# SECURITY MEGATRENDS

## Report Summary

ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) Research
Written by David Monahan
January 2019

**SPONSORED BY:**

DOMAINTOOLS®

EMA™
IT AND DATA MANAGEMENT
RESEARCH | INDUSTRY ANALYSIS | CONSULTING

# TABLE OF CONTENTS

## Executive Summary

Threats abound, but people are out there trying to deal with them. Organizations continue to fall behind, finding it increasingly difficult to identify and respond to threats in a timely manner. This report delves into several areas of concern today including cloud security issues, SecOps frustrations and tools, the Internet of Things, data sharing and leakage, DDoS, endpoint security, and artificial intelligence. The report identifies challenges and perceptions that enterprises, midmarket companies, and SMBs face across seven industry verticals including manufacturing, financial, and healthcare. The goal is to help readers to understand the common issues and where they are doing a better or worse job than others. Ultimately, the report will help readers understand how to handle threats better, no matter where they stand now.

## Demographics

This research report was distributed across North America and is thus focused. Further geographic division was not tracked. The respondents were primarily targeted from IT/cyber security, with additional extraction from executive management. In this research, line of business personnel were not queried because they do not have enough insight into the desired breadth or depth of security.

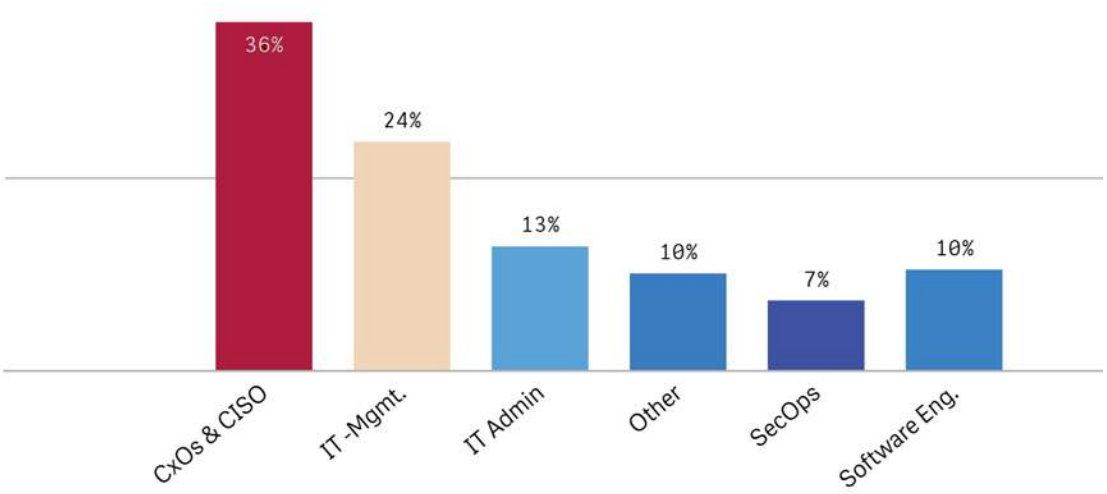

*Figure 1 Respondent role*

Organizations of all sizes and industry verticals have some security issues and challenges in common, but each also has its own specific challenges. The research looked across SMBs, midmarkets, and enterprises as well as multiple industry verticals to understand the commonalities and divergence in the trends.

