DARKReading RESEARCH

JANUARY 2021

THE STATE OF THREAT
Detection and Response

ANOMALI®

Executive Summary

Many organizations have invested in improving their threat detection capabilities over the past two years and express increased confidence in their ability to stop threats that have penetrated the network perimeter. However, these organizations also cite a number of weaknesses and areas for further improvement, including limited log visibility, limited threat visibility, and an over-reliance on manual processes. A plurality of organizations point to their security information and event management (SIEM) platform's limited view of events as a central issue and believe that greater process automation and intelligence-driven threat detection are critical to risk mitigation and management.

In May 2020, Dark Reading surveyed IT and cybersecurity professionals to understand how enterprises are detecting and responding to threats that have breached their network perimeter. The survey, conducted on behalf of Anomali, polled respondents on the technologies and processes they are using to detect threats, identify exposure to specific exploits, and search for incursions in historic log data. The resulting findings were used as the basis of this report.

The State of Threat Detection and Response

Security teams are under growing pressure to improve threat detection and response capabilities at their organizations. In recent years, attackers have shown a consistent ability to breach perimeter defenses and remain undetected on enterprise networks for extended periods. Many organizations have experienced major data breaches and financial consequences because they failed to detect a breach or a security threat quickly enough.

It's by now an industry truism that a security strategy focused solely on blocking threats at the network perimeter is no longer adequate. To reduce attacker dwell time and minimize damage, security teams need to be able to quickly detect threats that have penetrated the perimeter, assess their exposure to it, and initiate an appropriate mitigation plan. To do this effectively, organizations need the ability to search their event log data for threats back to the point in time when the threat started to be active—often years in the past—which is a challenge for the current generation of SIEM tools.

Many organizations have invested in tools such as IDS, EDR systems, and SIEM software as the core components of enterprise defense strategies. Far fewer have deployed additional advanced capabilities for identifying threats on their networks.

Tools and Technologies in Use

For years, organizations have relied on SIEMs, intrusion detection systems (IDS), and a diverse set of other technologies to help identify threats inside the network perimeter. Some have invested in tools for automating parts of the threat detection and response process and for extracting more value from the vast amount of security and event data generated on their networks each day. Many of these tools continue to be a core component of enterprise defense strategies.

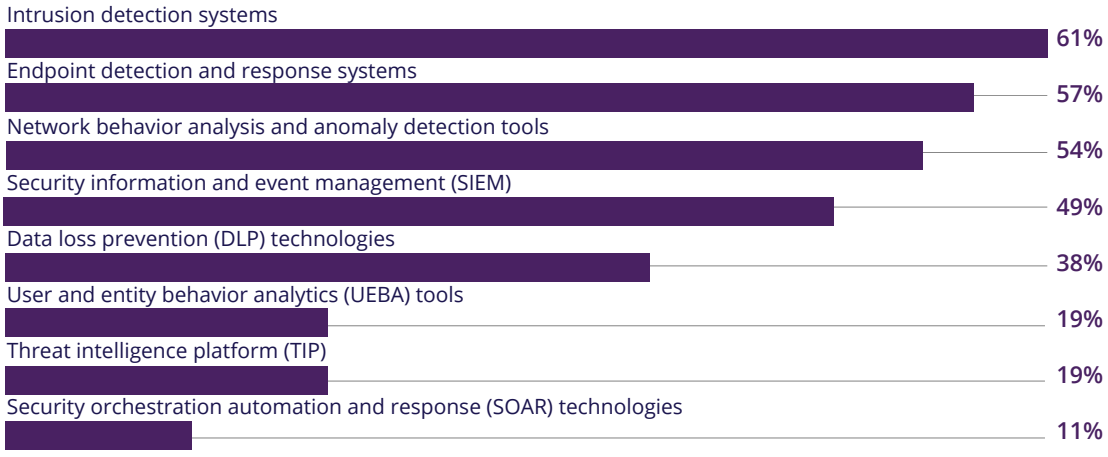
The Anomali and Dark Reading survey showed that 61% of organizations have an IDS; 57% use endpoint detection and response (EDR) tools; and 54% have some kind of network behavior analysis and anomaly detection capability (Figure 1). Nearly half (49%) of organizations use a SIEM to aggregate and correlate security information and event management data, and 38% have data loss prevention (DLP) controls.

