<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>3</td>
</tr>
<tr>
<td>Key Survey Findings</td>
<td>4</td>
</tr>
<tr>
<td>Familiarity with Threat Hunting</td>
<td>5</td>
</tr>
<tr>
<td>Threat Hunting Priority</td>
<td>6</td>
</tr>
<tr>
<td>Top Challenges for SOCs</td>
<td>7</td>
</tr>
<tr>
<td>Confidence in SOCs</td>
<td>8</td>
</tr>
<tr>
<td>Data Captured for Forensic Review</td>
<td>9</td>
</tr>
<tr>
<td>Threat Detection by Automated Tools</td>
<td>10</td>
</tr>
<tr>
<td>Vulnerability Scanning &amp; Analysis</td>
<td>11</td>
</tr>
<tr>
<td>SOC Threat Management Maturity</td>
<td>12</td>
</tr>
<tr>
<td>Resources for Threat Hunting</td>
<td>13</td>
</tr>
<tr>
<td>Time Spent on Threat Hunting</td>
<td>14</td>
</tr>
<tr>
<td>Attack Discovery</td>
<td>15</td>
</tr>
<tr>
<td>Financial Impact of Threats</td>
<td>16</td>
</tr>
<tr>
<td>Threat Hunters’ Job Satisfaction</td>
<td>17</td>
</tr>
<tr>
<td>Threat Hunting Adoption</td>
<td>18</td>
</tr>
<tr>
<td>Barriers to Adoption</td>
<td>19</td>
</tr>
<tr>
<td>Threat Hunting Performance</td>
<td>20</td>
</tr>
<tr>
<td>Benefits of Threat Hunting Platforms</td>
<td>21</td>
</tr>
<tr>
<td>Threat Hunting ROI</td>
<td>22</td>
</tr>
<tr>
<td>Key Features of Threat Hunting Platforms</td>
<td>23</td>
</tr>
<tr>
<td>Methodology and Demographics</td>
<td>24</td>
</tr>
<tr>
<td>Threat Hunting Overview</td>
<td>25</td>
</tr>
<tr>
<td>Sponsor Overview</td>
<td>29</td>
</tr>
<tr>
<td>Contact Us</td>
<td>31</td>
</tr>
</tbody>
</table>
In 2017, the Information Security Community on LinkedIn conducted a comprehensive online research project to gain more insight into the state of threat hunting in security operation centers (SOCs). When the 330 respondents were asked what keeps them up at night, many comments revolved around a central theme of undetected threats slipping through an organization’s defenses. Many responses included “unknown” and “advanced” when describing threats, indicating the respondents understand the challenges and fear those emerging threats.

We would like to thank our sponsors for supporting this unique research:

Cybereason | DomainTools | Infocyte | Javelin Networks | Palo Alto Networks | Sqrrl | Tenable

We hope you will enjoy the report.

Thank you,

Holger Schulze

Holger Schulze
Founder
Information Security Community on LinkedIn
hhschulze@gmail.com
KEY SURVEY FINDINGS

1. Respondents state that the frequency of security threats their organizations are facing increased significantly. Over 80% of respondents say threats have at least doubled in the past year. Based on the current trend, the number of advanced and emerging threats will continue to outpace the capabilities and staffing of organizations to handle those threats.

2. Threat hunting is becoming a top security initiative for many organizations. However, the inability to detect advanced threats and find expert security staff to assist with threat mitigation are the top two challenges SOCs are facing. As a result, about four in five respondents stated their SOC does not spend enough time searching for emerging and advanced threats.

3. The main benefits of threat hunting platforms include improved detection of advanced threats, creating new ways of finding threats, and reducing investigation time. Threat hunting platforms can cut in half the time spent to detect a threat, and it improves the average time to investigate and address a threat by 42%. Nearly half of respondents state that an investment in a threat hunting platform pays for itself within a year given its ability to detect unknown, emerging and advanced threats.