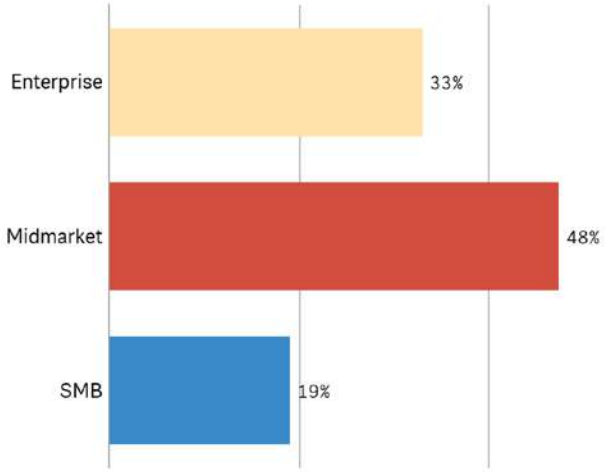

*Figure 2 Organization breakout by size*

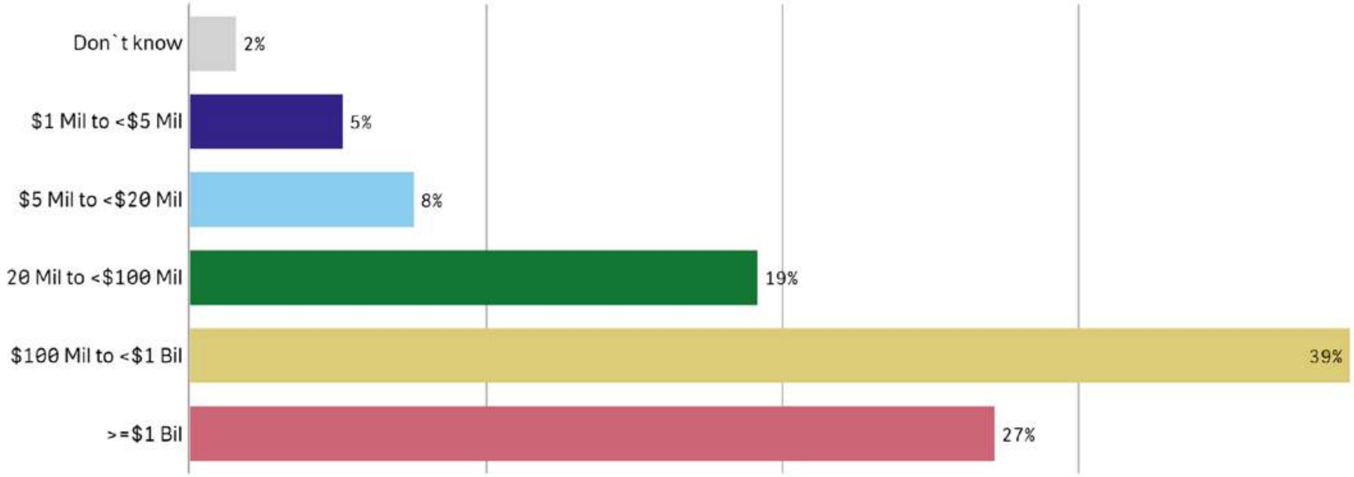

*Figure 3 Organizational breakout by revenue*

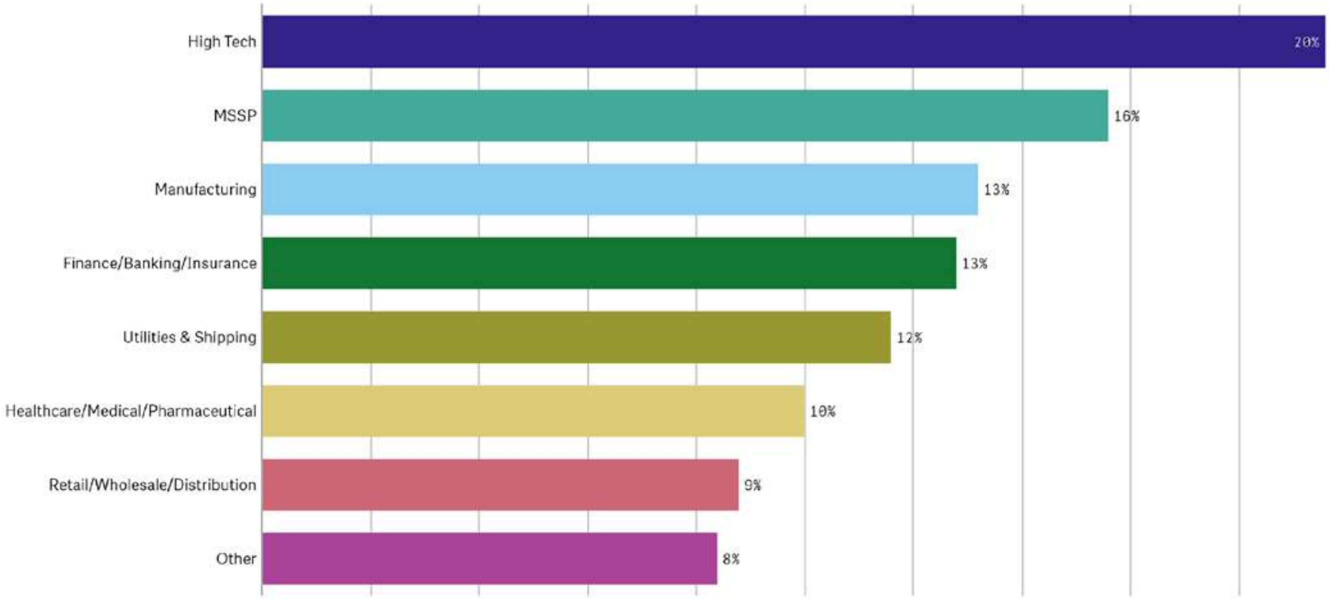

*Figure 4 Organizational breakout by industry*

## IT and Security Budgets

IT and security budgets are looking healthy. EMA has seen consistent growth in both over the last five years. IT budgets have been growing an average of 9 to 13 percent, while security has been higher in the 15 to 20 percent range. In this sample, only one percent of organizations reported a budget decrease for IT and security, which is common at this time. The most common annual IT budget increase was 10 to 24 percent and the average was just shy of 23 percent. The state of security over the last five years, with the changed perspective of assuming that the company has already been breached, pushed those budgets up annually far more significantly than in the previous fifteen years.

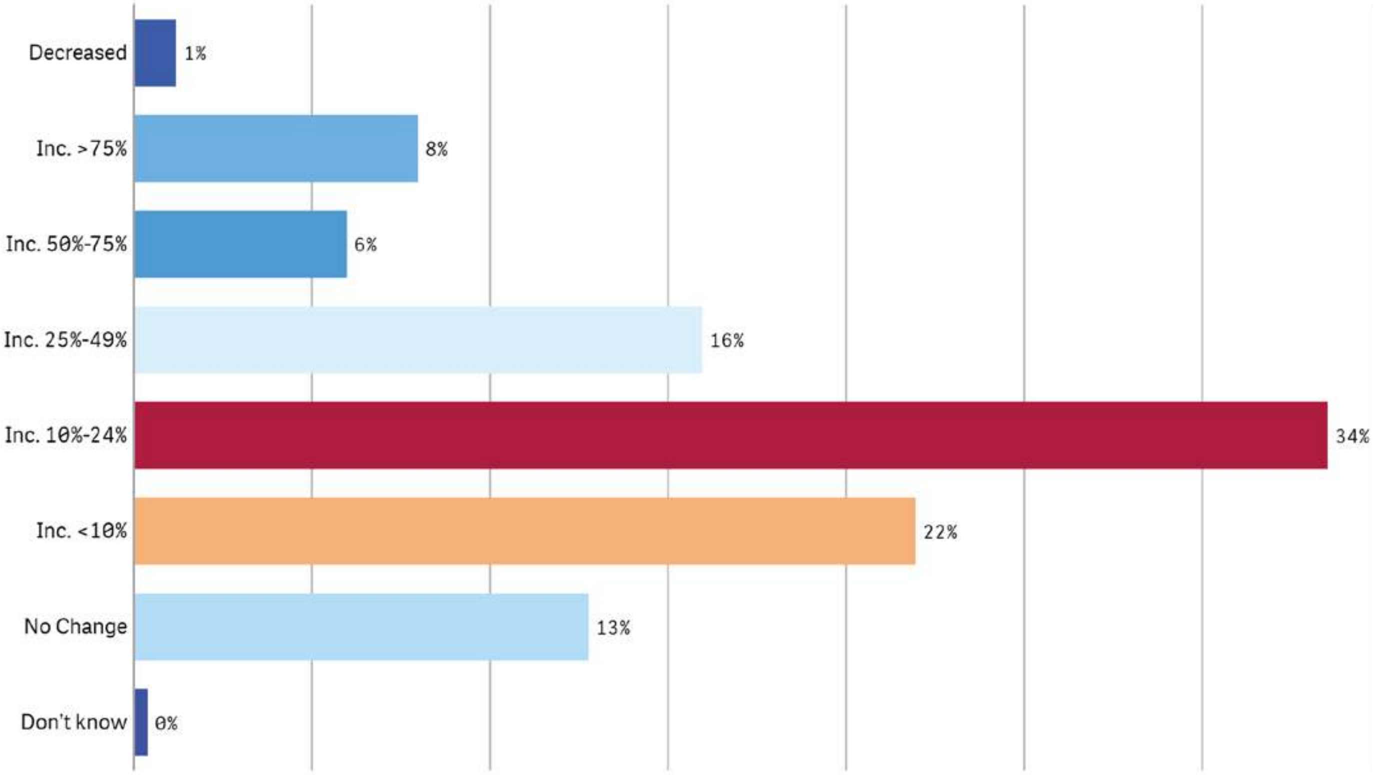

*Figure 5 IT budget increases from 2017-2018*

## Initiatives Affecting SecOps

Security operations teams have many challenges to meet the needs of the business. Issues that were once at odds, such as usability and security, now have to be managed and implemented cooperatively. Businesses are no longer willing to submit to security, and IT operations that are not agile are unable to meet the business delivery requirements. On the other hand, security must be maintained as tightly as possible to keep hackers out and malicious insiders at bay.

EMA asked about the status of major security initiatives within the business to understand more about where companies stand collectively in North America.

Only ten percent of the respondents indicated that none of these were a priority, leaving the remaining 87 percent working furiously to achieve their goals. This demonstrates the tremendous pressure on security organizations to not only perform, but also improve. This is a huge number of initiatives, with each having significant deliverables for the business. The good news is that most organizations are in the process of improving/expanding them, rather than starting them off. The bad news is that in general, one-third of them are in a position where they are just getting started on many of these, putting them behind in the battle for security.