A smaller proportion of organizations have deployed additional advanced capabilities for identifying threats on their network. For instance, 19% have user entity behavior analytics (UEBA) tools to alert them to suspicious or anomalous activity. These tools can be especially useful in identifying criminals using legitimate credentials and tools to operate within a breached network. About a fifth (19%) use a threat intelligence platform to collect and correlate threat data gathered from internal and external sources. Eleven percent use a security orchestration, automation, and response (SOAR) system to automate responses to identified threats on the network. Survey data showed that a greater proportion of larger organizations are using DLP, SOAR, UEBA, and threat intelligence platforms (TIPs) compared to smaller organizations with less than 1,000 employees. For instance, 59% of organizations with more than 1,000 employees use DLP compared to 23% of organizations with less than 1,000 employees. Similarly, 33% of larger organizations use TIPs compared to 9% of the smaller ones.

Figure 1

Detecting Threats

What tools and technologies do you use for detecting threats that have penetrated the network perimeter or are within your organization?

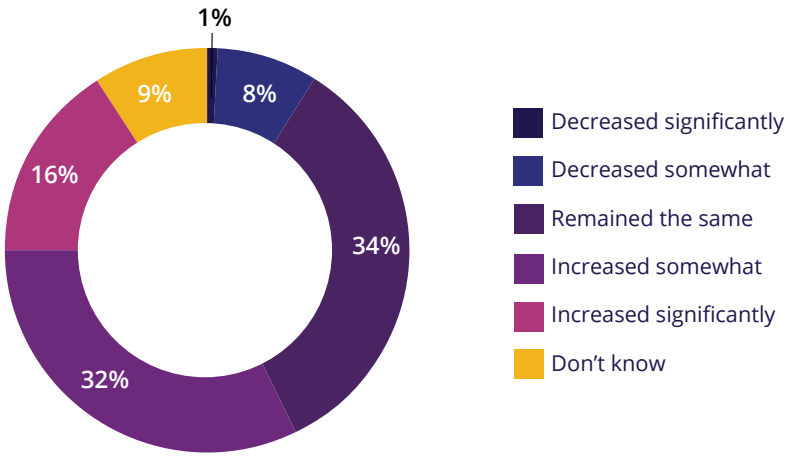


Note: Multiple responses allowed
Data: Dark Reading survey of 147 IT and cybersecurity professionals, May 2020

Figure 2

Change in Ability to Detect Threats

Over the last two years, how has your ability to detect threats on your network changed?



Data: Dark Reading survey of 147 IT and cybersecurity professionals, May 2020

Signs of Progress

When asked to assess their organization's threat detection capabilities, 48% of the IT and cybersecurity professionals in our survey described them as having improved either "significantly" or "somewhat" over the last two years (Figure 2). Some of the stated reasons for the self-assessed improvement included increased automation, increased use of SIEM and endpoint software, and, finally, accumulated experience. More than one-third (34%) assessed their detection ability as having remained unchanged over the same period.

Highly Secure? Or Misplaced Confidence?

While improvement over time is relative, many respondents in the Anomali and Dark Reading survey expressed a high level of confidence in their ability to detect threats inside the network. They claimed to have a level of responsiveness and speed that would indicate excellence at detecting and mitigating threats. However, other data points from the same respondents — such as those pertaining to process limitations and the ability to derive full value from a SIEM — suggest this confidence may be misplaced.

Sixty percent said they were able to detect most new threats in one day or less, and 16% claimed to be able to do it in near-real-time (Figure 3).

A noticeably smaller proportion of organizations appeared to have reservations about their ability to detect threats or to prevent perimeter breaches. Just 9% of organizations perceived their ability to detect network threats as having decreased over the past two years. Twenty percent described their detection capabilities as "fair" to "poor" and said they took anywhere from one day to more than one week to detect new threats.

