The State of the SOC:
An Enterprise Study on Threat Detection and Response

Chenxi Wang, Ph.D. Jason Clark, Dustin Wilcox

360Velocity

March 2018

Commissioned by Fidelis Cybersecurity

Introduction

Fidelis commissioned 360Velocity to conduct an enterprise study to examine current trends and practices of threat detection and response. The goal is to understand how large organizations set requirements for detecting and responding to threats, the metrics they use to measure success, and potential solutions to address the gaps in order to improve efficacy and efficiency.

For this study, 360Velocity drew from a dataset of 50 security practitioners from enterprise companies. These companies represent a cross-section of industries: SaaS, retail, financial services, healthcare, consumer services, and high tech. We also supplemented this data with 10 in-depth interviews with leading practitioners in the threat response and security operations space.

Examples of companies in our dataset include:

1. **Online retailer service:** One of the largest online retailers in the U.S. This company operates a mature incident response and threat hunting program.
2. **Consumer-facing financial services company:** This organization issues credit cards to consumers and offers a wide range of financial services.
3. **Provider of data analytics products and services:** This company offers analytics services and products for business intelligence and financial analysis.
4. **Large infrastructure-as-a-service cloud provider:** This organization offers some of the largest enterprise-facing IaaS services. The company also operates a range of SaaS services.
5. **US-based brokerage and financial advisory firm:** This firm is one of the largest brokerages in the US. They handle a tremendous amount of client data and trades.

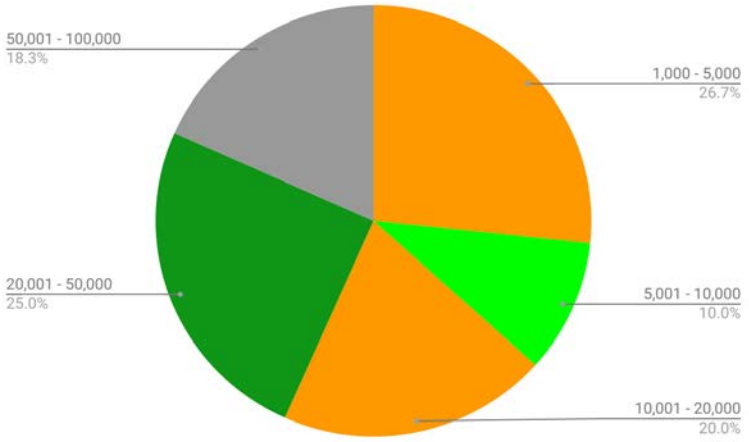

Figure 1: Size distribution of the companies in our study

Figure 1 captures the size distribution of the companies in our study. Of these, 63% have more than 10,000 employees, 10% are between 5,000 and 10,000 employees, and 27% have less than 5,000 employees.

All companies interviewed have dedicated security teams. Many operate a **Security Operations Center (SOC)** to detect breaches and respond to incidents. Others outsource either low level SOC analyst tasks (i.e. tier 1/tier 2) or the entire SOC functions to a third-party service provider.

Key Findings: Excessive Alerts, Outdated Metrics, and Limited Integration Lead to Over-taxed SOCs

Key findings of this study:

1. ## SOC analysts are being overwhelmed by alerts

   As the threat landscape changes and companies move to adopt more defensive technologies, SOCs are being overwhelmed by the sheer volume of alerts that require their attention. Many of our interviewees stated this was both a capacity issue and a skills/training issue: not only was the alert volume becoming increasingly unmanageable, they also struggled to recruit, train, and retain qualified SOC analysts.

2. ## Integrated investigation across endpoints and networks remains a major pain point

   Even though nearly everyone recognizes the importance of integrated investigation across user endpoints, servers, and networks, few are able to implement this in a meaningful and effective way. There's still a significant amount of manual work required to tie endpoint and network information together into one investigation.