4. Confidence in organizations’ ability to uncover advanced threats is low. Two-thirds of SOCs report that they are falling behind in terms of capabilities to address sophisticated threats. Confidence is further undercut by the increasing number of successful cyber attacks and the time it takes many organizations to detect and respond to a breach - many data breaches still have an average dwell time of 5 months.

5. Cybersecurity professionals who work with a threat hunting platform feel more appreciated, recognized, and valued by their organization. Virtually all respondents want to work for a SOC with lean-forward proactive security capabilities such as threat hunting, confirming the value respondents place on threat hunting capabilities to help them do their job more effectively.
Among the respondents to the threat hunting survey, six in 10 have some knowledge or are very knowledgeable about the topic. An additional 25% were aware of threat hunting but had no knowledge about the topic.

Q: How familiar are you with threat hunting?

18% I am very knowledgeable on threat hunting

15% I am unfamiliar with threat hunting

60% Have a moderate or high degree of knowledge about threat hunting

42% I have some knowledge on threat hunting

25% I am aware of threat hunting, but have no knowledge
Nearly four out of five respondents said that threat hunting should be or will be a top security initiative in 2017 with 42% saying that they strongly agreed with the statement. Over three-quarters of respondents believe threat hunting is of major importance.

Q: What is your level of agreement with the statement “Threat hunting should be or will be a top security initiative in 2017”? 

3/4 of respondents believe threat hunting is of major importance

- Strongly agree: 42%
- Somewhat agree: 37%
- Neither agree nor disagree: 11%
- Somewhat disagree: 6%
- Strongly disagree: 4%
The top two challenges facing SOCs are the detection of advanced threats (hidden, unknown, and emerging) and the lack of expert security staff to mitigate such threats. More than half of the SOCs face these two top challenges. All the challenges mentioned in the survey were ranked by at least 30% of the participants, suggesting that SOCs are dealing with a broad array of issues on a day-to-day basis.

Q: Which of the following do you consider to be top challenges facing your SOC?
The Challenges faced by SOCs, such as their inability to detect advanced threats, the lack of expert staff to assist, and the slow response time all weigh heavy on their level of confidence. Only 6% of respondents were fully confident in their SOC’s ability to uncover advanced threats; only 26% of respondents were confident to very confident.

Q: Using a scale of 1 to 5 where “5” is very confident and “1” not at all confident, how confident are you in your SOC’s ability to uncover advanced threats?
When asked about the type of data their SOC log for forensics review, three in four respondents said they log and review firewall/IPS denied traffic. Other commonly collected logs are firewall/IPS allowed traffic, DNS traffic, and Web and email traffic. The importance respondents see in keeping different types of logs for forensic review is evident by the fact that each data option was logged by at least 30% of the respondents.

Q: What kind(s) of data does your SOC log for forensic review later?

70% Firewall/IPS denied traffic
65% Web and email filter traffic
60% DNS traffic
58% Firewall/IPS allowed traffic
41% Server traffic
40% Packet sniff/tcpdump
33% Windows domain logs
16% Unsure
Nearly half of all threats go undetected by automated security tools (44%). Respondents’ answers ranged from single digits to more than 90%, implying that there is a wide range of perceived effectiveness of automated tools. Needless to say, this bodes very poorly for the current state of industry readiness.

Q: What percent of emerging and advanced threats are missed by automation security tools?

44% threats go undetected by automated security tools

Respondents overwhelmingly believe that their organization faced more security threats over the past year, with 82% saying threats occurred more frequently. In addition, nearly half (45%) stated the amount of threats they face have at least tripled or more in the past year.

Q: Which of the following best describes the frequency of security threats facing your organization?

- Increased at the rate of 5x or more: 12%
- Increased at the rate of 4x in the past year: 9%
- Increased at the rate of 3x in the past year: 24%
- Increased at the rate of 2x in the past year: 38%
- Not changed in the past year: 13%
- Decreased: 4%
Although identifying attacking threats seems to be of extreme importance to organizations, nearly 1 in 4 do not analyze vulnerabilities to determine if the threat is attacking a known CVE (Common Vulnerability and Exposure). 3 in 4 respondents stated they take measures to determine if a threat is attacking a known CVE for their organization.