Figure 3

Many of our survey respondents expressed a high level of confidence in their ability to detect threats inside the network. However, other data points from the same respondents — such as those pertaining to process limitations and the ability to derive full value from a SIEM — suggest that confidence may be misplaced.

Organization's Ability to Detect Threats

How would you rate your organization's ability to detect threats that have made it inside the network?

Data: Dark Reading survey of 147 IT and cybersecurity professionals, May 2020

Similar to their views on detection, many had the same upbeat assessment about their ability to stop threats at the network perimeter. Forty-eight percent said they were able to stop between 90% and 99% of threats, and 9% claimed they were able to block all attacks at the network perimeter (Figure 4). In general, the proportion of respondents that described themselves as doing a poor job blocking threats at the network perimeter was substantially smaller than the proportion that had an optimistic view. Twenty-seven percent, for instance, said they were able to block only between 50% and 89% of the attacks they encountered, and 9% admitted to being able to block less than 50% or none at all.

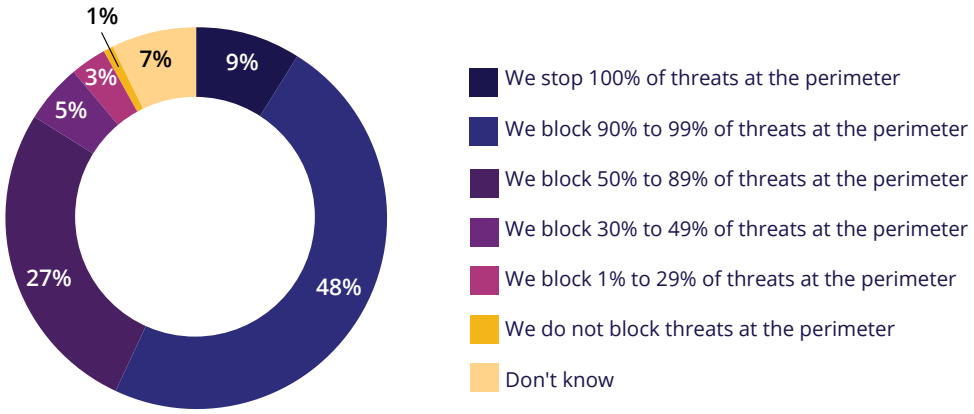
As discussed above, the Anomali and Dark Reading survey data showed that a majority of organizations feel they have improved threat detection capabilities or have maintained the status quo over the past two years. At the same time, the data also pointed to multiple barriers to continued progress and suggested that at least some IT and security professionals might be overestimating their organization's detection and response capabilities. Of particular concern were limitations in the processes that organizations have in place for:

1) quickly identifying exposure to specific threats,
2) analyzing historical data against new and existing threats, and
3) ingesting and operationalizing threat intelligence.

Figure 4

Effectiveness at Stopping Threats

How effective is your organization at stopping threats at the network perimeter?



Data: Dark Reading survey of 147 IT and cybersecurity professionals, May 2020

Most SIEM Alerts Ignored

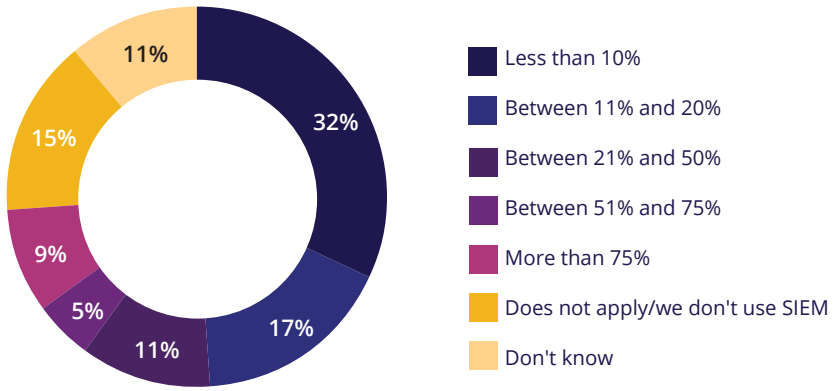
As many previous studies have showed, our survey highlighted that a majority of organizations are not investigating a large portion of their daily SIEM alerts. About half (49%), for instance, investigate a mere 20% or less of the alerts they receive, and 11% follow up on between 21% and 50% of them (Figure 5).