3. ## SOC and IR metrics are outdated and ineffective

   Every organization we interviewed uses some form of metrics to measure SOC and Incident Response (IR) effectiveness. However, most feel that the metrics being used today are archaic, ineffective, and do not reinforce the right behaviors. As such, organizations expressed a general desire to reinvent the SOC and IR metrics, but the industry lacks consensus and standards on which set of metrics to adopt.

4. ## Threat hunting is an elite operation that exists only in the largest and most sophisticated organizations

   Threat hunting is a recent innovation in the detection and response space. Threat hunters are typically experienced IR or security professionals. They utilize sophisticated identification techniques beyond signatures and indicators to look for suspicious

behaviors and our study showed that dedicated threat hunting practices are still rare and exist only in the most mature, large enterprises.

5. SOC investigations today remain largely signature-based; the focus on TTPs is few and far between

   Signature-based detection tactics are used extensively in today's SOC. Even though many told us they are shifting focus to Techniques, Tactics, and Procedures (TTPs), the mass majority of organizations are still heavily reliant on static signatures and indicators.

The Current State

Before we delve further into the specific pain points and opportunities of SOCs, it's valuable to understand the current state and shared practices that are being adopted within the security industry.

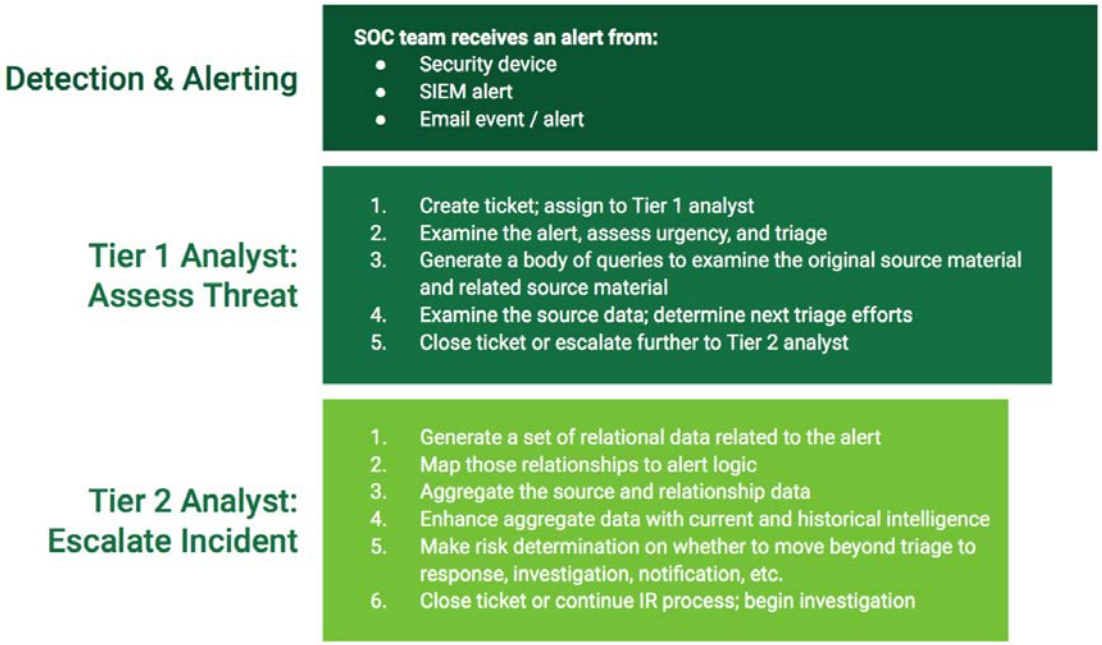

Figure 2: Example of a SOC workflow

As illustrated, an alert from a security device, a SIEM alert, or an email event can trigger a ticket being created and assigned to a tier 1 analyst. The analyst then carries out a two-stage triage task. The goal of the first stage is to quickly determine whether the ticket should be discarded/closed. The goal of the second stage is to determine whether the alert should be elevated to an incident.

