Report Summary: Unlocking High Fidelity Security 2019

By David Monahan

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) End-User Research Summary
July 2019

Sponsored by:

endace

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Report Summary: Unlocking High Fidelity Security 2019

Table of Contents

Report Summary:
Unlocking High Fidelity Security 2019

Executive Summary

Change is happening at a rapid pace in cybersecurity. The technology landscape is especially volatile, with new solutions and capabilities delivered daily. Especially intriguing is the evolution of breach simulation technology using vulnerability, asset, and patch information to find gaps in controls and accelerate risk reduction. This is a standalone technology that vulnerability and management vendors are creating and acquiring. Another area that is gaining ground quickly is packet capture. Respondents identified network data as the best means of early breach detection, but also identified the value of packet capture as a primary source. While 67% of organizations are using flow data, 74% are using information collected from packet capture for incident investigation.

The research identified that 78% of organizations are less than wholly comfortable with their current cyber risk, and 12% are moderately to very uncomfortable with their cyber risk. There are communication gaps between frontline operations, middle management, and executive leadership that lead to disparities in perception in program efficacy and maturity, as well as perception of cyber risk. Frontline personnel are only about half as comfortable with the organization's cyber risk as the senior leadership. In every case reviewed for program efficacy or maturity, senior management was more positive or confident than the frontline operations personnel.

At the same time there is concern over cyber risk, 87% of organizations indicate they feel their current controls are effective in protecting critical assets. This seems to present more of a security bravado than a real efficacy, especially considering 29% of organizations indicated they are not able to identify or stop a compromise until somewhere between the lateral movement phase and post event—a.k.a. way too late. Additionally, only 28% of organizations believe they are fully effective in proactively identifying security controls gaps.

Though the situation is improving in many ways year over year from both internal cooperation and vendor solution improvements, a lack of data sharing and integrations continue to impact security. Ninety-one percent of senior management believe security has access to all or most all of the data security operations teams need to be successful in their investigations, while only 64% of frontline personnel feel the same. That is a 27% gap!

Managed security services (MSS) continue to attract clients, but the primary driver is not the lack of people or skills. Eighteen percent of organizations surveyed are spending more than 50% of their security budgets on MSS, with 24x7 monitoring being the number-one service consumed and considered for purchase by new adopters. Forty-two percent of senior management believe that the information they receive from their MSS are significantly more accurate than the information they receive from their internal team, while only 26% of frontline management feel the same.

Another issue for security teams is that only 47% believe they have all the tools they need to be fully effective, but fortunately only 8% believe they are nowhere close to where they need to be. The numbers are similar for skillsets. Fifty percent believe they have all the skills they need in security to be successful and only 9% feel they are nowhere close.

Over 68% of organizations believe they need more frequent security controls testing, with those performing tests more frequently than annually being the biggest proponents of doing so. Respondents recognize that more automation is needed to find and close controls gaps, and also perform incident response and remediation. For choosing automation, tools accuracy is the number-one consideration. Avoiding accidental outages due to inaccurate logic, decision making, or execution was a key concern.

More details on these topics and other related aspects are shared in the report.

Demographics Overview

Respondents were required to have primary market operations in North America. Other global target markets were captured.

Which regions are your organization's primary/target market(s)?

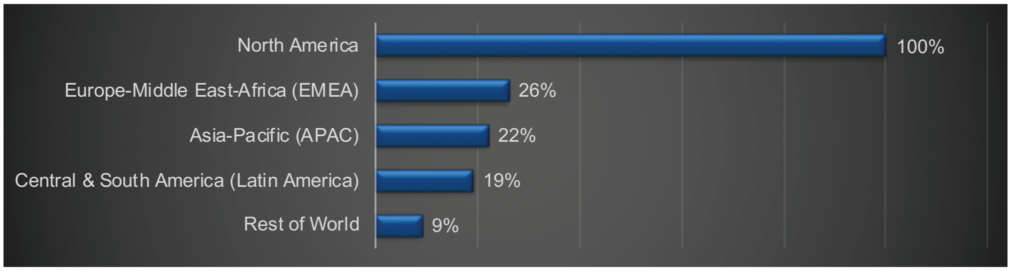

Figure 1: Respondent Target Markets

The report surveyed management and individual contributors, along with IT personnel in various operational roles. The following chart shows the breakout of the respondents' roles. Segmenting respondent roles is often crucial to identifying disconnects between management perspectives and what is often a different reality observed by the frontline operations personnel.

Which of the following best describes your role in the organization?

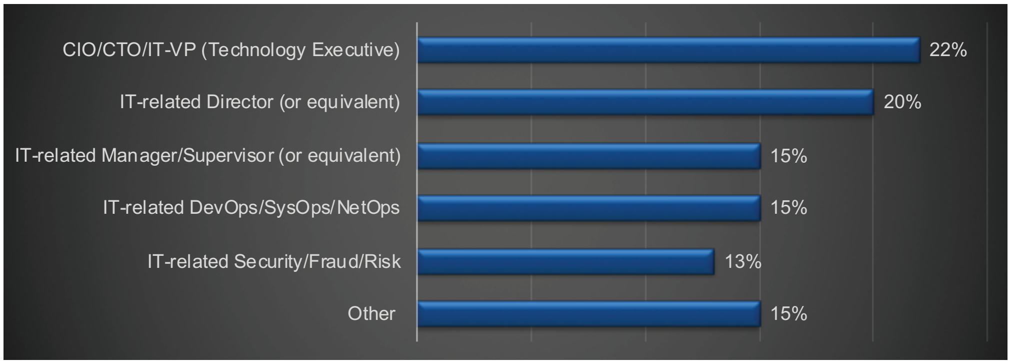

Figure 2: Respondents by Role

EMA sees that disconnect regularly in its research. This project was no exception. In most cases the disconnect is not an upper management issue so much as a frontline operations issue because the staff is not effectively communicating the true state of the environment. The motivation of that disconnect was not a part of this research, but the most common causes for it range from poor communication and reporting practices to actually hiding reality due to a toxic environment in which employees feel they have unattainable demands and thus do not communicate to preserve their jobs.

Organizational Sizes

The largest group of respondents came from the midmarkets. These are also referred to as small to medium enterprises (SMEs). The size ranges for each category listed in the figure are as follows:

1. SMB: less than 1,000
2. Midmarkets/SME: 1,000-4,999
3. Enterprise: 5,000+

The distribution of respondents was good at each level.

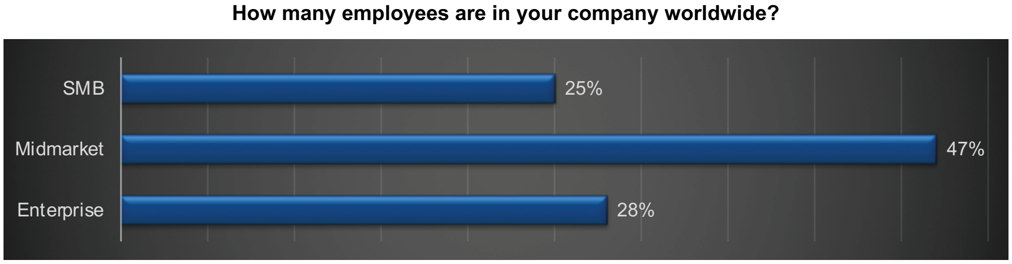

Figure 3: Respondents by Org Size

Respondent Industries

Service providers topped the list for the respondent industries in the report. This is useful since service providers, especially larger service providers, are power users of technology even more so than most enterprises. The scale and efficiencies they need are crucial to maintain operational profit margins while simultaneously meeting customer performance demands.