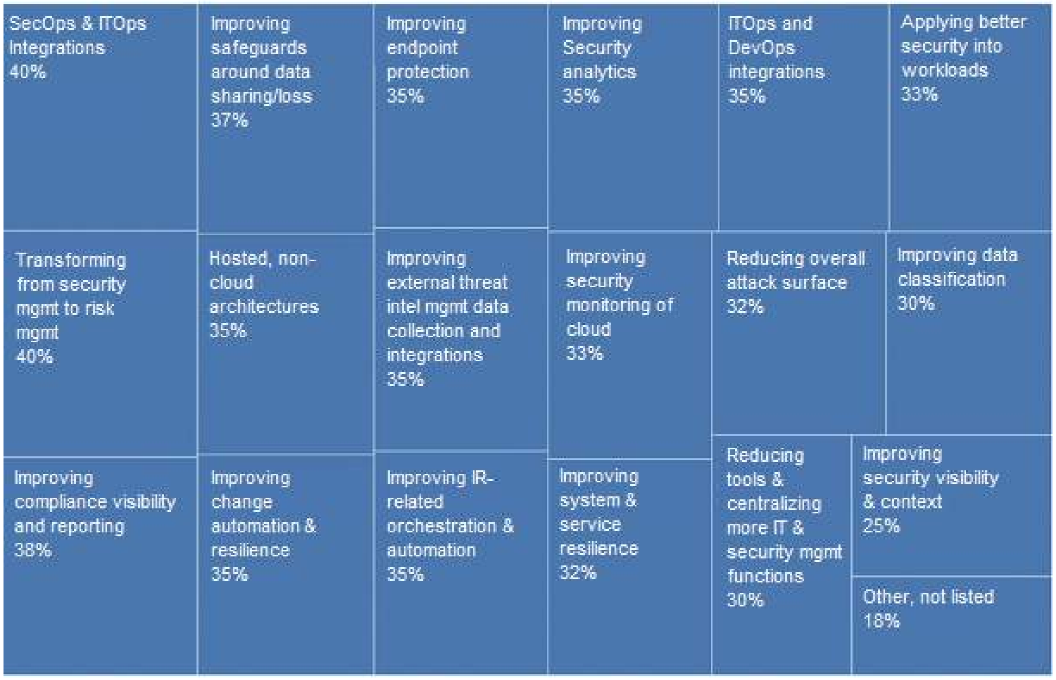

*Figure 7 Starting security initiatives*

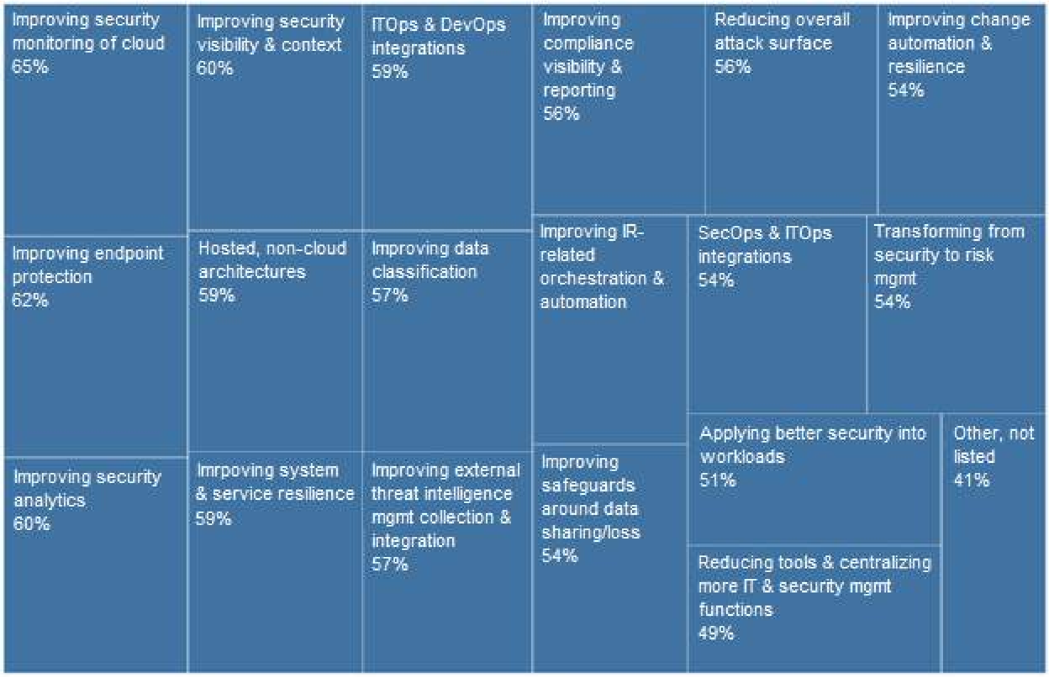

*Figure 8 Expanding security initiatives*

## SecOps Roles and Responsibilities

The first approach to combat the threats is to programmatically decide how to deal with security from both a macro and a micro perspective. The macro perspective is whether or not to keep SecOps in-house or to outsource it. The respondents opted to deal with the challenge.

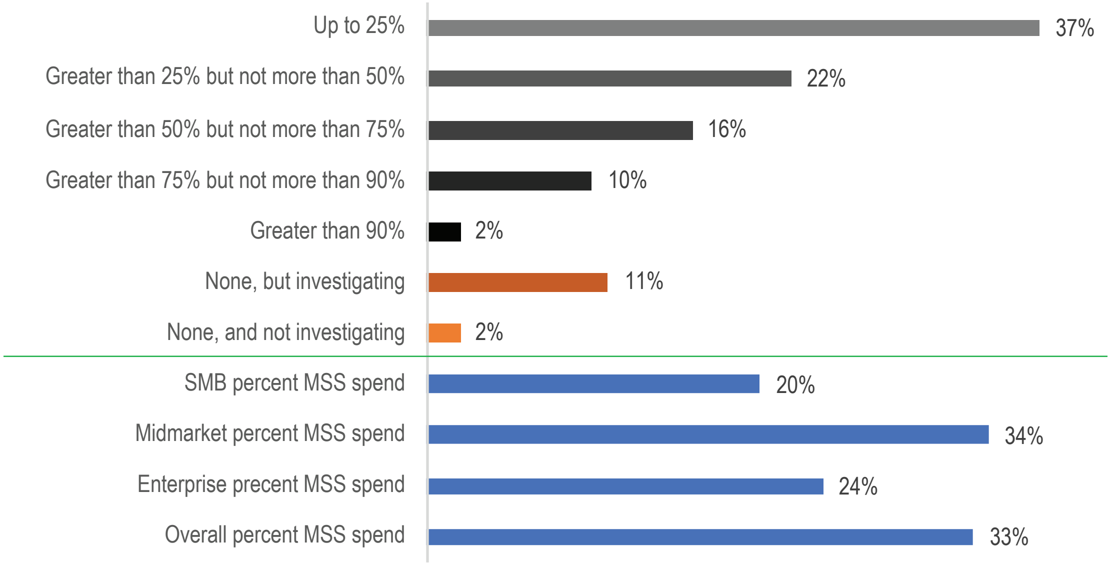

*Figure 24 Proportion of security budgets applied to outsourcing*

No one can deny that the roles and responsibilities of SecOps are getting tougher. New attack vectors are being discovered almost daily, and exploits of vulnerabilities bring breaches at nearly the same rate. Organizations have to be flexible and even creative in the way they manage security. SecOps can have a pretty tough time of it. However, respondents gave significant kudos to their internal teams.