A meager 9% of organizations investigate 75% or more of their SIEM alerts. SIEM platforms capture, analyze, and correlate log and event data from across the enterprise to surface actionable alerts. The technology is intended to be a linchpin in defending enterprises against security threats on the network. The fact that many organizations are continuing to ignore a majority of the alerts suggests they are not in a position to fully derive value from their SIEM investments.

Figure 5

Percentage of Alerts Investigated

How many of those alerts on average do you investigate?



Data: Dark Reading survey of 147 IT and cybersecurity professionals, May 2020

No matter the specific threat mix for any given organization, the end result is IT teams are being stretched thin by the resulting problems.

Retrospective Blind Spots

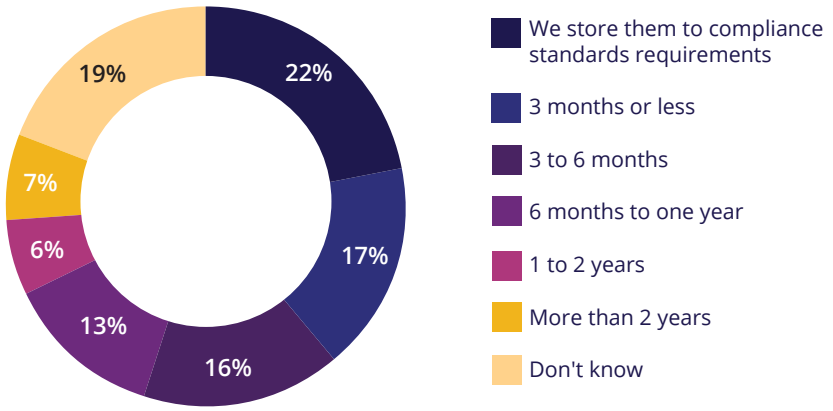
An equally critical issue limiting the ability of organizations to detect threats quickly is the amount of log data immediately available for retrospective threat analysis. For example, when a new threat is discovered that was active at some time in the past, security teams need to be informed by an analysis of log data to determine their historical exposure to the issue. A newly discovered threat that might not be evident in current data can sometimes lurk hidden in logs from a year ago or even further back. Unfortunately, SIEMs are generally optimized for real-time, forward-looking threat detection, and many struggle to do retrospective analysis, which requires complex manual queries and search times measured in hours or days.

In addition, retrospective analysis is limited by the amount of historical data that is kept online and searchable in a SIEM. The Anomali and Dark Reading survey showed that one-third of organizations keep six months or less of their SIEM platform log data available online for active analysis, meaning their ability to look for threats in older data is severely limited. Only 13% of respondents store between six months and one year's worth of log data for SIEM analysis, and 6% store one to two years' worth of data (Figure 6). A mere 7% said they have the ability to search through more than two years' worth of log event and security data for signatures and patterns similar to known or new threats, indicators of compromise (IoCs), and vulnerabilities.

Figure 6

Hot Storage of Online Data

How long do you store data online or keep it available in your SIEM for active threat analysis?

