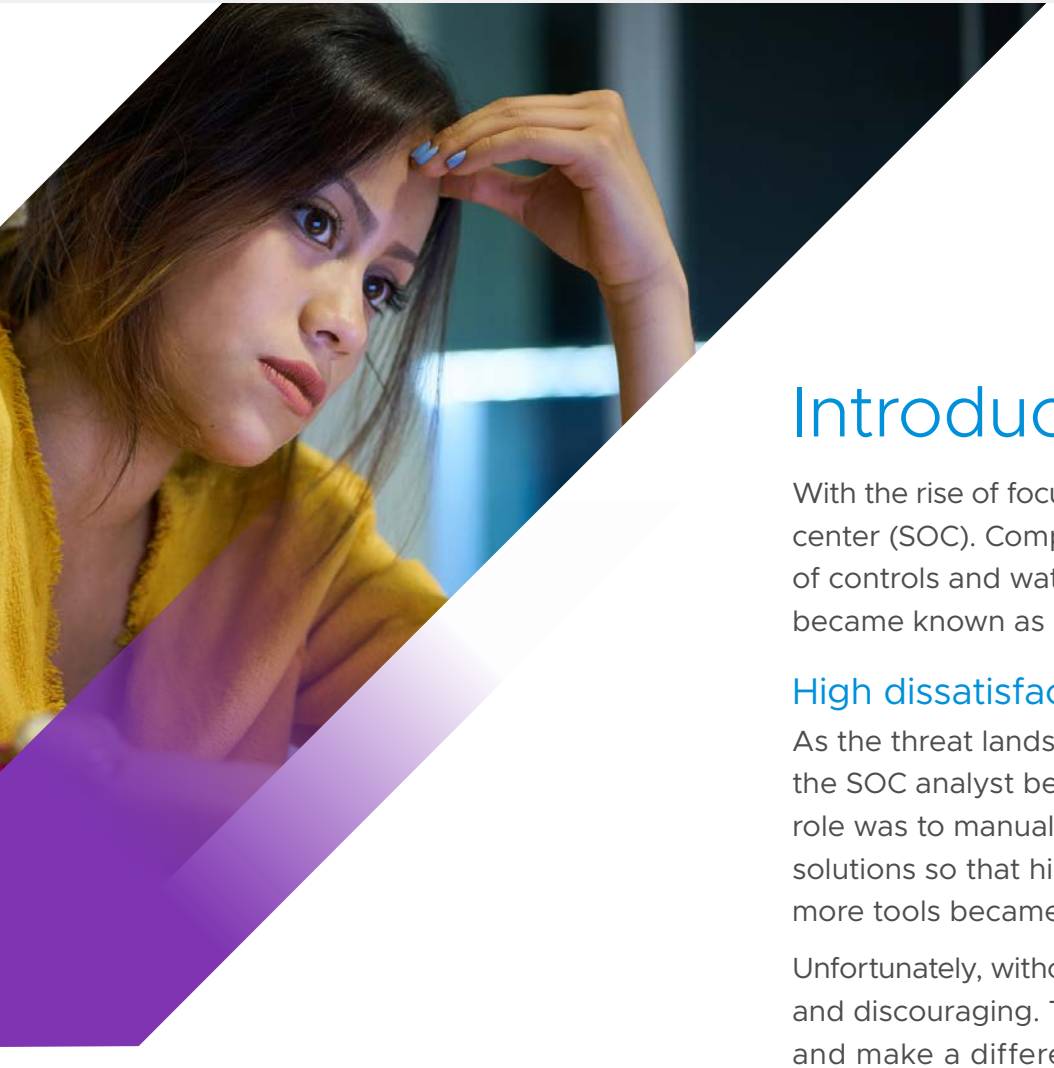
vmware Carbon Black

GET STARTED

Today's SOC Analyst Is Tomorrow's Threat Hunter



Introduction

With the rise of focused cyberattacks came the rise of the security operations center (SOC). Companies realized that they needed to establish a simple set of controls and watchers to protect their environment. The watchers soon became known as SOC analysts.

High dissatisfaction for a critical role

As the threat landscape evolved and security solutions became a must-have, the SOC analyst became a critical entry-level role in companies. Initially, their role was to manually filter out the noise of alerts generated by monitoring solutions so that higher-level resources could focus on the real issues. As more tools became available, more SOC analysts were hired.