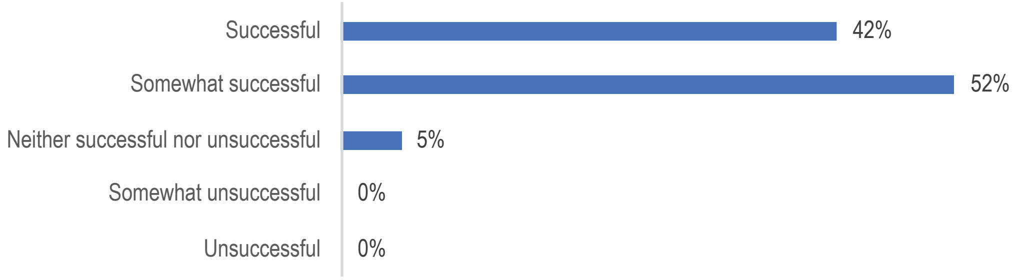

*Figure 25 Perceived success of internal SecOps teams*

With nearly half of respondents claiming success for their internal team and 95 percent feeling at least positive about their internal SecOps team accomplishments, the teams should feel pretty good. Based on their success, the organizations that decided to keep at least some portion of their security in-house are seeing returns on that investment.

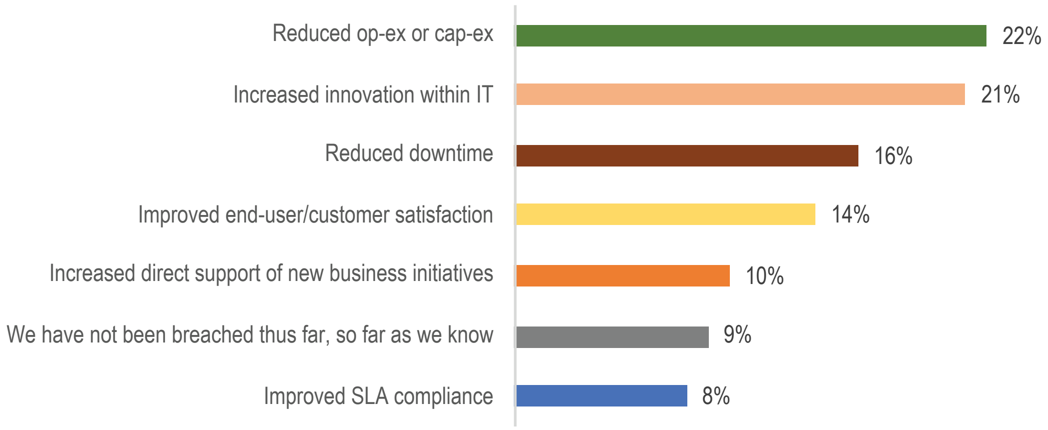

*Figure 26 Benefits achieved by using an internal SecOps team*

The largest surprise was the reduced op-ex or cap-ex. Security tends to be a significant cost center. Both the people and the tools are expensive. However, when executed well through automation integrations to reduce manual work, as well as the time to complete activities and improve outcomes, security begins to experience cost avoidance and cost reduction. Automation and integrations can reduce the number of tools needed, thus cap-ex outlay. It can also reduce the pressure to hire new people by getting more done with less, creating cost avoidance.

In evaluating their own performances and where they want to focus improvement over the next year, 53 percent of organizations said that the overall performance of security services significantly increased in importance, followed by 48 percent indicating expanding security response capabilities with 46 percent wanting to significantly improve proactive problem identification and security incident response automation. The least-focused category was creating performance SLAs, with only 35 percent having a significant increase in importance. It is not clear whether this is because those organizations already have sufficient performance metrics in place or because they are too distracted by fighting security “fires,” which is a common trap. Here are additional priority variances from the industries covered in the report.

| High Tech | MSSP | Manufacturing | Finance/ Banking/ Insurance | Utilities | Healthcare/ Medical/ Pharma | Retail/ Wholesale/ Distribution |
|---|---|---|---|---|---|---|
| Improving overall service delivery | Improving overall service delivery | Security IR automation | Improving overall service delivery | Expanding security response capabilities | Security IR automation | Improving overall service delivery |
| Expanding security response capabilities | Security IR automation | Security change automation | Expanding security response capabilities | Better proactive problem identification | Better proactive problem identification | Security IR automation |
| Security IR automation | Security change automation | Better proactive problem identification | Expanding security monitoring capabilities | Expanding security monitoring capabilities | Improving overall service delivery | Expanding security response capabilities |

*Table 1 Most significant improvement focus areas by industry*

## SecOps Frustrations: Tools

One of the reasons there is a huge value opportunity for MSSPs is because of the difficulty and frustration security has with managing all of their tools. Enterprises can have a huge number of management consoles to interact with to do their jobs.

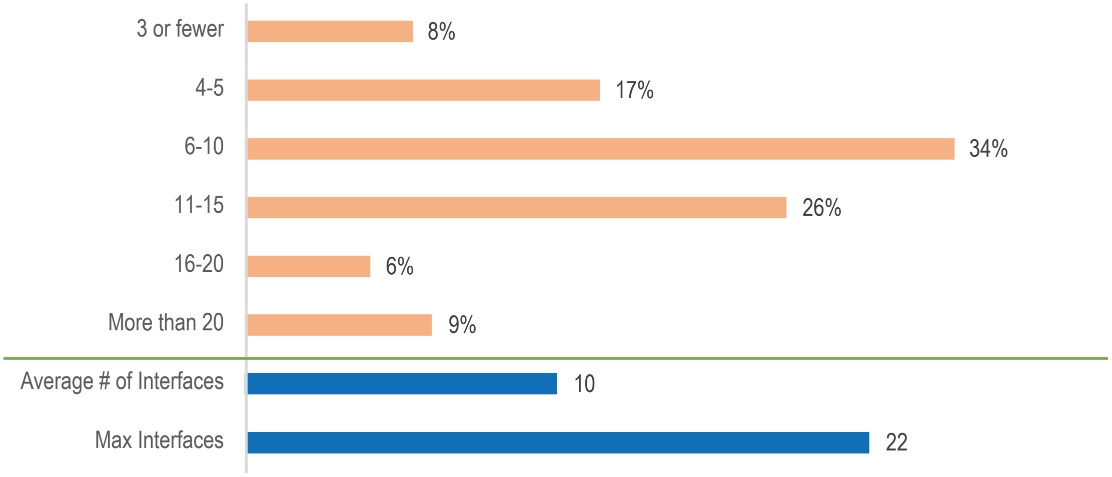

*Figure 27 Consoles security teams use to manage programs*

## SecOps Frustrations: Alert Fatigue

Another area of frustration for security professionals is referred to as alert fatigue. Alert fatigue stems from the large volume of alerts presented to analysts that they are required to validate, identifying whether they are really high severity or at the other extreme—if they are false positives that are really nothing to worry about. In many environments there is highly insufficient context for the systems to properly judge the criticality, so over 95 percent of the tickets that come in are classified as the highest priority.