The "Other" category is a combination of industries that did not a have a sufficient response volume individually to make a valid sample group. The major industry contributors to "Other" included government, oil/gas/chemical, utilities, education, and transport.

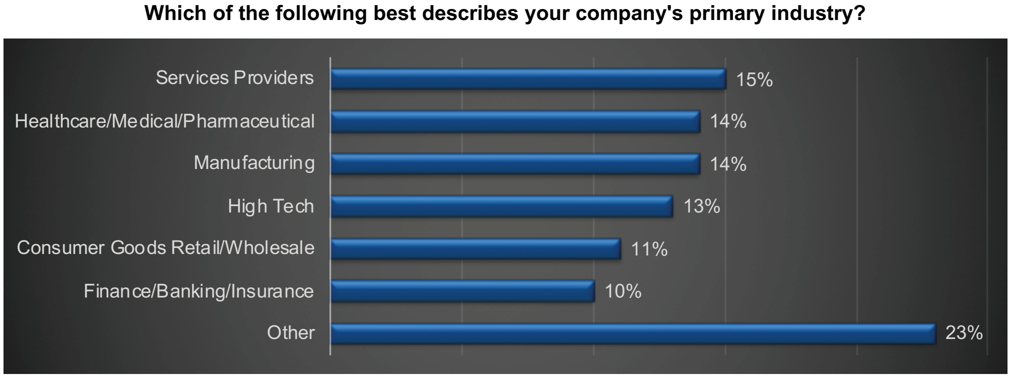

Figure 4: Respondent Industries

Current State of Cybersecurity in the Organization

Security bravado, or the security confidence façade, seems to also have reduced significantly. This is not to say that organizations still seem to have higher-than-warranted levels of confidence in their performance and risk, because they do. However, the gap is not as broad as EMA has seen in the past.

Risk in the Organization

Sixty-seven percent of respondents felt they were moderately comfortable to generally comfortable with some reservations. This indicates a knowledge of gaps in controls and/or visibility. The aggregate findings are listed below.

How comfortable are you with the current cybersecurity risk level in your organization?

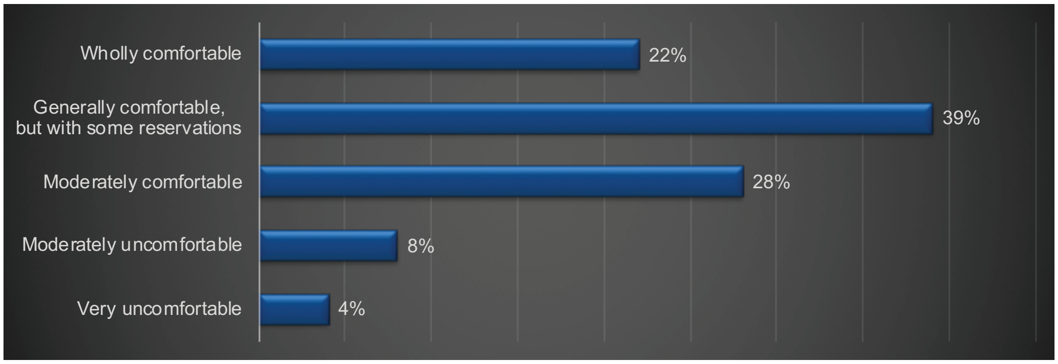

Figure 5: Comfortability with Current Organizational Cyber Risk

While this is a healthy range in aggregate, the dichotomy of upper management and frontline personnel is very significant in this area and creates a frightening contrast. Senior management was 1.7x more often "wholly confident" in their organization's cyber risk standing than middle management. Fewer middle management were "wholly comfortable" with the organization's cyber risk levels, but they were still much more aligned with frontline personnel having only a five-point gap between the two. This disparity clearly demonstrates a gulf between executive management and the frontlines, which can only be caused by poor communication.

Those using packet capture rated themselves as wholly comfortable with their organization's current cybersecurity risk level nearly 32% more often than those using flows, and almost 14% more often than those using endpoint or network, app, and systems logs.

Wholly comfortable by role: How comfortable are you with the current cybersecurity risk level in your organization?

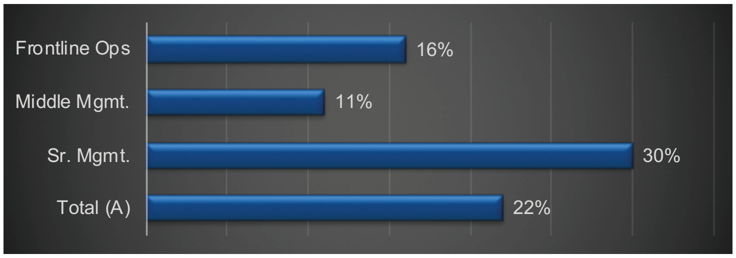

Figure 6: Respondents Comfortability with Cyber Risk, by Role

Program Efficacy and Maturity

An aggregate of 87% of respondents believe their controls are effectively protecting their critical assets. This seems high based not only on conversations, briefings, and interviews EMA conducted outside the context of the report, but also considering the low quantity of respondents that are confident in their security controls discussed later in this section.

Do you believe that your current cybersecurity controls are effectively protecting your critical assets?

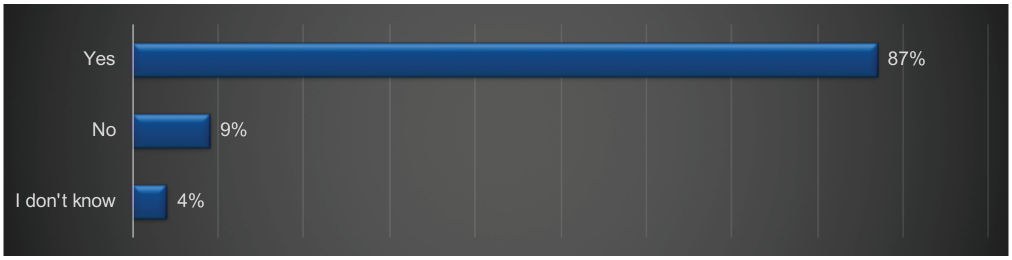

Figure 7: Are Current Security Controls Effectively Protecting Critical Assets?

This was the highest confidence rating across all of the telemetry collections and was more than six points higher than flows, endpoints, and network, app, and system logs.

As a group, respondents rated their organizations highly in terms of their efficacy in preventing, detecting and quantifying breaches. Each of the groups was pretty consistent with itself when comparing its answers in each of the three areas. However, the frontline personnel were significantly more conservative than management in rating themselves as having outstanding performance in either detecting or preventing breaches. Senior management was 65% more likely to rate their organization as "outstanding" in prevention and 85% more likely to rate themselves as "outstanding" in detection than frontline personnel. This is shown in the following graphs.