Q: When threat hunting, do you run a network scan/analysis of common vulnerabilities to determine if the threat is attacking a known CVE?

76% YES

24% NO

Over 75% of respondents stated that vulnerability scanning and CVE patching is helpful in limiting potential threats. These results support the prior question in determining the importance of analyzing and acting on vulnerable areas for security purposes. Only a small minority believe that scanning for and patching CVEs is unhelpful.

Q: How useful do you find network vulnerability scanning/patching CVEs in helping you limit the risk of threats?

77% think vulnerability scanning and CVE patching is helpful in limiting potential threats

53% Very helpful

24% Somewhat helpful

7% Neither helpful nor unhelpful

12% Somewhat unhelpful

4% Very unhelpful
When it comes to the state of their organization’s threat hunting capabilities, only 6% actually believe they are cutting edge, and 30% believe they are advanced. Nearly two thirds of respondents stated they’re minimally compliant or even behind the curve when it comes to addressing emerging threats. Although emerging and advanced threats seem to be a major challenge for SOCs, little action is being taken to address them.

Q: Which of the following best explains the status of your SOC in relation to addressing emerging threats?

- We are cutting-edge, ahead of the curve: 6%
- We are advanced, but not cutting-edge: 30%
- We are compliant, but behind the curve: 37%
- Our capabilities are limited at this time: 27%
When asked for an approximate amount their organization spent on security detection and defense technologies to identify and stop advanced threats, answers varied significantly. On average, respondents stated approximately $550,000 with some amounts ranging up to $6-8 million dollars.

Q: Approximately how much do you spend on security detection and defense technologies to identify and stop advanced threats?

Less than 2 in 10 employees within SOCs are threat hunting today. When asked approximately what percentage of employees were involved in threat hunting, the average response was around 14%.

Q: Approximately, what percentage of employees at your SOC are threat hunting today?

14% SOC employees involved in threat hunting
When compared to engaging in proactive and innovative detection, respondents spend nearly double the time with alert triage and reacting to security threats. An average of 43% of respondents’ time is spent reacting to security threats, while an average of 22% of respondents said that their time is spent proactively seeking threats. The rest of the time is spent on other activities. These results align with previous questions that revealed that many respondents’ organizations are behind the curve when it comes to taking steps to enhance their security and threat hunting capabilities.

Q: In a typical week, what percent of your time is spent with alert triage or reactive response to security threats versus engaging in proactive and innovative detection methods?

A staggering 4 in 5 respondents believe their SOC does not spend enough time searching for emerging and advanced threats. While many organizations and SOCs spend most of their time reacting to detected threats or other procedures, respondents clearly believe more time should be spent on proactively looking for these threats. Only 20% of respondents believe that their SOC spends enough time searching for emerging and advanced threats.

Q: Do you feel enough time is spent searching for emerging and advanced threats at your SOC?
ATTACK DISCOVERY

Attackers dwell on a network for an average of **40 days** before they're discovered, according to the survey. Some respondents said attackers were discovered much faster while others said the attack could go undetected for as long as three months or even longer. Nearly all respondents agree that attackers dwell on a network for some period of time before they’re discovered by the SOC.

Q: On average, how long do attackers who breach your security defenses dwell in your network before they are discovered by your SOC?

An average of 40% of security threats to the respondent’s SOC are missed, while an average of 60% were identified. With over 4 in 10 security threats being missed by SOCs, there’s significant potential for a breach.

Q: Missed and Detected Security Threats?

- **40%** MISSED Security Threats
- **60%** DETECTED Security Threats
Nearly 2 in 5 respondents stated a security breach could have a financial impact of up to $1 million at their organization. Almost half of respondents were unsure of the financial impact an undetected threat that results in a breach would cause. This number represents a significant lack of awareness around the potential damage that undetected threats can cause.