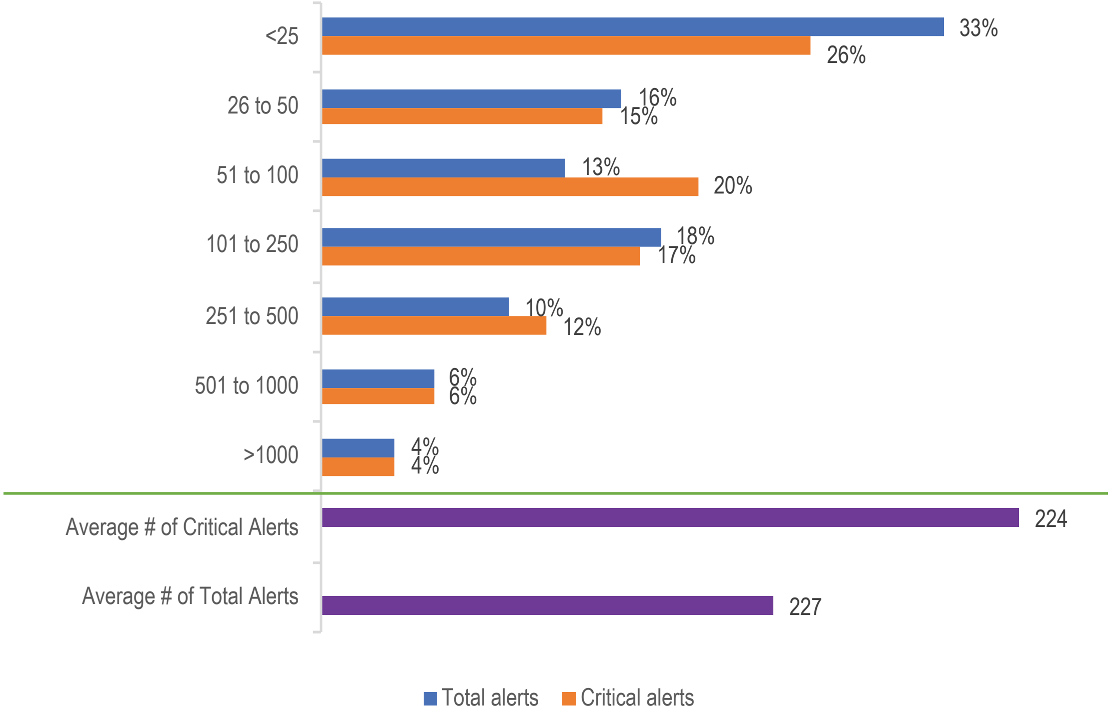

*Figure 28 Comparison of severe tickets to overall tickets*

## SecOps Frustrations: Handoffs

The final area of frustration covered in this report is inter-team handoffs. Seventy-six percent of respondents identified some level of impediment when trying to resolve an incident requiring inter-team handoffs or support.

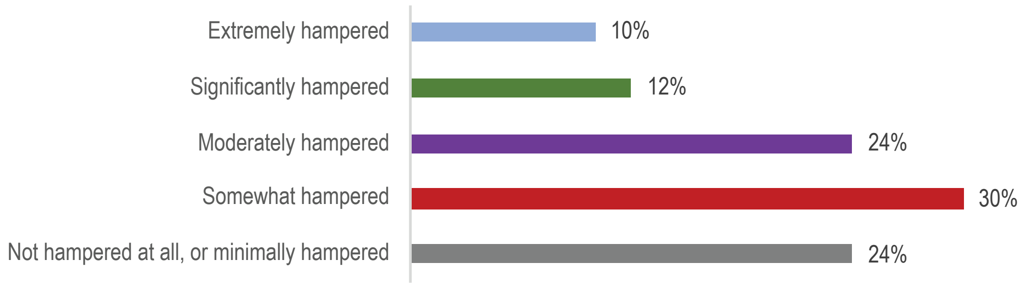

*Figure 29 Level of impediment experienced in inter-team handoff for incident investigation*

When trying to investigate and resolve an incident, security analysts are often required to engage members of other teams for one or more phases of the incident prior to closing. These frustrations are encountered at some level daily, which leads to job dissatisfaction. After enough frustration, personnel leave. MSSPs alleviate or at least significantly reduce many of these frustrations by handling the incident lifecycle. The degree of reduction is highly dependent upon how much of the lifecycle the MSSP controls.

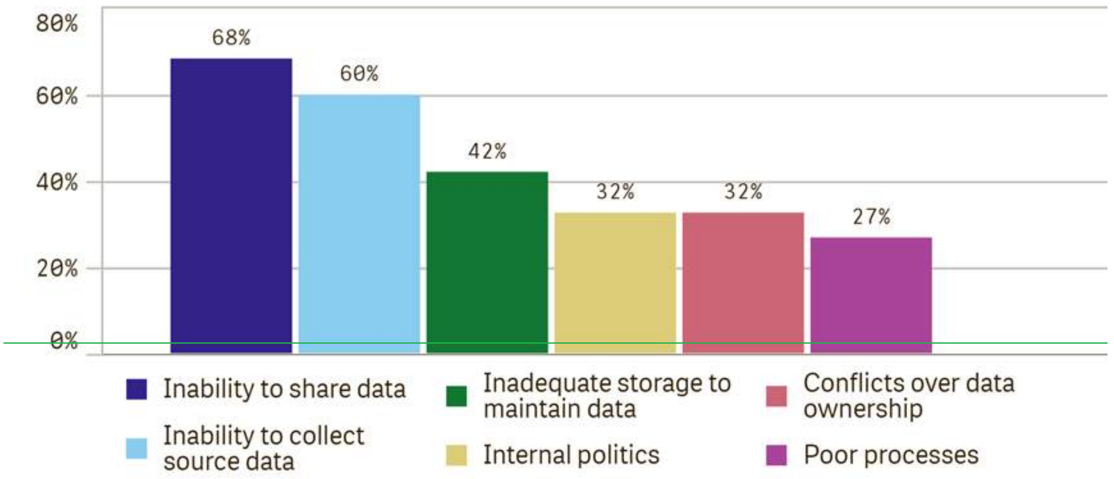

*Figure 30 Impediments experienced during incident investigation*

Seventy-four percent of enterprises experience the inability to share data, which is the highest impediment for them. Midmarkets identified both an inability to collect and inability to share data equally at 66 percent. Sixty-five percent of SMBs identified data collection as their largest impediment.

## Engaging an MSSP

Eighty-seven percent of organizations opted to engaging some level of managed security service (MSS), with as many as 98 percent either having one already or considering engagement.

Enterprises tend to have less of an overall percentage of their security budget applied to MSS, while midmarkets tend to spend the greatest proportion. SMBs tend to underserve themselves. Though there are several possible answers, there is no data to support a clear conclusion as to why.