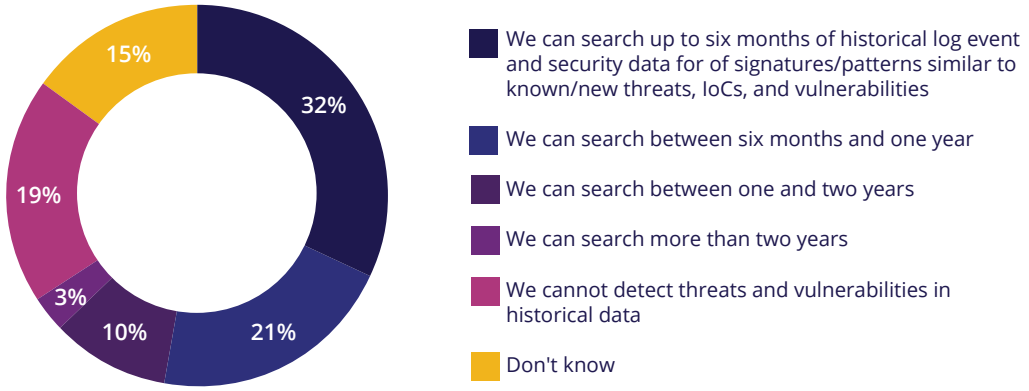


Data: Dark Reading survey of 147 IT and cybersecurity professionals, May 2020

Figure 7

Searching Historical Data

When you receive newly discovered threat intelligence/IoCs, how far back do you look for potential matches in your historical data?



Data: Dark Reading survey of 147 IT and cybersecurity professionals, May 2020

Twenty-two percent said they store such data for whatever period necessary to comply with regulatory requirements. These requirements can vary by industry and regulation. The Payment Card Industry Data Security Standard (PCI DSS), for instance, requires covered entities to keep three months' worth of log data available for immediate analysis and for logs to be stored for a period of at least one year. HIPAA requires logs to be stored for at least six years with a minimum of six months' worth of log data available for analysis in an uncompressed format.

Nearly one-fifth (19%), did not currently have the ability to detect threats and vulnerabilities in historical data at all (Figure 7).

Pricing and Scalability Concerns Limit Searchability

Cost and related scalability concerns appear to be major reasons why at least some organizations keep only a limited amount of log data available in their SIEM for active analysis. Thirty-two percent identified those two issues as factors limiting their ability to get the most from their SIEM (Figure 8). Seventeen percent described their SIEM platform as not being large enough to ingest all the data pouring into it from different sources. Unsurprisingly, 37% of organizations identified the time it took them to search through old data as one of their biggest challenges around detecting previously unidentified threats in older events (Figure 9).