Unfortunately, without further evolution, the role of SOC analyst grew repetitive and discouraging. These individuals wanted to grow into higher-level roles and make a difference fighting cyberattacks. Instead, many found themselves feeling unappreciated and undervalued, which has led to a turnover rate upward of 25 percent for the position.[1]

1. CriticalStart. "The Impact of Security Alert Overload." 2019.

Opportunity for development and security improvements

At this low point in job satisfaction comes an opportunity for development of those resources, which can result in big improvements to security postures. In this paper, we'll take a look at the SOC analyst role and provide specific steps to evolve the position into that of a high-value threat hunter. This approach is supported by the testimony of two SOC analysts (aka threat hunters) from a team that has already made this incredible transformation.

ABIGAIL (ABI) HERTZ
THREAT (SOC) ANALYST
VMWARE

SCOTT LUSSIER
THREAT (SOC) ANALYST
VMWARE

Today's SOC Analyst

While some SOC teams are beginning to evolve the SOC role, many are stuck in the same processes that originated the role. The majority of their day, around 80 percent, is spent managing low-fidelity alerts.[2] This is the process of opening an alert, verifying that it is not a concern and closing it. Open>Verify>Close. The remainder of their time is spent reporting on the efforts and performing shift ops and tool maintenance.

Measuring SOC analyst performance

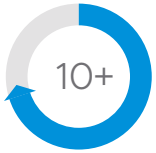
SOC management measures their analysts in accordance with these activities. Typical performance measures look at the reduction in alert investigation time and reduction in the volume of alerts. This means that alert tuning is incentivized as well as opening, verifying and closing alerts as quickly as possible. Neither of these measures encourages development or improvement of security postures.

2. CriticalStart. "The Impact of Security Alert Overload." 2019.

SOC analysts are unhappy

It is no wonder that a study from CriticalStart on *the impact of security alert overload* revealed quite a few problems with the state of SOC analysts today.[3]

SOC analysts are overwhelmed by alert overload.



More that 70 percent of SOC analysts investigate more than 10 alerts per day.

73 percent of SOC analysts say that 25–75 percent of alerts are false positives.

The longer that SOC analysts stay in their role, the more dissatisfied they are.

Job satisfaction is less than 50 percent after two years in the role.

SOC analysts don't feel they are making a difference.

28 percent of SOC analysts say they have never stopped an intrusion.

Turnover is high.

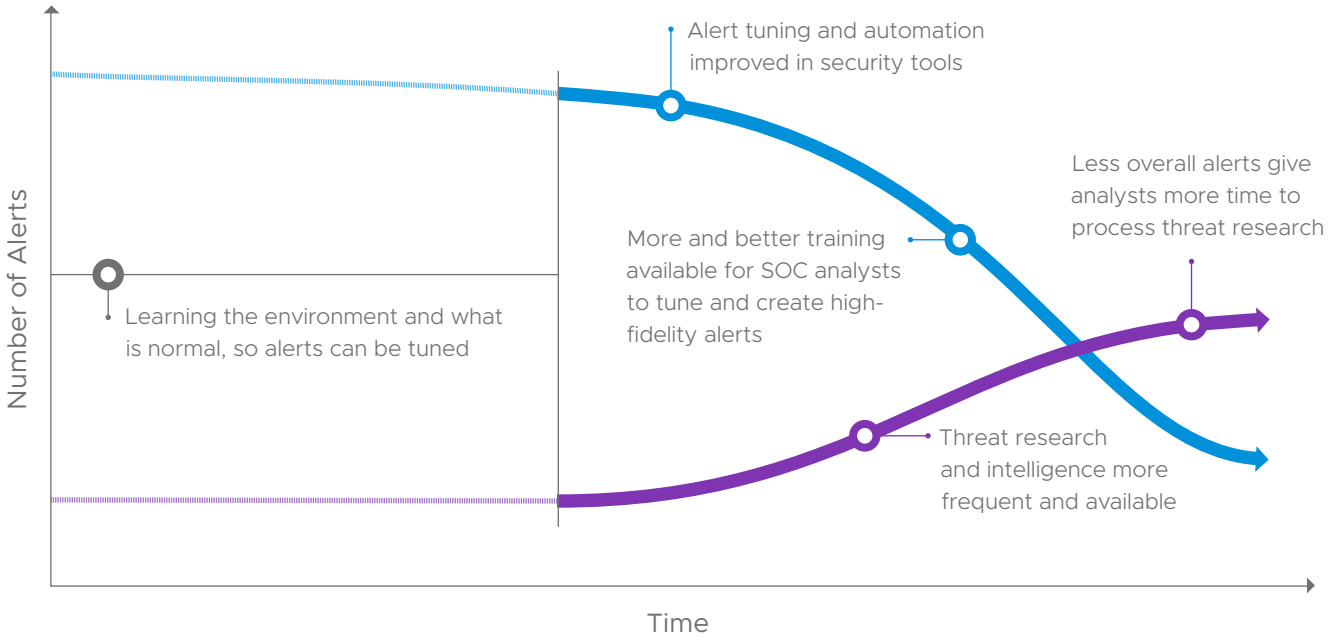
More than half of SOC analyst teams have seen a turnover of more than 25 percent.