Once that decision is made, the micro perspective depends on the macro choice. If the decision is to keep it in-house, then companies must build the program. They need to determine the functions that can be supported both financially and operationally. If the decision is to outsource, then the micro decision is not only to whom, but how much of SecOps goes out.

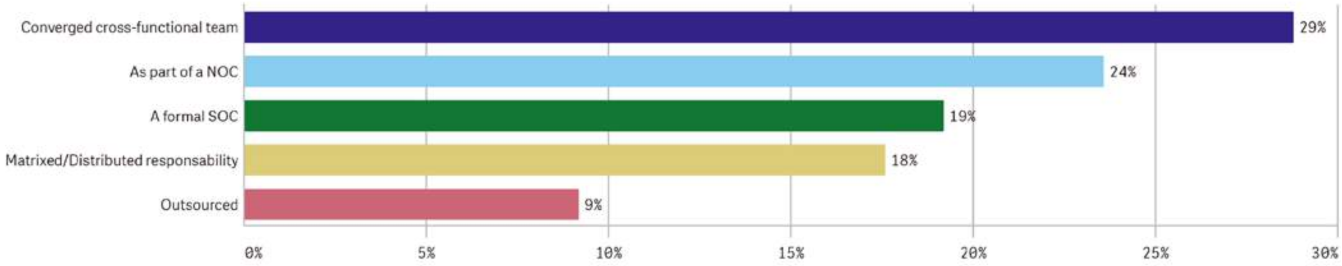

*Figure 31 Structure of SecOps coverage in-house*

However, for teams that are not using a SOC structure, 73 percent are in the process of setting up a SOC or have a plan to start one within the next 12 months. An additional 25 percent either have plans to start outside the next 12 months or are considering it, but do not have a current implementation plan in place. Forty-eight percent of enterprises that do not have a SOC are currently implementing one, while only 28 percent of midmarkets have a project underway. An additional 44 percent have a plan to start one in the next twelve months. Not surprisingly, only eleven percent of SMBs have a SOC in place. Those are the largest in that category. However, another 67 percent indicate they are starting a SOC structure in the next year. The only way for the smaller SMBs to accomplish that is through leveraging a significant number of outsourcing components with a central business liaison to coordinate activities.

The labor and skills shortages have driven many organizations to outsourcing. Listed are the top four most commonly outsourced security services.

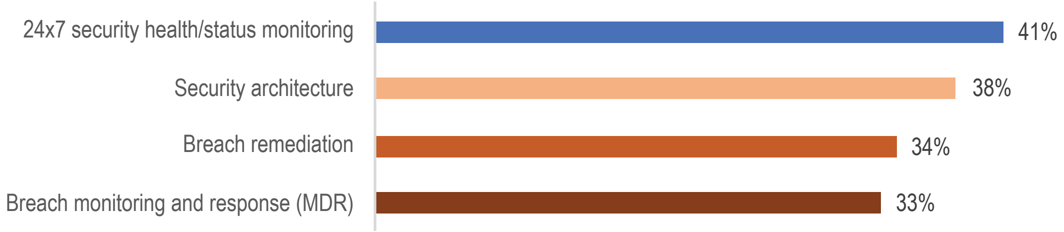

*Figure 32 Top four outsourced security functions*

Respondents identified their top reasons for engaging an MSSP. First was the belief that MSSPs perform better than their in-house capabilities. In fact, the top three reasons speak strongly for the MSSPs' capabilities and value-add than other motivations.

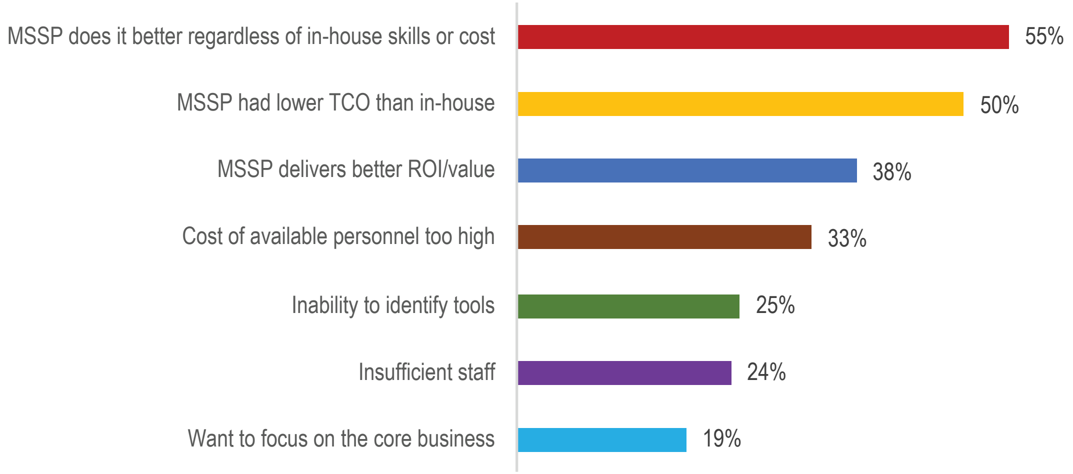

*Figure 33 Most significant drivers for engaging an MSSP*

Customers also indicated a generally high level of MSSP satisfaction and their willingness to put their money where their mouth is with increasing their spend with the service providers they have.

Listed here is the comparative satisfaction of internal teams versus those of the employed MSSPs.