Figure 8

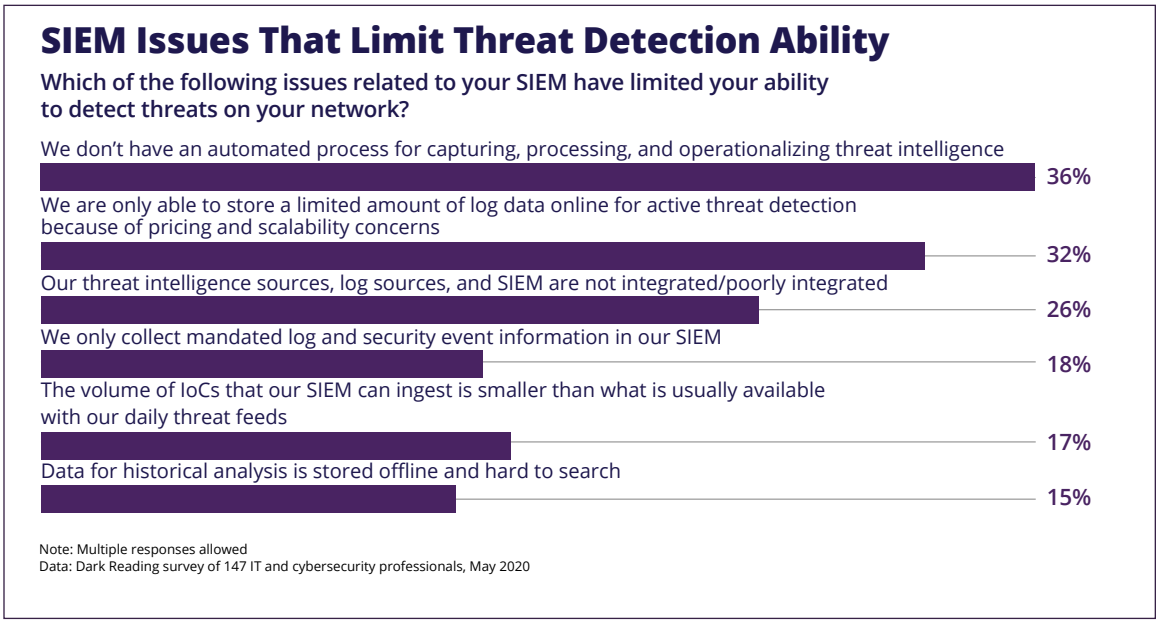
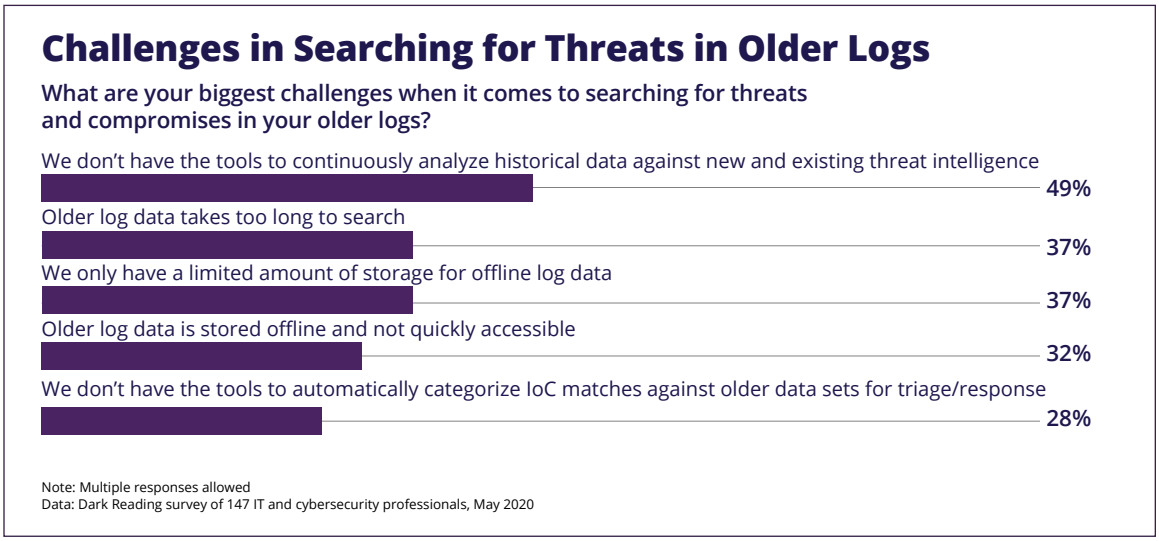


Figure 9



Additionally, a substantial number of organizations appear to be struggling to integrate their log sources, intelligence sources, and SIEM. Although many organizations use a SIEM, the technology is still widely regarded as being complex to manage because of the challenges in integrating the platform with the rest of the security infrastructure.

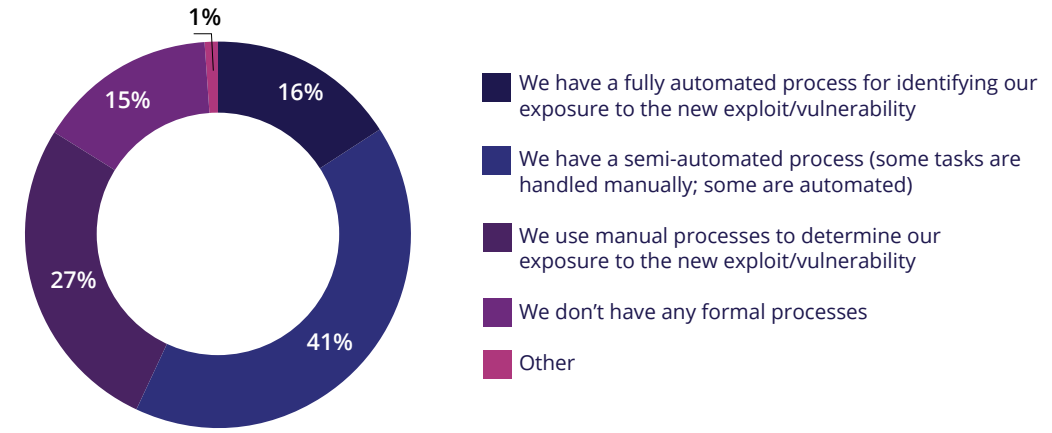
On top of that, organizations that subscribe to multiple threat feeds need to find a way to standardize and integrate the feeds with the SIEM. For 26% of organizations, these integration issues are limiting their ability to detect threats on the network."