3. CriticalStart. "The Impact of Security Alert Overload." 2019.

Opportunity to Evolve

New opportunity to evolve the SOC analyst

SOC analysts have made progress in understanding their environments and tuning out low-fidelity alert noise. With fewer low-fidelity alerts to open, verify and close, SOC analysts have an opportunity to develop their security expertise and grow their careers, resulting in greater job satisfaction and less turnover.



KEY FACTORS PROMOTING EVOLUTION

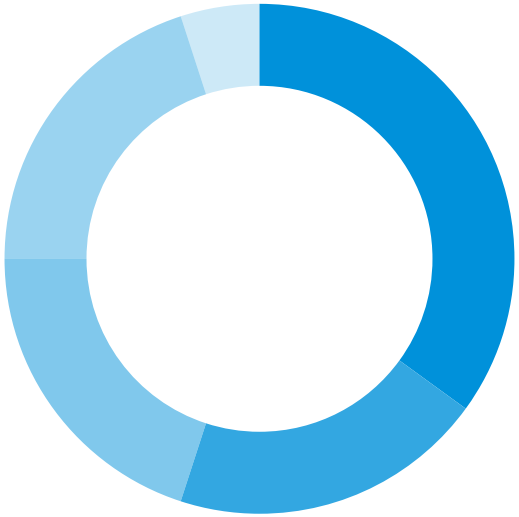
A few key developments over the past five years have helped create new opportunities:

- Security solutions have improved with more automation that helps SOC analysts reduce alert noise, giving them more time to take on strategic tasks.
- Security organizations, such as the SANS Institute, have developed training programs and certifications for SOC analysts that help them walk into the role with a much higher level of understanding than early SOC analysts had.
- *Threat research and intelligence* have become more readily available and more frequently published, so SOC analysts can start thinking about ways to create new alerts that protect their environment from new threats.

From SOC Analyst to Threat Hunter

Security tools will continue to monitor environments and trigger alerts for things such as audit events and new traffic or activity. However, much less of the SOC analyst's day needs to be spent on this. This allows time to absorb threat research detailing new attack methods and threats, and to process the information. These resources can then document tactics, techniques and procedures to handle and/or prevent these threats. They can also create defenses and alerts highly focused on a malicious event—high-fidelity alerts.

The evolved VMware SOC analysts interviewed for this eBook say their days breakdown like this:



05% investigating high-fidelity alerts

20% working on strategic project playbooks for threat analysis

20% monitoring and investigating audit and new activity alerts

20% maintaining and configuring security tools

35% reviewing threat intelligence and applying to the environment

Measuring the performance of the evolved SOC analyst

The evolved SOC analyst is being measured on how well they add to the protection of their environment with threat intelligence. Metrics include the number of new alerts put into effect and the number of new protective and defensive measures created.

Rebranding the SOC analyst

With the increase in responsibilities and the direct impact on security posture in both analyzing and creating high-fidelity alerts, a rename of the role seems warranted. Our evolved SOC analysts have rebranded the SOC to the threat operations and response center (TORC). Their titles changed correspondingly to threat analysts.