Ninety-one percent of those having deployed packet capture technology believe that their cybersecurity controls are protecting their critical assets effectively.

In your perception, how effective is your existing security program with regard to the following aspects of breaches?

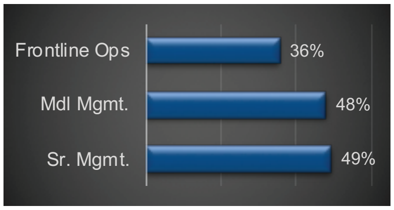

Figure 8a: Effectiveness at Quantifying Breaches

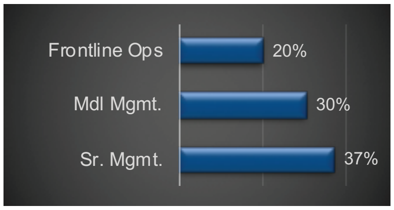

Figure 8b: Effectiveness at Detecting Breaches

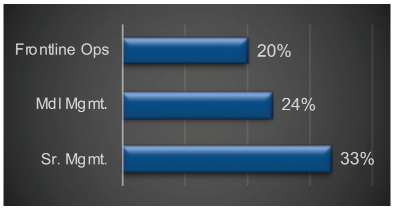

Figure 8c: Effectiveness at Preventing Breaches

While overall responses for program maturity were in the "very good" range, there were some variances that were interesting. In general the variances between each operational group were close, but only frontline personnel rated their programs as "poor."

When asked about their perception of the effectiveness of their security program in preventing, detecting, and quantifying the scope of a breach, those deploying packet capture rated themselves as outstanding in preventing and quantifying breach scope more often than those using any other telemetry method. They rated themselves as outstanding 33% more often than those using flows and nearly 20% more often than those using endpoint in preventing a breach.

How would you rate the maturity of your overall security program?

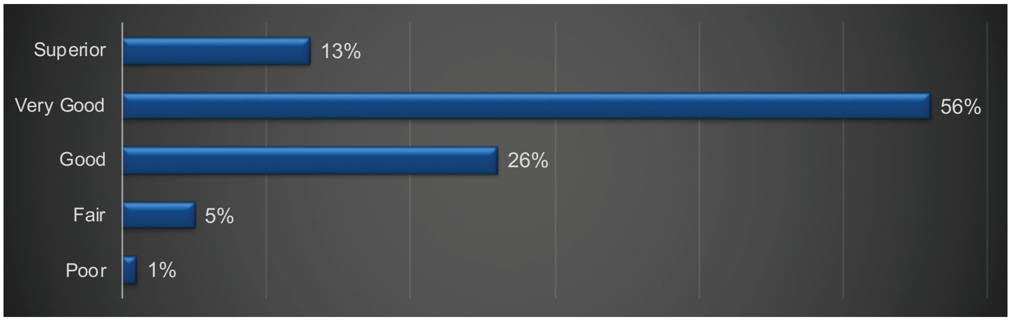

Figure 9: Security Program Maturity

When asked about individual components of their programs, the vast majority of respondents identified their maturity as "very strong to strong."

Thirty-six percent of organizations believe they have very strong performance in documented policies. This is higher amongst senior management, increasing to 44%. This is significantly higher than middle management and frontline personnel, with only 27% rating that area as very strong. Though the numbers vary, this is a common theme across the majority of the areas. In "security incident monitoring," 55% fewer of the individual contributors rated themselves as very strong."

EMA sees a high correlation between organizations using packet capture and their overall internal perception of IT and security maturity. There is also a high correlation between those organizations and better documented and stable workflows that support that internal assessment. Packet capture tools can be used for numerous types of security and operations investigations, thus making it easier to document the workflows for multiple types of processes.

Investigating the opposite end of the spectrum as to which controls the respondents have the least confidence in, the deltas in the employee groups were insignificant. EMA proposed the following areas of controls:

Table 1: Sample Security Controls Presented to Respondents

Breach investigation and incident response	Data loss prevention/ detection	Endpoint protections	Insider/internal threat detection
Perimeter protections	Unauthorized change detection	Vulnerability management	Confident in all areas listed

The top three are listed below. In addition to the top three least confident controls is a marker for how many respondents were confident in all of the listed areas. These seem to meet expectations in analysis for the other areas, such as program maturity and cyber risk.

Referencing the following controls, which would you say are the three with which you are least confident within your environment?

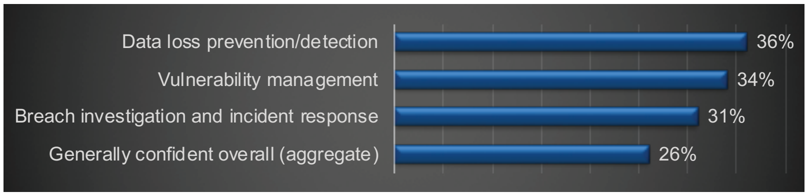

Figure 10: Top Three Least Effective Cybersecurity Controls

Respondents using packet capture had higher confidence in virtually every control identified. The only concern was vulnerability management. Their overall confidence level in deployed controls was 42% higher than the aggregate.

Security Services Adoption

Security Services

Services Consumed or Being Considered

Below, EMA identified 12 common managed services being consumed.

Table 2: The 12 Most Commonly Consumed Managed Services

24x7 security incident monitoring	Managed firewall	Threat hunting
Managed detection and response	Red team testing	Managed SOC
Off-hours security incident monitoring	Security-related change management	Risk assessment
Compliance assessment (not auditing)	Endpoint security monitoring	Security architecture

EMA also had an “other” category not listed in the table. That had less than one percent response, so EMA feels it was able to identify the most prominent areas.

The next chart shows the percentage of respondents consuming the top five services and the following chart identifies the top five services that are most considered for purchase by all respondents, based off the same services list, except for the small group that did not have services and were not looking to purchase any.

Which of the following functions are outsourced?

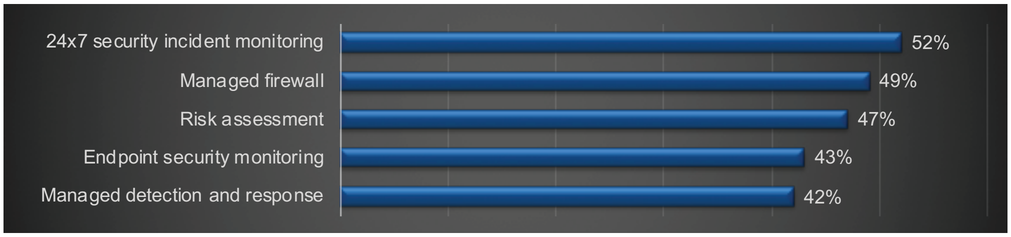

Figure 11: Top 5 Services Being Used

There are still quite a few organizations looking to augment their 24x7x365 security monitoring. Managed detection and response (MDR) is gaining significant attention as a mainline service. This is quite interesting since EMA sees MDR as a value-add service to normal 24x7x365 incident monitoring. After all, if an MSSP is monitoring for security events, they should see something attacking to or from the endpoints. The issue then is just how far their contract extends into the process beyond notification.

Which of the following security services are you considering engaging?