In the second stage, the analyst would gather a multitude of information from different devices in the environment, such as endpoints, network devices, and historical log storage, and link the

indicator from the alert with the information gathered from the different points. The analyst would then make a risk-based decision on whether to elevate the ticket to an incident, which will kick off an IR or investigation phase.

The second stage of triage is sometimes handled by a tier-two analyst. To put the workflow in context, let's look at a concrete example of a phishing email event.

Sample SOC Scenario: Phishing Emails

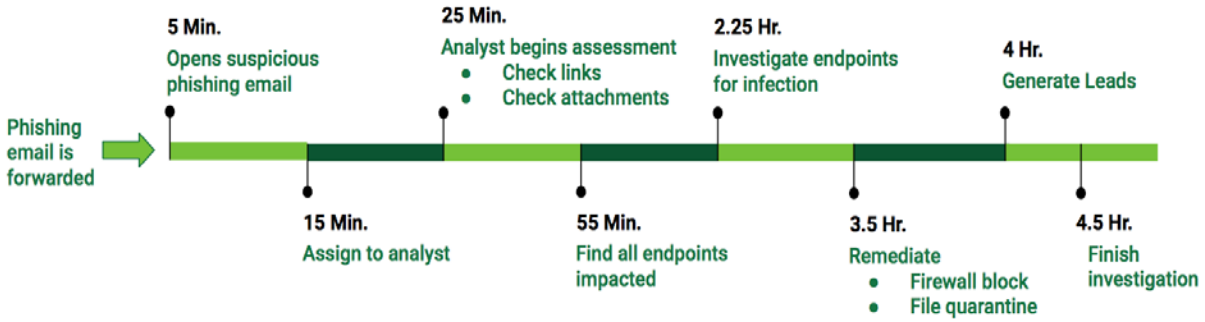

Figure 3: Example scenario of a phishing email event (source: Microsoft)

In this scenario, an email security system has spotted a potentially suspicious email and quarantined it. This triggers an alert and a ticket is generated and assigned to an analyst. The analyst opens the quarantined email, quickly scans the attachment to determine whether it's worth further investigation. If the answer is yes, the next step is to find all the endpoints that may have been affected by the email. This means querying Active Directory (AD), Splunk, and the mail server. Once you find all the endpoints, you pull information from the endpoint to decide whether any of the endpoints have been infected or need to be remediated. The final step is remediation, which could mean establishing new firewall or email gateway policies, cleaning up infected files from any endpoint, or reimaging endpoints if necessary.

From start to finish, this process may take an analyst 4 to 5 hours to complete.

SOC Analysts Are Experiencing Alert Fatigue

Based on the current state of the SOC workflow, it's evident that an average SOC analyst has limited bandwidth per day to respond to alerts and complete investigations. The survey and the interviews we conducted confirmed this. Here's what our study found:

Figure 4: Most SOC analysts can only handle between 7-8 investigations in a day

Overall, we asked the companies how many investigations a SOC analyst can realistically handle in a day. Summary of responses as shown in Figure 4:

- 60% said "7 to 8 investigations."
- 30% said "5 to 6 investigations."
- 10% said "8 to 10 investigations."

The study shows that the upper limit of investigations a trained, competent SOC analyst can reasonably handle in a day is 7-8. When the number of investigations shot up to 10 a day, our interviewees reported cases of analyst fatigue, which often resulted in lower fidelity investigations and missed attack signals.

Yet, alerts and incidents are skyrocketing

When we interviewed one of the top cloud service providers in the US, the company indicated that they currently have more than 300 million active user accounts. They see 450 billion Active Directory logins on a daily basis. As a result, the service generates double-digit petabytes of logs a day, including roughly over 1 million compromise attempts.

The company currently employs roughly 200 SOC analysts. Even assuming 10 investigations a day, the most they can handle is 2000 investigations in any given day. With more than 1 million compromise attempts every day, 2000 investigations are far from enough.

With a rising threat landscape, continued constraints on both the availability and bandwidth of well-trained SOC analysts, SOCs are increasingly burdened. One senior manager of a SOC for a large financial services institution said: “18 months ago, I could still afford some manual work, but that is not the case this year. Manual efforts now are untenable and my #1 priority for security operations is to reduce manual work and increase automation.”