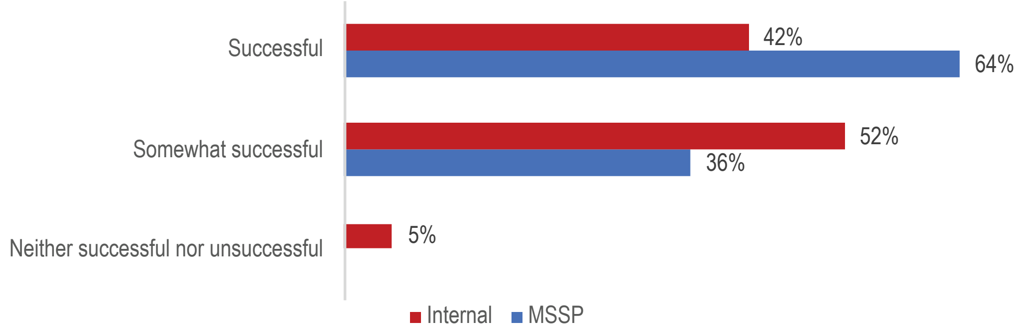

*Figure 34 MSSP success in delivering services over the past year*

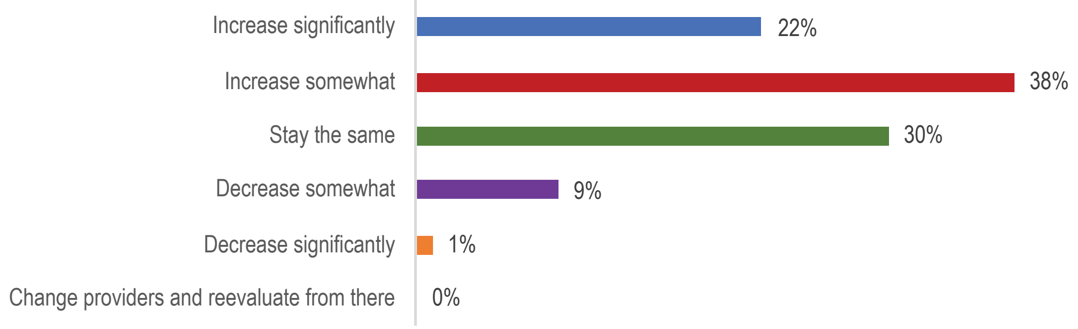

*Figure 35 Customers' MSSP spending intentions*

There has been an increasing trend of MSS adoption over the last five years with no indications that it will slow down. So long as providers are able to offer services with high perceived value, customers will continue to sign up, even if the dollar cost may be somewhat higher than doing it in-house. The key is how to continue to deliver the breadth and value so they can increase services once they are in the door. The largest threat to MSSP expansion is the security automation vendors. These vendors are also on a significant rise and may ultimately cap MSSP growth. They have different strengths, but focus on automating security policies and change management, incident investigation, and incident response from both a process and a technical execution perspective.

## SecOps Tools

### Consolidation Through Integration and Automation

There are over 1,400 different vendors that supply cyber security tools. SecOps has between 10 and 22 management interfaces to get the security job done. The adoption of niche or point solutions has been tremendous, but is now beginning to contract. Because point solutions were originally seen as better at the job, security shops purchased those to deal with their problems. Now, with the menagerie of point solutions, the problem of paying for and managing those tools has come to a head. To properly couch this, it is important to say that point solution vendors have their place and more often than not solve their problems well, so getting the job done is not generally the problem. However, there is nothing they can do to reduce the number of interfaces used to manage security. Consolidation of tools is the only way to do it. SecOps teams are actively trying to reduce the number of interfaces they deal with.

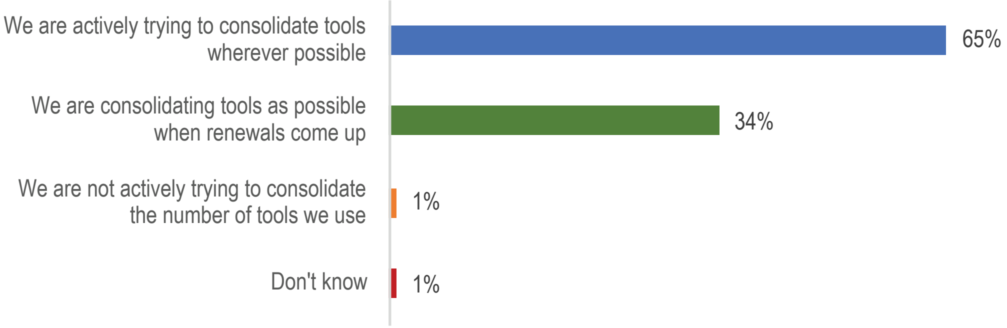

*Figure 36 SecOps is consolidating tools*

The cloud is solving some of this issue, but not all of it. Platform vendors are also addressing it, probably more so than just using the cloud. There has been significant merger and acquisition activity in the security space over the last five years, with the larger vendors absorbing and integrating smaller vendor functionality. This is a double-edged sword because sometimes vendors purchase other vendors to remove them from the competition—not to integrate. Other times, integrations are not successful and some functionality is lost, as well as larger companies' processes and roadmaps hampering innovation. Partnership is quite appealing to both point solution vendors and the customers because the customers get to keep the solutions they like while improving data sharing and reducing their needed interfaces. Technology consumers are leveraging all of these options to achieve the goals of tools reduction.

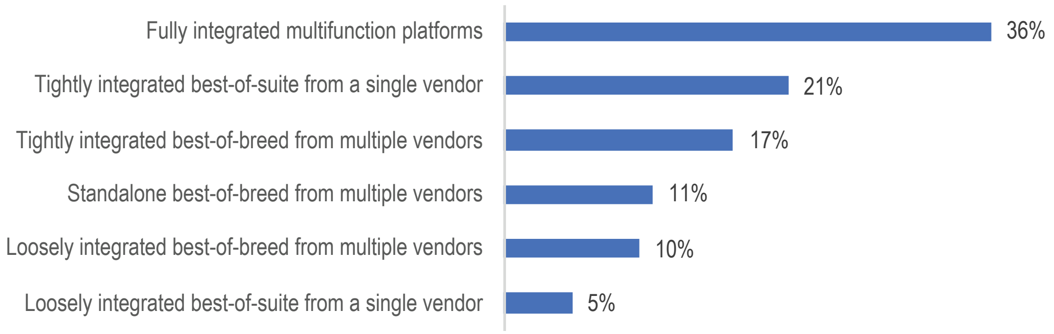

*Figure 37 SecOps approaches to consolidating tools*

When queried about the most important security management features to meet their business requirements, the majority of respondents said that integration with other IT management products was first order.

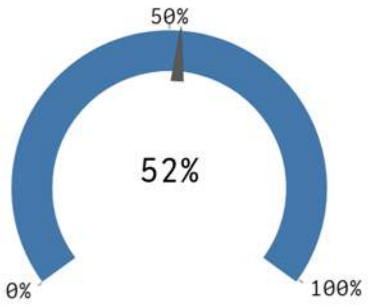

*Figure 38 Most important is integration with other IT mgmt. products*

Integration with automation and orchestration is the top integration driver. As this movement continues and is successful, it will remove some of the pressures driving customers to MSSPs.

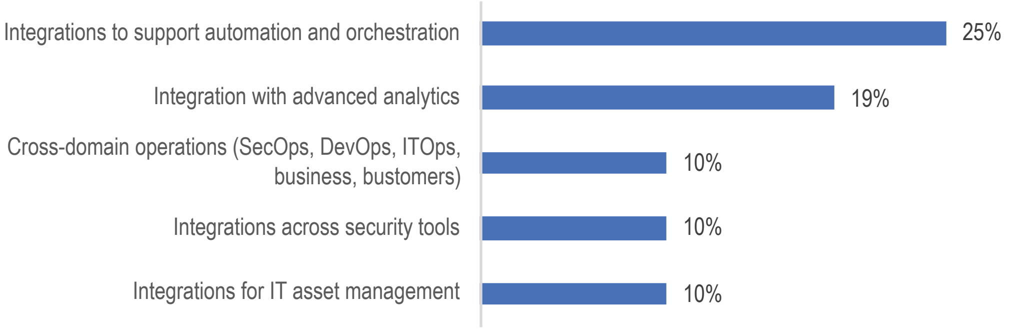

*Figure 39 Integration drivers for SecOps*

Integrations are a common driver for improving SecOps, and the primary integration driver is for automation and orchestration. Four of the top five monitoring features desired are automations.