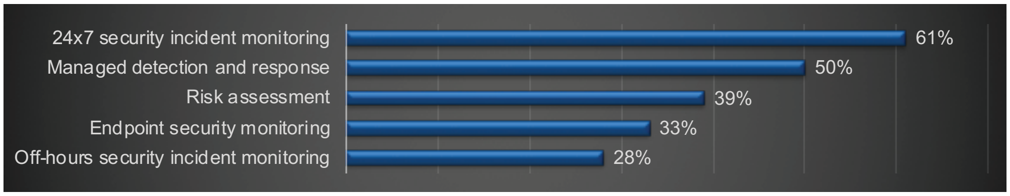

Figure 12: Top 5 Managed Services Under Consideration

Security Operations

Security Service Delivery

There seems to be a perspective that MSSPs deliver better alerting than internal counterparts. Though internal teams should know the environment better, the MSSPs often have far greater experience with the tools and spend a significant amount of time managing and tuning them to produce the best outcomes. This is part of doing business. Too little information being produced, poor alert classification, or too many alerts all mean missing a critical incident, thus lowering satisfaction and losing customers. The chart below identifies the perspective based on the aggregate responses, and is also broken out without the service providers' responses and by functional level of senior management, middle management, and frontline ops.

In general, how would you rate the quality of the notifications or alerting you receive from your MSSP compared to the notifications or alerting you receive from your internal security team?

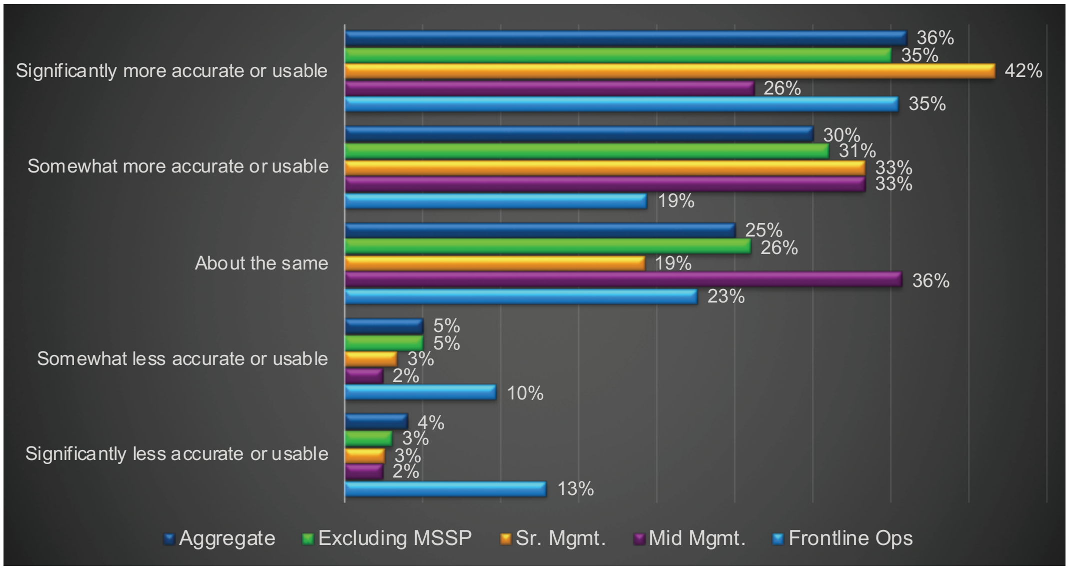

Figure 13: Perceived Quality of MSSP Alerts vs. Internal Security Alerts

While more senior management employees believe the service providers do a better job, middle management believes outputs are about the same. While the largest group of frontline ops personnel believe they deliver better results than the MSSPs, nearly one-quarter of them believe they are not doing as good a job as their MSSP counterparts, which is more than 2x more skepticism than any of the other groups.

Compromise Detection

For the subject of this research, a compromise is a situation where an indicator could be a breach in which some sort of losses were incurred, or when a compromise was detected but no data or other losses were incurred. EMA used the published Lockheed Martin Kill Chain model®[1] for the purposes of identifying how soon organizations are detecting and stopping incursions. EMA finds it receives more candid responses by allowing flexibility in the language. More respondents are willing to admit that "something" happened than identifying a breach that may have other legal and compliance implications.

The research asked respondents two different questions at different points in the research with regard to identifying and stopping attacks and incursions to aid in determining the accuracy of the responses. If the two are largely out of alignment, then it would be a reasonable conclusion that the respondents were giving more guesswork and not able to recall the previous series of answers. Fortunately, the responses (as seen in the next figure) were closely enough aligned for users to believe that they are accurate. Unfortunately, only about 28% to 31% of the incursions were identified and stopped at the earliest two stages. It appears that the majority of incursions and about 20% of the breaches were not identified or stopped until data was going out the door or totally after the event.

In general, what percentage of compromises or breaches in your organization are identified or stopped at each of the attack stages below?

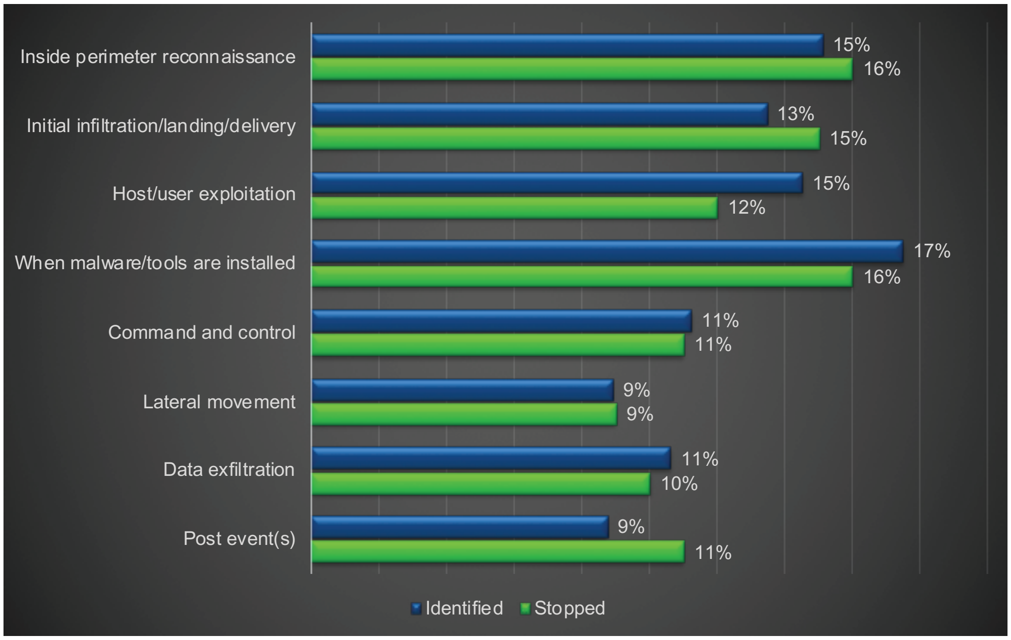

Figure 14: Attack Stages Compromises and Breaches are Identified or Stopped

[1] Lockheed Martin Cyber Kill Chain®

When evaluating their ability to detect attacks against the stages of the Kill Chain model, those using packet capture had the highest confidence that they were detecting viable threats at the reconnaissance stage. This is the first stage and the most effective at reducing dwell time when detected at this point. This is almost 28% higher than the average and over 36% higher than those using endpoint or network, app, and systems logs as telemetry.