From the data gathered, we can conclude that automation is not only becoming increasingly important for SOCs but mandatory.

SOC Automation: The Gap Between Theory and Practice

A big theme in security operations today is automation. Increasing automation can lead to improved efficiency, reduced dwell time, and ultimately, better performance.

Opportunities for automation

Where are the opportunities for automation in today’s Security Operations? Our interviewees suggest the following as top automation targets:

- **Alert triaging and prioritization:** This is the task of processing alerts, triaging and prioritizing the alerts to determine which ones should be dropped and which ones should be elevated to “incidents.” Automating this step is key to increasing SOC efficiency, as every minute an analyst spends on triaging is a minute that is not spent on incident investigation.
- **Information and data collection:** To start an investigation, analysts need to collect further information from relevant endpoints, network devices, or a SIEM system. The process of deciding which information to collect and from where is a step that many are looking to automate.
- **Common repetitive tasks:** In a SOC operation, analysts face many repetitive tasks such as ticket generation and reporting. These steps should be automated without involving manual analyst time.
- **Common logics:** A security investigation would often involve “pivoting” or logics to perform additional context gathering. For example, seeing an indicator on the network may lead to a query of the Active Directory Server. Or, reviewing a quarantined email may lead to the retrieval of PCAPs (packet captures). These common logic steps can be captured in “pivot” logics and potentially automated.

Today, organizations typically approach automation by standardizing processes, steps, and controls. Some of them utilize playbooks, which codifies common logics and tie pivoting to pivot steps across multiple devices and information within the same environment.

Automating alert triaging

Alert triaging is the first step of an analyst's workflow. Unfortunately, without automation, alert triaging can be a tedious process. We asked our respondents what percentage of their daily alerts are triaged (as opposed to dropped) and their answers were very interesting.

As shown in Figure 5, respondents indicated:

- 30% had less than 10% of the alerts triaged
- 62% had less than 25% of the alerts triaged
- 83% had less than 50% of the alerts triaged

What percentage of the alerts are triaged in a day?

Alert Triaged	Number of Companies
<10% are triaged	**30%**
11-24% are triaged	**32%**
25-49% are triaged	**21%**
50-74% are triaged	**11%**
75% or more are triaged	**6%**

Figure 5: Average percentage of alerts triaged today?

The reason that not all alerts are triaged is precisely due to the lack of automation. In this case, the analyst has to manually triage most of the alerts, which is why 83% of the companies had less than 50% of the alerts triaged daily.

The 6% of the companies that responded with "75% or higher alerts are triaged daily" include companies that utilize both commercial and home-grown automation tools extensively. Only one of those companies was able to push its alert triage rate to 90%+.

The case for integration

A growing frustration within IR and SOC personnel is the lack of integration between different sensors as well as between enforcement points in the infrastructure. For instance, extracting IOCs from endpoints and automatically pivoting from one endpoint to others and to network investigations is still a difficult task.

One SOC analyst told us that when querying a particular network IDS, she found that the IDS wouldn't take the indicators that she wanted to use. Ultimately, she had to rewrite the indicator to fit the format of the IDS just to be able to query it. Consequently, the task took excess time to complete.

The lack of integration impedes not only the speed of investigation, but also the speed of remediation and control. When an investigation uncovers credible evidence of an intrusion, pushing new blocking policies to different network devices and endpoints still requires a fair amount of manual scripting and testing today.

When asked what percentage of security controls in their environment was integrated for incident response or security investigation purposes, 35 out of 50 respondents said at least half of their security controls were NOT integrated. Of the 50, 13 said less than a quarter of their security controls were integrated (see Figure 6).

What percentage of security controls in your environment is integrated?