Figure 10

A majority of organizations are hampered by a lack of automation in managing threats properly. Without appropriate automation, security analysts can end up spending most of their time just gathering and analyzing information with little opportunity to investigate and act upon it.

Process for Identifying Exposure to Vulnerability

When a new exploit or vulnerability is announced, what is your process for identifying your organization's exposure to the specific exploit or vulnerability?



Data: Dark Reading survey of 147 IT and cybersecurity professionals, May 2020

Detection Still a Heavily Manual Game

A majority of organizations are also hampered by a lack of automation. To manage threats properly, security analysts need to be able to analyze and triage alerts surfaced by their intrusion detection systems and prioritize responses based on the risk that a specific threat might pose to different systems. Often this means being able to collect, ingest, and consume external threat data and mapping it with internal telemetry so that a threat can be put into proper perspective. The massive volume of log and security event data generated daily on modern enterprise networks can make this task impossibly hard using manual processes alone. Without appropriate automation, security analysts can end up spending most of their time just gathering and analyzing information with little opportunity to investigate and act upon it.

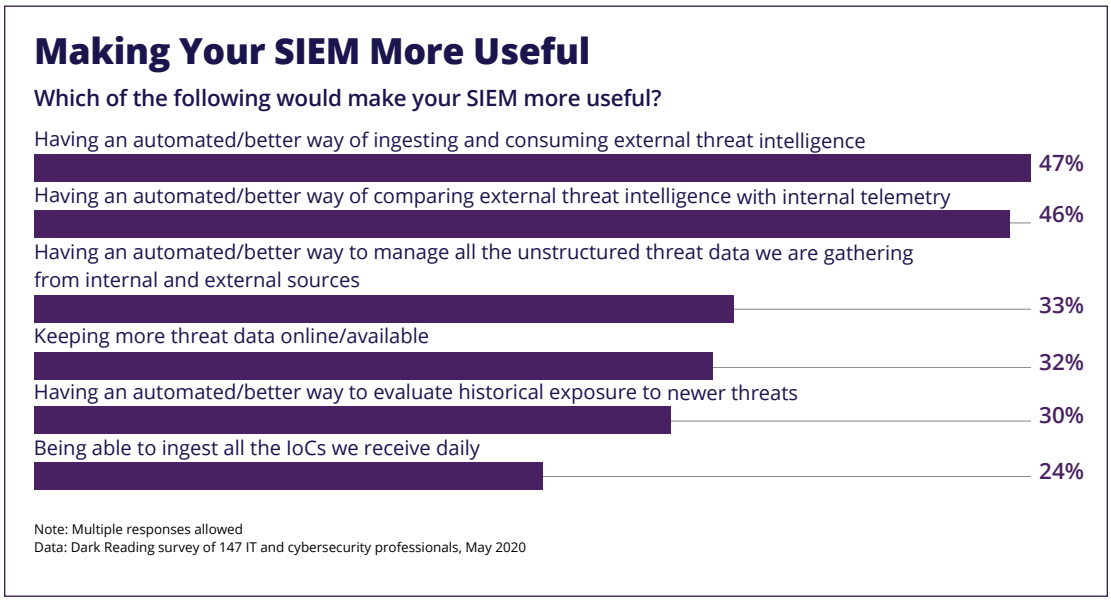
Some 68% of respondents in the Anomali and Dark Reading survey said their ability to identify organizational exposure to a new security threat was limited because they only had semi-automated or manual processes in place (Figure 10). Forty-nine percent said they did not have the tools to continuously analyze historical data against new and existing threat intelligence (Figure 9).