When evaluating their capability to stop attacks operating at the various stages of the Lockheed Martin Kill Chain model, those using packet capture and flows had the highest confidence that they were stopping viable threats at the reconnaissance stage. This is the first stage and least costly when the attack is stopped at that point.

Additionally, when asked about their perception of the effectiveness of their security program in preventing, detecting, and quantifying the scope of a breach, those deploying packet capture rated themselves as outstanding in preventing and quantifying breach scope more often than those using any other telemetry method. They rated themselves as outstanding 33% more often than those using flows, and nearly 20% more often than those using endpoint in preventing a breach.

Participants were asked what types of data they believe are most useful for early breach detection. The responses were different than expected and added some insights into differing perspectives. For example, vulnerability data and dark web monitoring were ranked the top two sources, respectively. By its nature, vulnerability data is not an indicator of any sort of compromise. Those who chose that option interpreted it as a means of proactively identifying where attackers could have the most success. By having better telemetry about where their weak points are, security can focus resources proactively, thus avoiding the compromise altogether. The mindset is similar with dark web information. While it is obvious that the data itself is a post-breach artifact, proactively searching for those artifacts can offer insights into previously unidentified breaches where logs do not exist or were missed when the breach occurred.

What are the top three type(s) of source data that provide security operations with the best *early* detection of an attack or breach?

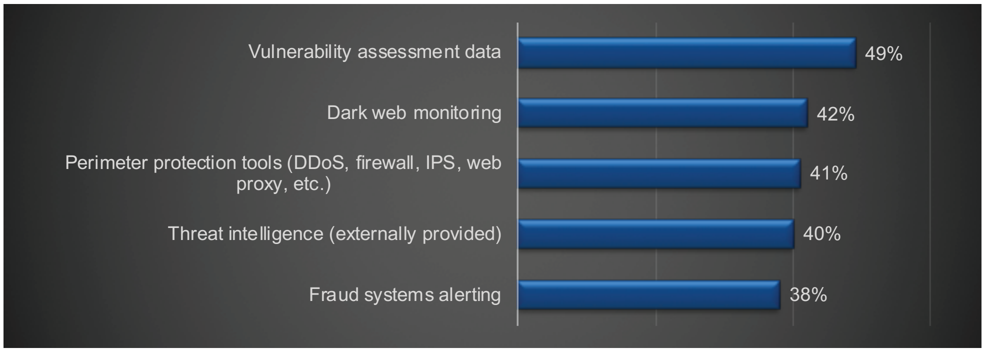

Figure 15: 5 Top Sources for Early Compromise Detection

In the same vein, participants were asked how effective they were at identifying gaps in their current controls. Twenty-eight percent felt they had everything under control. This is a reasonable number given the overall climate based on current overall volume of breaches and other indicators. The aspect that was uncharacteristic was healthcare coming in at the second from the top, with 35% fully effective. EMA will watch this to see if that trend continues. Normally finance/banking/insurance are in the top spot for these types of questions, with high-tech often in the second spot.

How effective do you feel your organization is at proactively identifying security controls gaps?

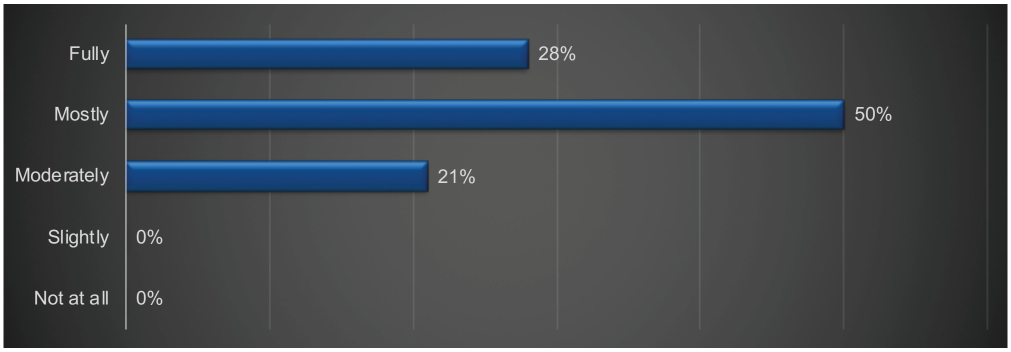

Figure 16: Efficacy in Proactively Identifying Controls Gaps

Even with a "mostly" effective ranking, the 50% in this category are still doing well. Though their risk of compromise is higher, continued diligence in this area should see them move higher in the next iteration of this line of questioning. Fifty-four percent of the finance/banking/insurance respondents placed themselves here. It is not clear if this is based on a more conservative group of respondents or if they are becoming more accurately self-aware of where they are in the security lifecycle process.

Those who used packet capture identified their ability to investigate security incidents effectively and efficiently with regard to the following areas as superior more often than the other telemetry collection methods (with the exception of investigation workflows and processes):

- Suitability of the security tools that you have available
- Quality of available data/evidence
- Ability for teams to share tools and data and work collaboratively
- Integration between different tools for efficient workflows
- Overall visibility into network activity

Impact of Management Interfaces on Efficiency

In earlier research conducted by EMA, organizations indicated they were using, on average, ten management interfaces for security and as many as 22 management interfaces in large enterprises. The primary delineator on the number of tools was not the size of the security team, but the overall organization size and, of course, the associated security budget. There are significant problems in operational efficiency, especially in the process and workflow of investigations, and data sharing with that many management tools.

Eighty-five percent of respondents felt it was important to very important to have a single management console for security. At the current time, this is understandably seen as an unachievable state. As APIs, product integrations, automations, and other cooperative efforts continue, it is conceivable to whittle this number down into the single digits.

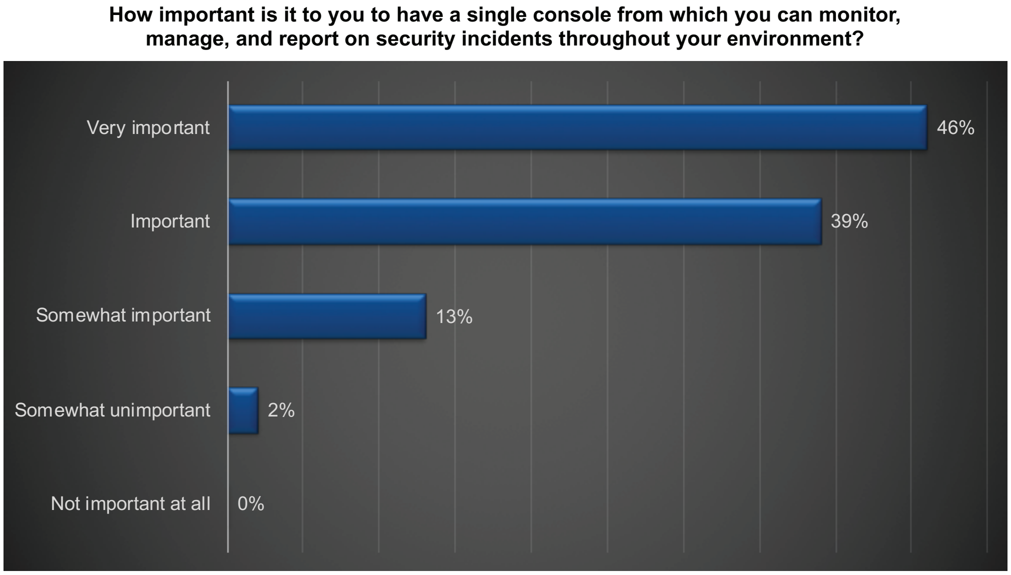

Figure 17: Importance of Having a Single Management Console for Security

Advanced packet capture delivers a single console standardizes numerous troubleshooting, hunting and investigations work flows improving time to detect and respond.