Companies	Level of integration	Average alert triaging rate
13 out of **50**	Less than 25%	11%
35 out of **50**	Less than 50%	21%
13 out of **50**	At least 50%	39%
01 out of **50**	At least 75%	61%

Figure 6: Varied levels of security controls integrations across respondents

Interestingly, there seems to be a correlation between the companies that achieved a high triaging rate and those that have more integrated security controls (see Figure 6). Even though our sample size may be a little small for causality analysis, we observed that as the level of integration (of security controls) goes up, so does the average alert triaging rate.

The verdict: Integration is key for SOC automation

Overall, there's a clear negative impact on performance and efficacy of security operations if the company does not have integrated controls for threat detection and incident response.

The (In)Effectiveness of SOC Metrics

An important part of our study is SOC metrics. We wanted to understand how organizations measure the efficiency and effectiveness of their security operations. In particular, which metrics do they use to measure different aspects of security operations? Are the metrics sufficient? If not, are there opportunities for new metrics to better capture performance, return on investment, and impact to the organization?

When it comes to SOC metrics, many feel that current metrics are ineffective or have room for improvement. When asked how effective current SOC metrics are, the responses were:

- 60% said they were "not effective"
- 20% said the metrics had "room for improvement"
- 20% said the metrics were "acceptable"
- None said the metrics were "satisfactory"

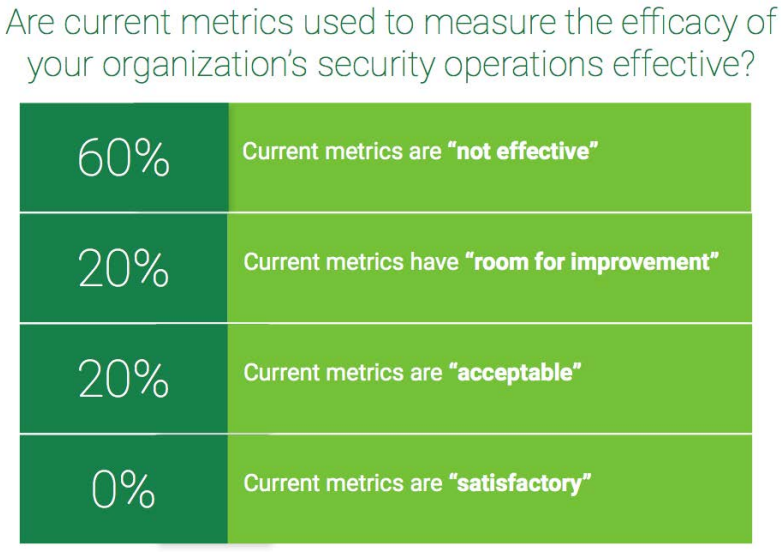

Figure 7: Most respondents don't consider current security operations metrics effective

Why do people feel current SOC metrics are not effective? We asked the drivers behind SOC metrics: "What was the reason that your organization developed SOC metrics?" Interestingly, the top answer was "Management needs metrics so I need to generate them." The other two

popular answers were “I need something to measure return on investment,” and “We need visibility into efficacy of the SOC.”

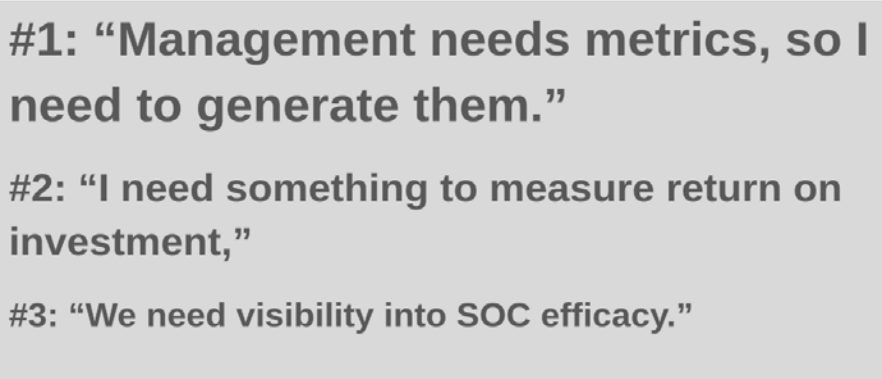

Figure 8: Top three reasons people use SOC metrics

One of our interviewees, an Incident Response manager for an online retailer, said: “If you are using metrics purely to please your manager, you may not be looking at the right measures that truly impact your organization.”