Lack of Automation Hampering Visibility

The news on the threat visibility front wasn't all that great either. Although many respondents rated their organization's threat detection capabilities highly, they also acknowledged relatively big gaps in their ability to leverage threat intelligence more effectively. External threat intelligence feeds provide enterprises with vital information on new and emerging threats, vulnerabilities, ongoing

Figure 11

Many organizations are confident they could derive better value from their SIEM investments if they had a more automated process for managing external threat intelligence and correlating it with internal telemetry. Capabilities that give security analysts a way to quickly prioritize and respond to detected threats are key.



attack campaigns, and adversary information including emerging tactics, techniques, and procedures (TTPs). By correlating this intelligence with telemetry from internal systems, organizations can get an ongoing and contextual understanding of their cyber exposure.

Our survey showed that 47% of organizations are not fully satisfied with their current capabilities for ingesting and consuming threat intelligence (Figure 11).

That directly contradicts the confident sentiment that many respondents expressed about their ability to quickly detect and respond to threats on the network. A nearly identical proportion (46%) wished they had a more automated or better way to compare external threat intelligence with internal telemetry, and one-third wanted a better way to make use of all the unstructured threat data they were gathering from internal and external sources. The SIEM's limited view of events, as previously noted, was another concern, with 24% saying they wished they could ingest all daily IoCs, and 32% saying their SIEM would be more useful if they had more threat data readily available online for threat analysis.

Getting All the Value From Your SIEM

Many organizations are confident they could derive better value from their SIEM investments if they had a more automated process for managing external threat intelligence and correlating it with internal telemetry. They view the ability of their SIEM platform to keep more data online for analysis as critical to properly evaluating current and historical exposure to new threats. Better integration between the SIEM platform and internal and external threat data sources is also perceived as critical to a good threat defense.
The survey data suggests that many organizations could benefit from using more of their event log data and more of the available threat intelligence. Such a solution would leverage diverse threat intelligence sources for full visibility into relevant threats and allow organizations to store event log data for considerably longer than currently possible, incorporating it into the analysis of new threats. Key attributes prioritized by respondents include alerts to be sent back into SIEM and SOAR environments as well as automatically associating detected threats to adversary TTPs. Also important are capabilities that give security analysts a way to quickly prioritize detected threats — and respond to them — based on asset value, vulnerability, and risk score.

Conclusion

Many organizations appear to have invested in bolstering their capabilities for detecting and responding to threats on the enterprise network over the past two years. They are using a diverse set of technologies such as SIEM, IDS, EDR, and network analytics tools to find and contain threats that have penetrated the network perimeter. While a majority of security and IT professionals in the Anomali and Dark Reading survey perceived themselves as being able to mitigate new threats quickly, they also identified several factors that are hampering further progress.

Among them are limited threat visibility, data integration challenges, an inability to easily perform historical log analysis, and a lack of automation.

About Anomali

Anomali® delivers intelligence-driven cybersecurity solutions, including Anomali ThreatStream®, Anomali Match™, and Anomali Lens™. Private enterprises and public organizations use Anomali to gain unlimited visibility, speed time to detection, and constantly improve security operations. Anomali customers include more than 1,500 global organizations, many of the Global 2000 and Fortune 500 companies, and large government and defense organizations around the world. Founded in 2013, it is backed by leading venture firms including GV, Paladin Capital Group, Institutional Venture Partners, and General Catalyst.

Learn more at **www.anomali.com**

Survey Methodology

Dark Reading conducted a research survey on behalf of Anomali in May 2020. The survey collected responses from 147 IT and cybersecurity professionals with titles such as IT director, CIO/CTO, CSO, cybersecurity manager, and cybersecurity staff at predominantly North American companies. The questions were designed to uncover how enterprises are detecting and responding to threats that have breached their network perimeter. The survey polled respondents on the technologies and processes they are using to detect threats, identify exposure to specific exploits, and search for incursions in historic log data.

Respondents represented small, medium, and large organizations from more than 12 industries including banking and financial services, healthcare, information technology, communications, services, and aerospace. Informa Tech research was responsible for all aspects of survey administration, data collection, and data analysis. Informa is the parent company of Dark Reading. These procedures were carried out in strict accordance with standard market research practices and existing US privacy laws.