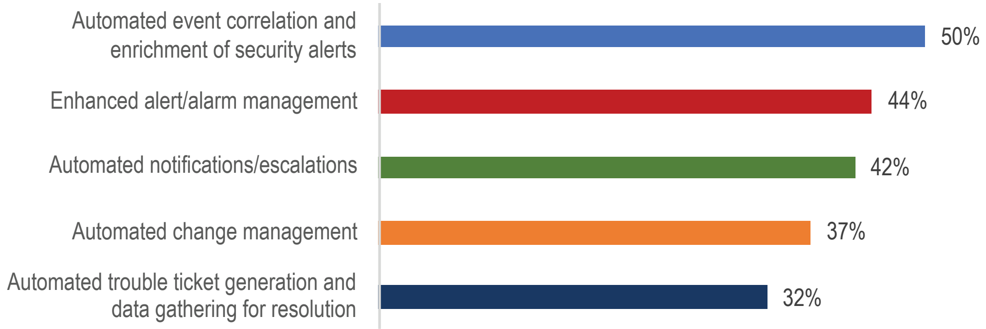

*Figure 40 Monitoring features providing the most value to SecOps*

Change management has traditionally been a sore spot for the business because poorly affected changes cause the vast majority of unplanned outages or service interruptions. SecOps is also looking at how to be a better internal service provider to the business by automating aspects of change management.

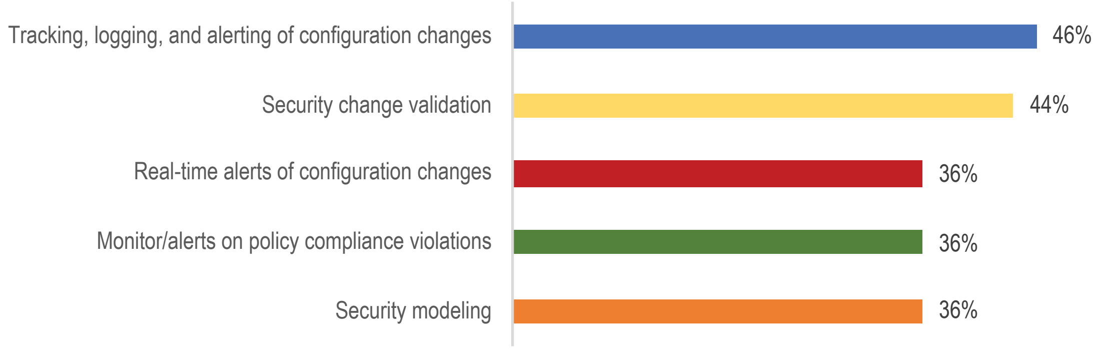

*Figure 41 Desired change management automations*

## Analytics

After automation and integrations, analytics is the next big hitter in security. Though automation and integration scored higher in the polls, there is a strong argument that better analytics should come first. Analytics transforms data into actionable information and intelligence. If companies can reduce the volume of tickets and better categorize them through better analytics, then they reduce the workload and allow SecOps to get the most important work done first. After all, automating a bad process gets business to the wrong places faster and more often.

Good analytics needs two things: good algorithms and as much good data as possible. It is important to understand the types of data a prospective analytics package or platform can ingest before you purchase.

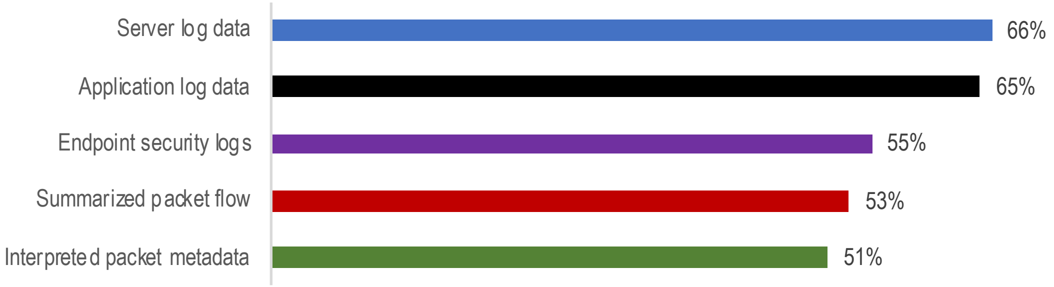

*Figure 42 Five types of data most often used in security analytics*

Once the data is being ingested, SecOps can get to work. Listed are the top three uses cases for security analytics:

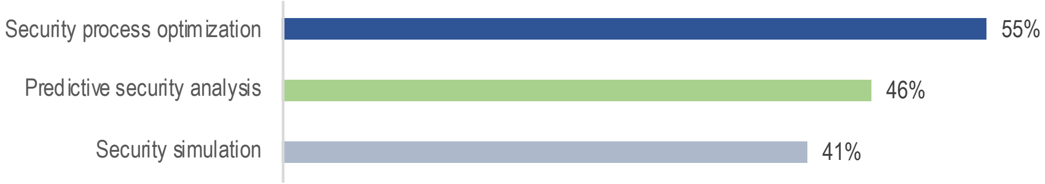

*Figure 43 Top three use cases for security analytics*

While there is no doubt that these are all valuable, it was surprising that behavioral analytics, though on the list, was not in the top three. The question asked "which were the most important," not "which are the most widely in use," so that could make a difference.

Understanding the importance of analytics, EMA evaluated why more operations do not have them in place. Though budgets are growing they do have limits, so EMA put budgets off to the side and focused on operational impediments.

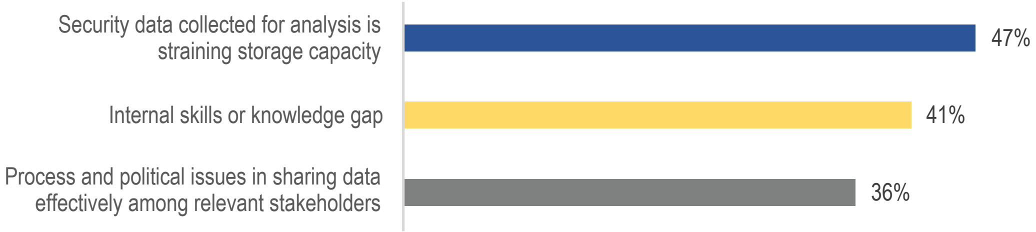

*Figure 44 Top three operational impediments to implementing security analytics*

Storage is cheap, but when companies start looking at petabytes for larger enterprises to store data for a year, it can put a strain on the budget. Given that sort of constraint, SecOps has to make tougher decisions on whether to reduce the timespan of data stored or whether there are more judicious choices to be made around data selected for ingestion. Not all data is good data. Some definitely provides better telemetry than others.

## EMA Perspective

There are a lot of common security problems in the world today. One report can't possibly cover all of them. A key finding is that while there are absolutely nuances to some of the problems that are specific to a vertical, there are very few, if any, security problems totally unique to any company size or vertical. Threat actors may be more persistent and the potential losses may be larger, but a solid security program is based on reducing risk. Each company has to prioritize its risk and address the most significant problems in a way they see most fit. If companies invest appropriately based on their true risk tolerance and follow best practices, they can be compliant and secure without worrying about which compliance regulations they are or are not meeting.

### 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 blog.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

3793-DomainTools.011719