Some of the common metrics organizations use today to measure security operations efficacy are as follows:

1. **Alert to incident ratio:** This is an interesting metric, as it indicates the distribution of tier 1 and higher-tier tasks. If the alert-to-incident ratio is too high, staff may not be processing alerts sufficiently or thoroughly. If the ratio is too low, staff may be escalating too many things to the higher tiers, which could overwhelm senior analysts.

2. **Mean Time to Detection or Mean Time to Remediation (MTTD or MTTR):** MTTD is the time period between the onset of an event of interest and its actual detection**.** MTTR is the time period between case creation and case resolution. While these metrics convey meaningful information, too much focus on MTTD or MTTR can lead to sloppy investigation or response. For example, if MTTD is the only metric mattered, analysts might be incentivized to prematurely conclude cases, favoring a quick resolution rather than the right resolution.

3. **Dwell time:** The duration a threat actor has in an environment before they are detected or eliminated by the security team. This is an interesting risk-based metric -- the lower the dwell time, the more effective your security program is, and the lower the risk is for the organization.

4. **Case per analyst per day:** This one is controversial, as it encourages analysts to move quickly through investigations, which can result in shallow case work and increased risk.

5. **Cost per incident:** Some organizations keep a log of the incidents and the cost of security operations. They then calculate a per-incident cost. This metric is commonly seen in organizations where tracking return on investment is important.

The verdict: Pivoting to impact-based metrics

Many of those we interviewed expressed the sentiment that, instead of operational or behavior-oriented metrics, which could be misused, organizations should adopt impact-based metrics. Impact-based metrics are exactly how they sound - they help organizations measure the impact of security operations on mitigating risks or improving security postures.

Our interviewees suggested these impact-based metrics to consider:

- **Coverage of triaged alerts**: This rate indicates the number of alerts triaged vs. abandoned. As organizations move to adopt automation, triage coverage should go up.
- **Percentage of investigations completed with conclusive results:** In an ideal world, each investigation should conclude with a definitive result -- either it should be elevated to an incident or resolved to be business as usual. In reality, however, many investigations are closed with non-conclusive results. The percentage of investigations that reach conclusive results is a telling metric to the maturity and efficiency of the SOC.
- **Number of investigations that led to security re-prioritization:** This metric tracks the number of times the conclusion of a security investigation led to a change in the organization's architecture direction, an urgent patching task, or the adoption of a new defense tool.
- **Number of new TTPs attributed to SOC investigations:** Instead of signatures or indicators, more sophisticated SOCs and threat hunters aim to extract Techniques, Tactics and Procedures (TTP). Each time a TTP is added to the SOC or threat hunting workflow, it improves the power of security defense.
- **Number of new IOCs found:** If the investigation discovers new Indicators of Compromise (IOC) not present in the threat feeds, adding that to the list of IOCs SOC analysts track improves a defensive posture.
- **Number of new vulnerabilities identified by SOC activities:** If an investigation uncovers a vulnerability previously unseen within the organization, that investigation has just contributed positively to understanding and possibly reducing the organization's attack surface.
- **Number of campaigns/threat groups identified by the investigations:** Identifying a new threat group or a campaign targeting your organization is probably one of the most valuable things a SOC, Incident Response, or a threat hunting team can contribute. Knowing your organization is under a concerted attack by a certain group may help you fortify your defense in a specific way to counteract that threat group's tactics.

It is worth noting that dwell time and Mean-Time-To-Detection are also impact metrics. Some of these metrics may be aspirational - your security operations may never identify or uncover a new threat campaign against you. But if they do, you know they are making a visible impact.