Automation and integrations are the key factors in reducing tool interfaces. Details on those are discussed later in the report.

The supposition going into the research was that SIEM or ticketing systems would be the primary interface for incident management, but the findings were quite different.

1. Very large enterprises (organizations with 20,000 or more people) primarily use a custom management interface (25%).
2. Enterprises (organizations between 5,000 and 10,000 people) identified the use of the native management console or UI from one or more security tools other than a SIEM or log management (24%).
3. Midsized (organizations between 1,000 and 4,999 people) identified using homemade or commercial tools with automation and orchestration (SOAR-like) functionality (23%). This was highly unexpected and warrants more investigation in future research. While expanding rapidly, commercial SOAR tools do not have that sort of market penetration yet, so this would have to be mostly made in-house.
4. SMB (organizations with less than 500 people) identified two primary interfaces. The first is a centralized log management tool that is not a SIEM (19%). The second is an analytics tool interface. This was very surprising. SMBs have traditionally shied away from SIEM due to the cost and have now leap-frogged it with analytics. Depending on the package, it can still be less expensive than traditional SIEM. However, all of the leading SIEM vendors added significant analytics capabilities to their SIEM engines, so the delta is not so much a functionality issue as it is still a cost issue.

Tools and Data Integrations

Data silos, especially in security, are not at all uncommon. In recent years, great strides have been made to begin breaking down the silos within security and between operational groups. Many of these efforts can be labeled as part of SecOps, DevSecOps, and NetOps movements.

Within security, respondents identified the tools they are most often using to try to overcome their security data silos. The graph depicts both the aggregate responses and the top used tool by industry. The most surprising thing was that traditional SIEM only came out as the primary tool in healthcare/medical/pharma for any of the industries. Three of the six primary industries, excluding "other," are using some form of analytics tools and three are using some form of centralized log management tool.

Which technologies or methods is your organization using to correlate across the security data silos?

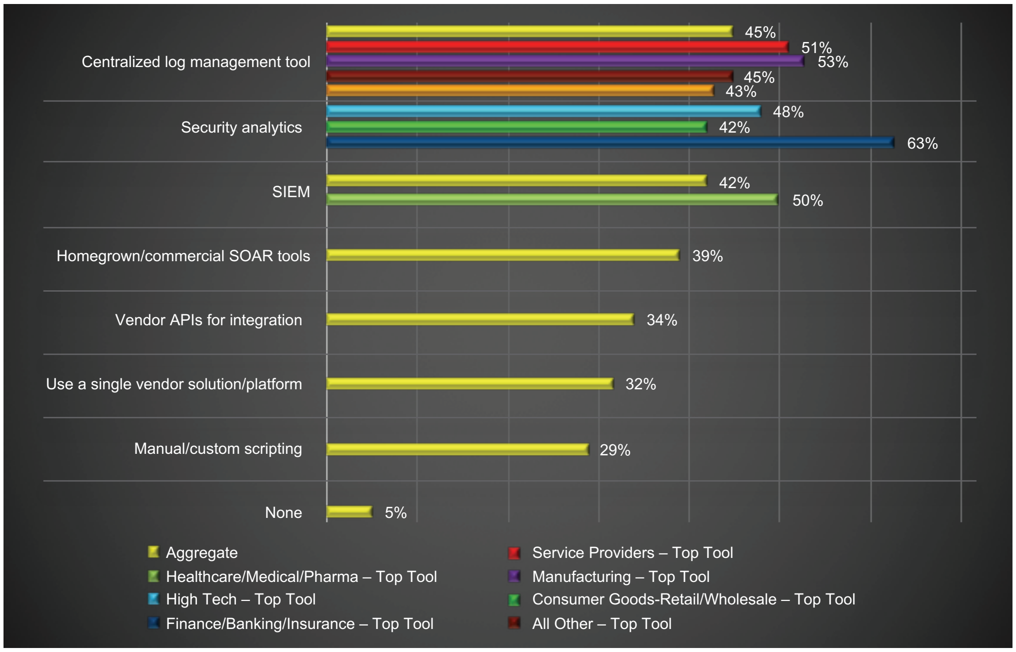

Figure 18: Tools Used to Collect Data Across Silos

As the traditional SIEM vendors continue to pivot into security analytics, distinguishing the two will be more difficult and may require the use of vendor names to best classify the type of tools being used.

Data integration for improved detection and response is a security imperative today. The majority of participants identified that breaking their data silos and integrating their data was critical for their success and was a primary requirement for their ongoing tools selection. The following chart shows the percentage of respondents that identified each of the listed criteria as "very important to indispensable."

Please rate each of the following methods of integration as to its importance to you when assessing a security solution for insertion into your security architecture.

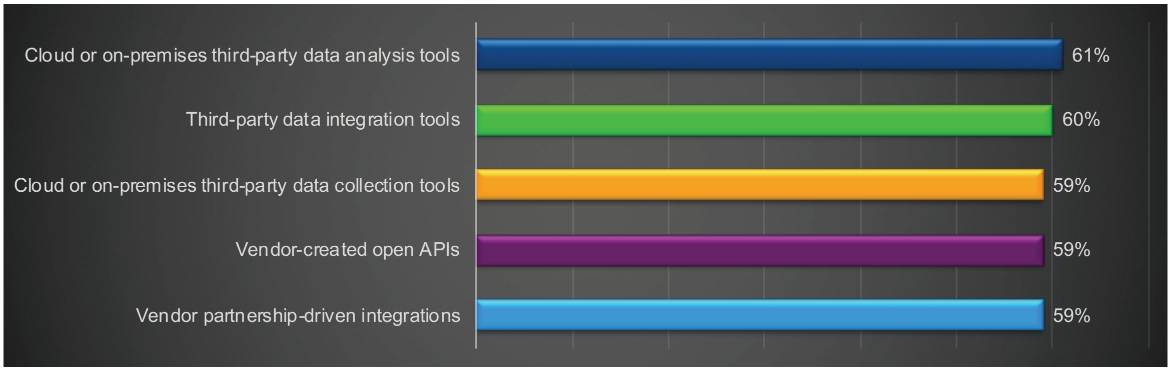

Figure 19: Data Integration Methods Rated as Very Important to Indispensable as Tool Selection Criteria

The top three drivers or motivators for integrating data are shown in the next figure. Those that do not have data integrations completed or on the roadmap suffer from the first issue—high levels of false positive alerts. Their detection systems receive limited telemetry and are therefore inhibited in making quality decisions.