Threat analyst satisfaction

"Our days are much more exciting. We are more proactive instead of waiting for things to happen."

"I love being able to investigate a problem, solve it, then stop it from happening again."

ABIGAIL (ABI) HERTZ
SOC (THREAT) ANALYST
VMWARE

"Learning about a threat, hunting for it and then creating protection against it is awesome."

"We are much more strategic now. Alerts are tuned so we only see things that make the most impact."

SCOTT LUSSIER
SOC (THREAT) ANALYST
VMWARE

Evolution of the SOC Analyst

SOC analyst

How they spend their day:

- 80 percent managing low-fidelity alerts (click>validate>close)[4]
- 20 percent reporting, doing shift ops and maintaining tools[4]

How they are measured:

- Reduction in alert volume
- Reduction in alert investigation time

Job satisfaction:

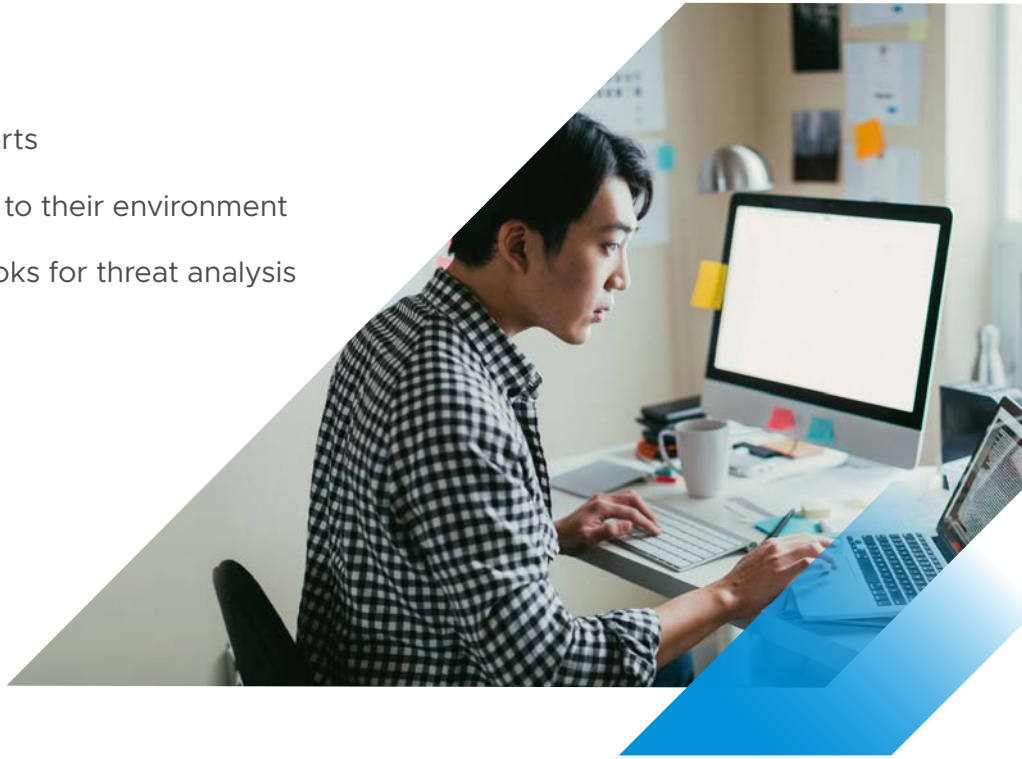
- 73 percent of SOC analysts say that 25–75 percent of alerts are false positives[4]
- More than 70 percent of SOC analysts get overwhelmed by investigating more than 10 alerts per day[4]
- Job satisfaction falls to less than 50 percent after a just a few years in the role[4]
- 28 percent of SOC analysts say they have never stopped an intrusion and don't feel they are making a difference[4]
- More than half of SOC analyst teams have a turnover of less than 25 percent[4]

4. CriticalStart. "The Impact of Security Alert Overload." 2019.

Threat hunter

How they spend their day:

- 5 percent investigating high-fidelity alerts
- 20 percent monitoring and investigating audit and new activity alerts
- 35 percent reviewing threat intelligence and finding ways to apply to their environment
- 20 percent working on strategic projects, such as creating playbooks for threat analysis
- 20 percent maintaining and configuring security tools