Q: What is the typical financial impact of a security threat which goes undetected and results in a breach at your organization?

2 of 5 of respondents think a security breach could have a financial impact of up to $1 million at their organization.
THREAT HUNTERS’ JOB SATISFACTION

Overall, 61% of respondents in SOc without a threat hunting platform stated they feel appreciated, 53% say they are recognized, and 59% believe they are valued at their organization. However, respondents who work in a SOC that uses a threat hunting platform feel significantly more appreciated, recognized, and valued. Of those respondents, 72% state they feel appreciated, 61% state they are recognized, and 67% believe they are valued.

Q: Do you feel the work you do is: Appreciated?, Recognized?, Valued?

<table>
<thead>
<tr>
<th></th>
<th>WITH threat hunting platform</th>
<th>WITHOUT threat hunting platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appreciated</td>
<td>72%</td>
<td>61%</td>
</tr>
<tr>
<td>Recognized</td>
<td>61%</td>
<td>53%</td>
</tr>
<tr>
<td>Valued</td>
<td>67%</td>
<td>59%</td>
</tr>
</tbody>
</table>

Respondents overwhelmingly stated that they would prefer to work in a SOC with lean-forward proactive security capabilities such as threat hunting, an opinion shared by nearly 95% of respondents. Respondents value the importance of threat detection capabilities for not only their own work, but also for their organization.

Q: Would you prefer to work in a SOC with lean-forward proactive security capabilities, such as threat hunting?

YES 93%

NO 7%
Nearly two-thirds of respondents stated their SOC does not currently use a threat hunting platform for its security analysts, indicating a lower adoption rate. Respondents agree that the need and importance to identify emerging and advanced threats is paramount but many organizations have yet to adopt technologies to do so.

Q: Does your SOC currently use a threat hunting platform for its security analysts?

Among those who do not use threat hunting platforms, more than 3 in 4 (76%) stated they would like to see their organization upgrade security capabilities by purchasing a threat hunting platform. This supports the themes in which detecting advanced threats is a major challenge to SOCs, magnified by a lack of expert staff, and the fact respondents believe not enough time or budget is allocated to threat hunting tools.

Q: Would you like your organization to purchase a threat hunting platform for its security analysts?
**Lack of budget remains the top reason** why SOCs have not adopted a threat hunting platform, an answer given by 35% of respondents. Lack of training on threat hunting was the second most common reason, said 20% of respondents. This puts more responsibility on threat hunting platforms to prove their value, accelerate onboarding times and improve comprehension with SOC staff.

Q: What is the main reason your SOC does not have a threat hunting platform for its security analysts?
When asked to estimate the amount of time it takes to address threats without a threat hunting platform, the average time it took to “detect” a threat was 38 days, and the average time to “investigate” a threat was 26 days.

Q: On average, how long does it take to detect / investigate threats without a threat hunting platform at your SOC?

When asked to estimate the same time to “detect” and “investigate” threats with a threat hunting platform, a much different story emerged. With a threat hunting platform, the average time spent to “detect” dropped to 15 days and the average time to “investigate” the threat lasted just 14 days. The average time spent to detect the threat improved by 61% and investigating the threat improved by 42%.

Q: On average, how long does it take to detect / investigate threats with a threat hunting platform at your SOC?
The top efficiency benefits from a threat hunting platform as mentioned by respondents were **improving the detection of advanced threats (72%)**, creating new ways of finding threats (68%), discovering threats they could not discover otherwise (67%), and reducing investigation time (66%).

Q: What do you think are the main efficiency benefits from a threat hunting platform for security analysts?

- **72%** Improving detection of advanced threats
- **68%** Creates new ways of finding threats
- **67%** Discovering threats I could not discover otherwise
- **66%** Reducing investigation time
- **58%** Saves time manually correlating events
- **56%** Reducing time wasted on chasing false lead

Ability to quick connect disparate sources of information 43% | Reducing extra and unnecessary noise in the system 41% | Reduces attack surface 40% | Saves time scripting and running queries 39% | Other 4%
Nearly half of respondents believe an investment in a threat hunting platform would pay for itself within a year. A small minority of respondents stated the investment in a threat hunting platform would take three years or more to break even.