Individual solutions vary considerably in the type, quantity, and quality of the data they can collect. While any single solution may have a detailed picture of what is happening within its defined monitoring context, no one detection tool can see everything and therefore requires additional information to create the complete picture of an attack/breach. Included in the next chart are the top three drivers for combining security data.

Please identify your top three drivers for using combined security data.

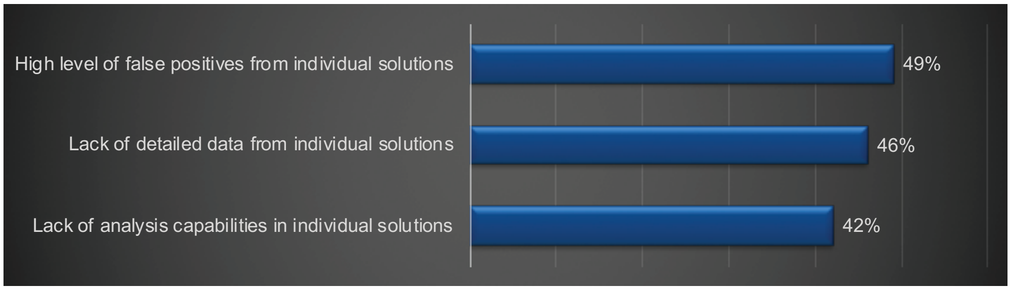

Figure 20: Top 3 Drivers for Creating Combined Security Data

Additionally, EMA asked about the primary motivation for combining data. Preventing breaches was the top answer. At first, that may seem a little counterintuitive, but it really isn't. Having a full picture of activities in the environment can't stop an attack and may not stop a compromise, but it can stop a breach. A compromise means something made it past a control, while a breach means that something was taken or destroyed. In compliance terms, users don't have to report a compromise, but they are required to report a breach if compliance-related data was accessed, taken, or destroyed. With the proper centralized telemetry and analytics, early indictors of a compromise can be detected, thus enabling a response pre-breach.

Please choose your top three most important reasons for integrating security data.

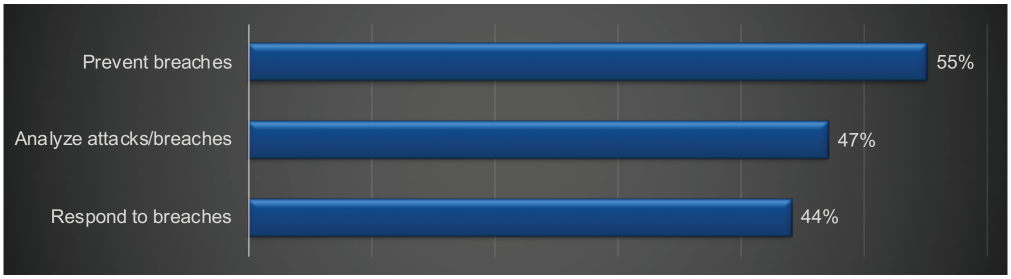

Figure 21: Top 3 Drivers for Security Data Integration

The factors inhibiting data integrations have not changed much over the last few years. However, the percentage of each has adjusted. More vendors are supplying their own APIs, so APIs have decreased as an inhibiting factor. On that same vein, the quality of those APIs varies considerably by vendor. Some are very robust, well maintained, and well documented, while others are not. In speaking with vendors about this, the majority see their APIs as either a differentiator or even a business advantage. Those who do apply considerable resources to maintain that quality, pulling ahead of those that have not yet decided to make APIs a priority. Within the next couple of years, a quality API will be playing stakes in most areas of security.

Please identify up to three of your top challenges limiting your ability to combine your security data.

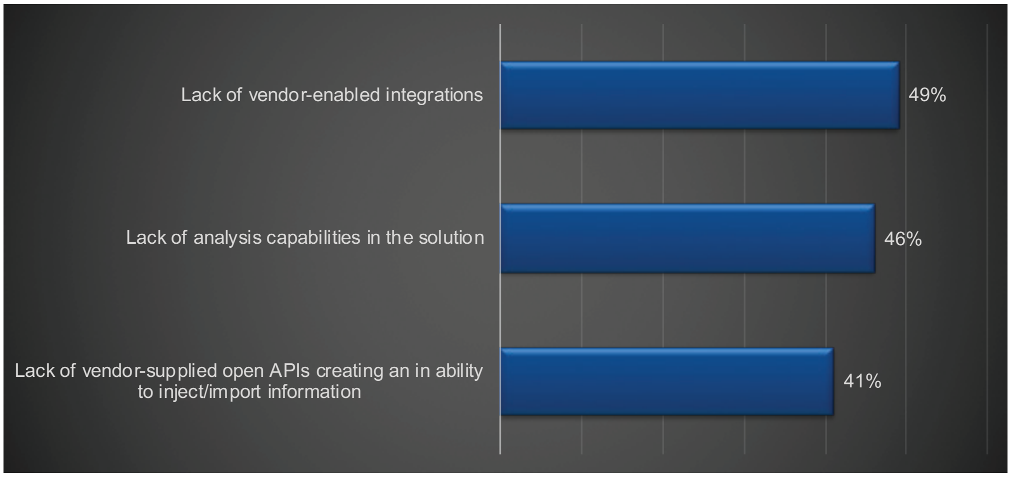

Figure 22: Top 3 Challenges Inhibiting Security Data Integration

The need for analytics in security is critical. Participants identified that if they do not have analytics capabilities, they are not motivated to break down the data silos. The term "analytics" has a very broad definition. The level of analysis applied to any dataset can vary considerably. Having the attitude of not trying to integrate data because analytics is seen as all-or-nothing is terribly shortsighted.

For those not making data integration a priority, get those plans in the roadmap as soon as possible because circumstances may change faster than anticipated. Being prepared to use the data sooner rather than later will never be a bad choice.

NetOps

While 89% of organizations believe that having a baseline of activity for their network is important, only 59% have actually gotten around to doing it. This is not a trivial task, but is well worth it. To do that, organizations must have the ability to combine analytics with packet capture or at least NetFlows. The latter requires less specialized equipment and less storage, and therefore less cost, for a given period. However, it also provides far less fidelity.

Do you have a historical baseline of network data for performing behavior and anomaly detection?

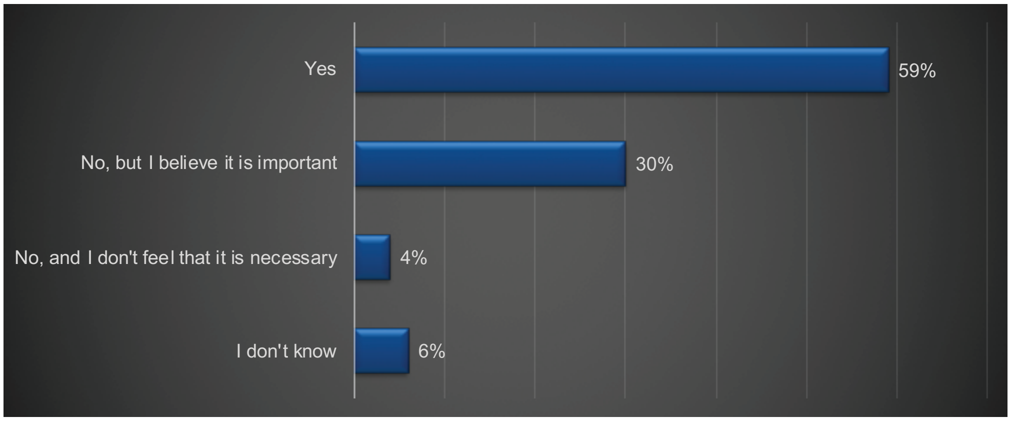

Figure 23: Organization Keeping a Baseline of Historical Network Activity Maintained

Each type of data collected provides an additional and valuable view of the context as to what is happening. Each dataset or type has its own intrinsic value. However, respondents believe that network data is more valuable for early breach detection than endpoint. Again, this is not to say that endpoint data is not important or that it does not provide unique data for incident resolution. There is no doubt that it does. However, if properly implemented, network data provides insights into what is happening on the network before a host is compromised. This "proper implementation" requires having some kind of baseline for network activity and some form of UEBA analytics to understand when entities are behaving out of character.