How they are measured:

- Number of artifacts processed with ATT&CK tags
- Amount of threat intelligence cases
- Number of alerts and defensive measures created
- Number of continuous monitoring capabilities

Job satisfaction:

- "Our days are much more exciting. We are more proactive instead of waiting for things to happen." – Abi
- "I love being able to investigate a problem, solve it, then stop it from happening again." – Abi
- "We are much more strategic now. Alerts are tuned so we only see things that make the most impact." – Scott
- "Learning about a threat, hunting for it and then creating protection against it is awesome." – Scott

Advice

How to transition from SOC analyst to threat analyst

Our evolved SOC analysts provided three pieces of advice for companies looking to increase security sophistication.

Invest in security solutions

The first step in developing SOC analysts is to get them the advanced security tooling they need to begin to make the transition from low-fidelity alert management to high fidelity. Abi comments that tooling can help to get SOC analysts out of chaos mode. "Companies need to increase the overall importance of security and the value of the SOC role. SOC analysts need to have the tools to do a great job. They can't be strategic if they don't feel they are supported and being taken seriously."

Scott also commented that security solution vendors could help advance the SOC by listening to SOC analysts as they build in new features. "Everyone that makes security products needs to listen to SOC analysts. That collaboration would significantly improve tools and advance security sophistication."

Invest in SOC analyst development

Many changes in technology can be researched structurally to find answers, but investigating a threat hypothesis can oftentimes be more akin to an art form. Evolved SOC analyst, Scott, formerly a desktop support engineer, agrees that the role is different. "The SOC analyst/threat hunter role isn't something you can just figure out. You need continuous learning, and luckily there is a lot of great information and training out there from organizations such as SANS."

Scott goes on to say if you "get them the tools and training, they can play a key role in making security more sophisticated."

Trust your SOC analysts

If you make sure your SOC analysts have the right mindset, you can allow them the leeway to experiment and make improvements. Scott comments, "A security professional that wants to learn and solve problems is the key to having the right people in this role. A security mindset is what keeps companies protected."

Yet, as more threat research becomes readily available to ever-growing security teams, the SOC analysts become barraged with opinions. Abi describes this challenge, "There is so much more security knowledge, and everyone has their own opinions. This means we have a lot more to absorb and validate. It also means you can at times have 50 people with other opinions against what you are trying to do." More than ever, companies need to trust that their SOC analysts deep in the trenches of day-to-day threat response understand the environment and the best ways to protect it.

Scott adds that investing in security solutions does not mean a cut back in SOC analysts. "A lot of security vendors advertise their tool as the end-all and be-all for security and minimal staff is needed. The reality is that you always need a person to think about the alert, the problem and the possible result. Tools are great, but you still need a person with an investigative mindset running it."

Benefits, Predictions and Summary

Short- and long-term benefits of SOC investment

Taking a new approach to the SOC analyst role can create immediate benefits, the first being talent retention. Analysts seeing the investment in tools, in training and the change in how they are measured will be more likely to stay. This helps reduce the cost of recruitment and training in a highly competitive field.

Another significant benefit will be continuous improvement of the protective measures surrounding the environment. Trusting in the analysts to absorb threat research and use it to create new alerts to prevent new threats will continue to reduce the risk of breach.

The SOC analyst title may change, but as Scott comments, this is necessary for people retention. "The SOC analyst role will go away in favor of a threat-centric role. It will be a more strategic, more proactive, threat-focused role. And the name will change. If companies are smart, they'll grow the SOC analyst into this new role to retain people with this knowledge."

More threat analysts needed

The only certainty that has carried through in the past decade of cybersecurity is that cyberattacks will continue to increase and evolve. That means that the SOC analyst (or threat analyst) role will continue to be in high demand.

Abi agrees. "The changes in the last four years have been so big I can't even imagine what four years out will look like. What I do know is that there will inevitably be new tools and new attacks. The threat landscape will keep changing. Processes might change, but SOC analysts will still be needed. There will be new technology and therefore new vulnerabilities, so our role will continue to grow. We will need more SOC analysts doing more proactive threat hunting work."

See how you can combat threats in your environment.

Schedule a demo >

Join us online:

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com