Threat Hunting Is an Emergent Function

Today, mature security organizations may staff a dedicated threat hunting team independent of the normal SOC operations. While SOC analysts take on alert triage, incident investigation and response, the threat hunters focus predominantly on deep threat detection. The goal is to uncover previously unknown indicators, threats, and TTPs.

Most threat hunters are senior level security professionals with many years of operational or threat-related experiences. They are the “elite squad” within the enterprise in terms of all things threat-related. The need for threat hunting was born out of the necessity that rather than simply responding to the ever-increasing onslaught of threats, organizations need to get in front of them. Threat hunting by definition is intended to include the hunt for the “unknowns,” rather than detecting only “known bad.”

When asked whether their organizations have a dedicated threat hunting team, this is what respondents told us, as shown in Figure 9:

- 17% of the organizations we interviewed answered “yes”
- 42% of the respondents indicated that “threat hunting is either not mature or is partially handled by existing SOCs”
- 28% said they do not staff for threat hunting
- 13% were “not sure”

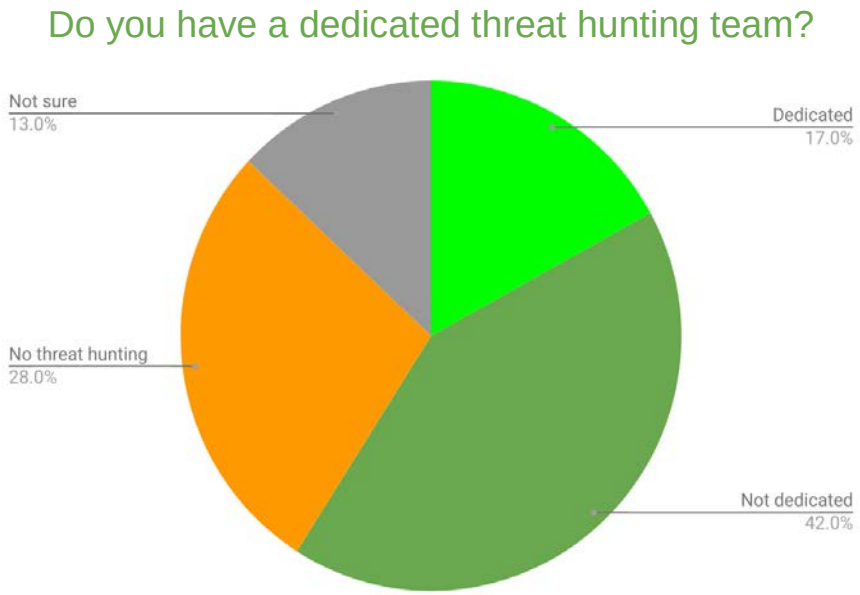

Figure 9: Only 17% of organizations have a dedicated threat hunting team

Case study: how a sophisticated security operator uses threat hunters

An organization we interviewed operates one of the most mature SOC and threat hunting operations on the planet. The company has over 250 full time employees dedicated to various aspects of threat hunting, incident response, and security operations. The core threat hunting team size is in the single digits, but they work closely with the incident response side of the house.

The hunting team focuses on discovering things that are not caught by commodity security defenses. For example, if they find a malware infection that is not detected by the current AV or custom signatures, the team would package up the signature of the new malware and ship it to the SOC, whose analysts would then use it in investigation and response actions.

Organizations with a mature threat hunting function are more likely to demand integrated investigation, triaging, and query capabilities. The lead threat hunter of this company told us: “Often a standard PCAP analysis is not enough for threat hunting purposes. We had to drop custom toolkits onto a system to collect specific data. That is a labor-intensive task -- any means to automate deep data gathering on a multitude of systems in an integrated fashion will have a huge impact on threat hunting.”

We are also seeing an increased use of machine learning and other advanced techniques in threat hunting. More specifically, a machine learning team may take datasets from the threat hunting team and develop specific models that capture patterns of new threats. The threat hunting team will then take the model to test and determine its relevance and effectiveness.