Q: How long does it take for a SOC to break-even on the investment of a threat hunting platform?

44% believe the investment in a threat hunting platform would pay for itself within a year.
The most appealing features of a threat hunting platform are the forensic details and automated analytics (machine learning used for automating decisions). All features carried some appeal with respondents. None of the features received an average score below a “3” on a 1 to 5 scale of appeal.

Q: Using a scale of 1 to 5 where “5” indicates very appealing and “1” indicates not at all appealing, how appealing is each of the following when selecting a threat hunting platform?
The 2017 Threat Hunting Report is based on the results of an online survey of over 330 cybersecurity and IT professionals to gain more insight into the state of threat management in SOCs. The respondents range from security analysts and IT managers to CISOs. The respondents represent a representative cross section of organizations of varying sizes across many industries, ranging from financial services to telecommunications and healthcare.

### PRIMARY ROLE

<table>
<thead>
<tr>
<th>Role</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Analyst</td>
<td>20%</td>
</tr>
<tr>
<td>IT Manager, Director or CIO</td>
<td>19%</td>
</tr>
<tr>
<td>Security Manager or Director</td>
<td>19%</td>
</tr>
<tr>
<td>CSO, CISO, or VP of Security</td>
<td>15%</td>
</tr>
<tr>
<td>Security Administrator</td>
<td>11%</td>
</tr>
<tr>
<td>Threat Analyst</td>
<td>6%</td>
</tr>
<tr>
<td>Systems Administrator</td>
<td>5%</td>
</tr>
<tr>
<td>Auditor</td>
<td>4%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
</tr>
</tbody>
</table>

### COMPANY SIZE

<table>
<thead>
<tr>
<th>Size Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 100</td>
<td>22%</td>
</tr>
<tr>
<td>100 to 499</td>
<td>15%</td>
</tr>
<tr>
<td>500 to 999</td>
<td>11%</td>
</tr>
<tr>
<td>1,000 to 4,999</td>
<td>19%</td>
</tr>
<tr>
<td>5,000 to 9,999</td>
<td>13%</td>
</tr>
<tr>
<td>10,000 or more</td>
<td>20%</td>
</tr>
</tbody>
</table>

### INDUSTRY

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial services, banking or insurance</td>
<td>20%</td>
</tr>
<tr>
<td>Telecommunications or ISP</td>
<td>14%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>9%</td>
</tr>
<tr>
<td>Government</td>
<td>8%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>6%</td>
</tr>
<tr>
<td>Retail or ecommerce</td>
<td>5%</td>
</tr>
<tr>
<td>Energy or utilities</td>
<td>4%</td>
</tr>
<tr>
<td>Other</td>
<td>33%</td>
</tr>
</tbody>
</table>
THREAT HUNTING OVERVIEW
Today’s attacks have become more sophisticated while their means and methods are increasingly difficult to detect. Upon gaining access to a network, most advanced persistent threats (APTs) work silently and stealthily to gather intel and gain more access to their target network. In the past, APTs using this methodology were extremely difficult to detect and sometimes were active for months or even years before being discovered. However, many SOCs are beginning to take the fight to the enemy by employing threat hunting techniques to seek out malicious activity before it is able to do significant damage.

Mapping to the Cyber Kill Chain

The clear majority of attacks faced by organizations today can be mapped via the cyber kill chain model. Under this framework, attackers will start out by gathering intelligence on and surveilling a network, exploiting weaknesses, and moving on to escalating privileges. However, at every level of the kill chain, attackers are vulnerable to detection and potential disruption.