Though it depends on the type of attack, in general or for the majority of cases, which do you do feel is better for the earliest detection of a breach?

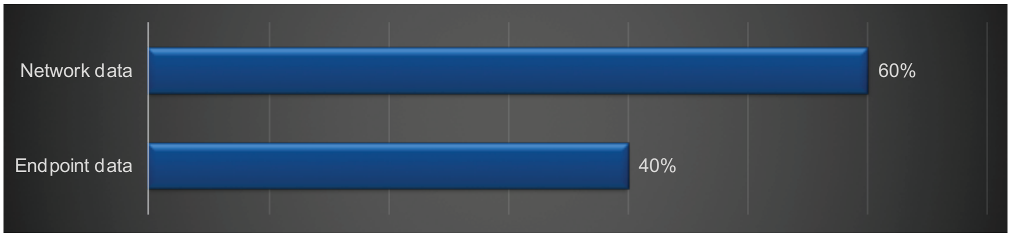

Figure 24: Greatest Value Data for Early Breach Detection

Just over 74% of respondents indicated they are collecting some kind of packet data for incident investigations. This is a significant increase over past EMA studies.

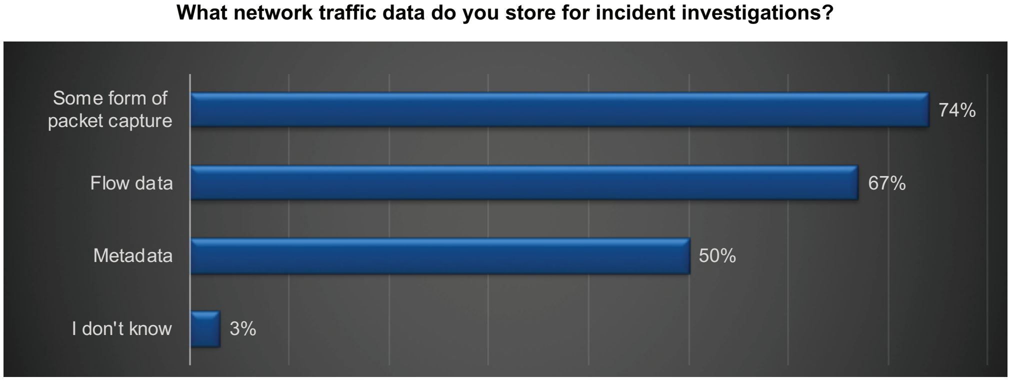

Figure 25: Network Data Stored for Incident Investigations

The greatest inhibitor to capturing and storing full packet data has been equipment and storage costs. In the past year, several packet capture vendors released high-speed, high-capacity solutions that seriously changed that cost paradigm. EMA expects to see a higher percentage of organizations performing packet capture over the next year.

The newest entrant into the game is metadata. Metadata is data about the data captured. It is not the actual packet data, but insights into the data. An example of data from packet collection would be the IP address. An example of metadata about the IP address would be its country of origin. There are hundreds of different pieces of metadata that can be generated from a full packet capture. When overlaid with the source data and analyzed, metadata becomes high-value telemetry. In the chart, readers can see how valuable the personnel collecting it believe it is for incident investigation.

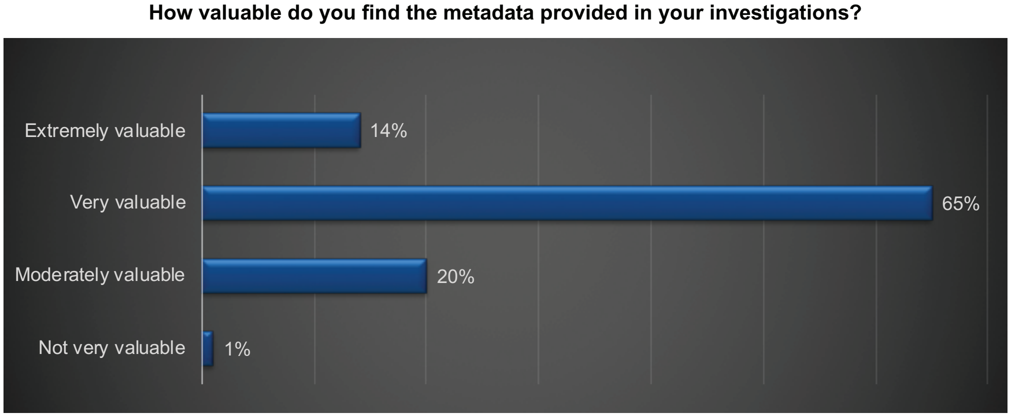

Figure 26: Value of Network Metadata for Investigations

Conclusion

The vast work of maintaining cybersecurity programs at the level of risk that is acceptable to the organization is not trivial. It is, in fact, often daunting. This report identifies numerous efforts being conducted to improve cybersecurity, but is not all-encompassing. Each of the areas discussed shows similarities and differences in perspective and approaches between operations and management across industries.

One significant commonality in the report was the confidence of organizations using packet capture in their toolsets. This was not an expected outcome, but made for an interesting investigation. It is clear that those using packet capture as part of their normal toolset, rather than not at all or on-demand, were more confident in the telemetry they received about their environments. They had shorter breach detection and response times and they had more confidence in their workflows and processes. There were numerous other aspects of their security program that they felt operated at a superior level, more so than others not employing packet capture. Those include better records of their assets and especially critical assets, the level of in-house skills maintained, quality of available data/evidence, overall visibility into network activity, and the ability for teams to share tools and data and to work collaboratively.

When taken as a collective, this creates a very strong story for the use of packet capture as one of the staples in the security program. While network packets do not contain all of the information needed to complete an investigation, the fact that 99% of daily activities cross a network makes it easy to understand why companies feel they have a heightened sense of awareness. They are able to detect issues faster than businesses replying on perimeter, systems, application, and authentication logs.

Though all points are applicable to most organizations, it is important that organizations keep the information provided in the proper context as they consider how they compare to the responses. Some risks that are acceptable to one organization, even in the same industry, may not be acceptable to another. The same is true of the chosen solutions. Each environment has differing requirements and budgetary limitations that drive variations in the chosen solutions. Ultimately, maintaining diligence and a programmatic approach will always serve the organization well.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com
3845.073119