Interest in automated threat validation is high

In the threat hunting discussions, one issue that emerged repeatedly was that once a threat was detected, how easy would it be to validate whether the threat had already resulted in an incident (or could result in a real incident)? This is a critical for threat hunting. Without it, false positives will arise, which may significantly impact the efficacy of security operations. We asked our respondents if they would be interested in a technology that could automatically verify if a threat did anything malicious or could be malicious. The answer was overwhelmingly positive.

“Would you be interested in a technology that automatically validates if the threat did anything bad?”

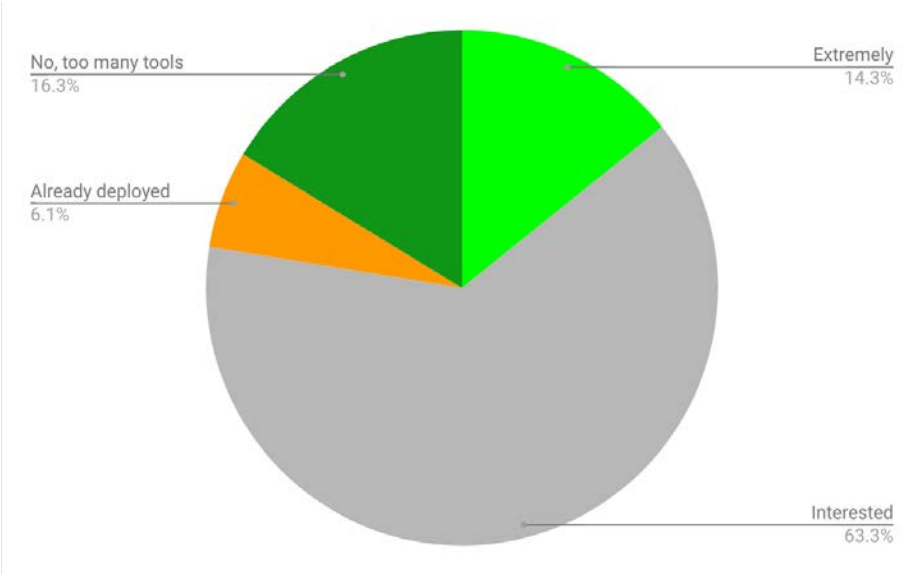

Figure 10: 78% are “interested” or “extremely interested” in a technology that automatically validates threats

As shown in Figure 10:

- **14% said they would be “extremely interested”** and in fact, they have been “waiting for a capability like this for a long time”
- **63% said they would be “very interested”**
- **6% indicated that they already had a tool** that provided this function, and
- **16% were reluctant** to bring in yet another functionality as they already had too many tools in their environment.

The interest in automatic threat validation is high. This is regardless whether the organization has a designated threat hunting function.

The verdict: threat hunting is immature but will significantly impact security operations

Overall, we found a wide spectrum of maturity in terms of threat hunting. A small percentage of companies are ahead of everyone else in terms of staffing, processes, and expertise for threat hunting, while the vast majority do very little in terms of proactive threat hunting and management. On the other hand, many organizations do recognize the value of threat hunting and expect to adopt hunting practices in the near future.

Conclusion

We conducted this study over the span of 3 months, interviewing and surveying over 50 users from different organizations, in an effort to understand how different organizations manage SOC, incident response, and threat hunting tasks.

Our study uncovered a number of strong findings. For organizations that want to operate efficient, highly effective security operations, we recommend following these best practices:

Do this now - take these immediate steps: Automating tier 1 and tier 2 analysts tasks, including alert collection, triaging, and common pivot actions. Refresh and establish key SOC metrics.

Next 3 to 6 months - plan these near-term tasks: Identify further opportunities for automation, such as common tasks or logic performed by SOC analysts. Shift investigation focus from identifying signatures and indicators to techniques, tactics, and procedures.

Beyond the next 6 months - prepare these for the longer term: Standardize processes and procedures for threat detection and response. Allocate resources to establish a proactive threat hunting practice.