By understanding how attackers utilize the kill chain, hunters can engage their targets before adversaries compromise or steal valuable information. In other words, monitoring, targeting, and engaging threats before they cause damage. In this process, hunters will start out by hypothesizing and mapping out potential means and methods that can be used by attackers. Hunters should therefore be able to collect actionable intelligence that enables them to further refine their data-gathering techniques and provides jumping-off points for future hunts.
All attackers have signatures that can be used to identify who is attacking and how. These can include anything from the attacker’s IP address, network/host artifacts, and tactics, techniques and procedures (TTPs). Collectively, these methods are referred to as Indicators of Compromise (IoCs). By identifying relevant IoCs and denying their use, hunters can make attacks upon their networks more time-consuming, costly, and difficult. In short, by picking out IoCs through the use of behavioral analytics, intelligence gathering, etc., hunters can pinpoint and deny potential avenues of approach to malicious actors.

This method of disrupting threats is encapsulated within the “pyramid of pain” model. The pyramid maps the levels of IoC that are used by adversaries and correlates them with the relative amount of inconvenience that can be caused by forcing attackers to change their techniques. By relying on behavior and data-driven intelligence (as opposed to reactive automated defenses), hunters are able to predict the tactics most likely to be used by adversaries.
Each organization’s ability to seek out IOCs can be mapped according to the hunting maturity model. The framework rates SOCs on their ability to utilize intelligence indicators and data collection to predict and identify threats. SOCs are assessed on their defense techniques (e.g. entirely automated vs intelligence-driven), their collection and use of data, and their adaptability. The model also evaluates SOCs based on the frequency, sophistication, and institutionalization of their hunt techniques.

This model provides SOCs with a broad-view outline for assessing their effectiveness, as well as laying out a roadmap for improving operational effectiveness. Under this framework, the most effective SOCs are those that consistently incorporate intelligence and “lessons learned” from hunts into alerts and automated responses, as well as those that invest in specialized, scalable tools for hunters.
Cybereason | www.cybereason.com

Cybereason is the leader in endpoint protection, offering endpoint detection and response, next-generation antivirus, and managed monitoring services. Founded by elite intelligence professionals born and bred in offense-first hunting, Cybereason gives enterprises the upper hand over cyber adversaries.

DomainTools | www.domaintools.com

DomainTools helps security analysts turn threat data into threat intelligence. Our solutions give organizations the ability to use create a forensic map of criminal activity, assess threats and prevent future attacks.

Infocyte | www.infocyte.com

Infocyte is an endpoint threat hunting technology leader with an innovative solution that focuses on post-compromise detection of persistent attackers and cyberthreats. Infocyte’s agentless hunt platform is designed to allow security and IT teams to rapidly assess endpoints for evidence of compromise to defend an organization’s networks and critical information.

Javelin | www.javelin-networks.com

Javelin protects what others cannot - the Active Directory. Javelin is the first Artificial Intelligence-based Autonomous Breach Detection, Investigation, Hunting and Containment Platform to protect the Corporate Domain environment. Javelin’s lean forward approach reduces the effort, time and error when trying to identify and contain breaches.
Palo Alto Networks  |  www.paloaltonetworks.com

Palo Alto Networks is the next-generation security company, leading a new era in cybersecurity by safely enabling applications and preventing cyber breaches for tens of thousands of organizations worldwide. Built with an innovative approach and highly differentiated cyberthreat prevention capabilities, our game-changing security platform delivers security far superior to legacy or point products, safely enables daily business operations, and protects an organization’s most valuable assets.

Sqrrl  |  www.sqrrl.com

Sqrrl is the only cybersecurity solution purpose-built for threat hunting. Sqrrl’s primary value proposition is to help analysts discover new, unknown threats that were neither previously detected nor properly prioritized.

Tenable  |  www.tenable.com

Tenable transforms security technology through comprehensive solutions providing continuous visibility and critical context, enabling decisive actions to protect organizations of all sizes. Tenable eliminates blind spots, prioritizes threats and reduces exposure and loss.
Interested in co-sponsoring the next cybersecurity report, or producing your own research?

Contact Crowd Research Partners to learn more.
✉️ info@crowdresearchpartners.com