White Paper

Enabling the Next-Generation Security Operation Model

Sponsored by: Cisco Systems

Curtis Price
May 2020

IDC OPINION

Managing an organization's security posture and mitigating risk are top of mind concerns for corporate executives and boards of directors. Consequently, organizations are spending more time and money on implementing the appropriate security technologies and procedures within security operations (SecOps) to effectively minimize their security risk. The rapid rise in data breaches, ransomware, and phishing attacks has disrupted business operations for organizations of all sizes and has had devastating financial impacts. Owing to the costs and long-term reputational damage of a security breach, business leaders are putting more scrutiny on the effectiveness of the spend needed by their security teams to thwart attacks. This in turn has forced security operations teams to rethink their approach and increase their focus/attention on enterprise security management.

SITUATION OVERVIEW

For years, organizations have been engaged in an "arms race" to keep pace with the frequency of malicious attacks and sophisticated adversaries using advanced technologies to conduct attacks. To defend themselves, organizations have deployed a plethora of security technologies and tools to combat a variety of attacks, including phishing attacks, ransomware, denial-of-services attacks, data breaches, and viruses.

In 2018, spending on security products and services totaled over $100 billion worldwide, with the market being split evenly between products and services, and IDC expects that over the next five years, this spending will grow approximately 11% and reach $168 billion by 2023. Despite this level of spend, multiple industry sources estimate that the total cost of data breaches, which includes legal fees, regulatory fines, and remediation, in 2018 ranged from $500 million to nearly $700 million, with the average cost of a breach for U.S. companies reaching $8 million. In addition to the costs of a breach, high-profile incidents at notable companies can have negative ramifications on an organization's brand, which could take years to overcome.

There is no doubt that the solutions organizations implement to improve their security posture are compromised by the increasing sophisticated capabilities of adversaries. Attackers are highly motivated and well-funded and are using advanced technologies and tools to circumvent the technologies that were designed to thwart their attacks. Attackers often use more advanced technology than what enterprises use for defense purposes.

IDC believes that today's model for security operations is still largely built on a reactive approach to dealing with security threats where responses can typically occur well after an attacker has gotten past an organization's security defense. However, this current model is rapidly succumbing to the challenges and dynamics inherent in today's cybersecurity market and forcing a shift to a more proactive model that takes advantage of advanced threat hunting techniques to accelerate the time to detect a security breach.

Security operations teams face a mix of technology, process, and organizational culture issues that have increased the complexity of enterprise security management. These challenges include the following:

- **Increasing volume of alerts.** Security operation center (SOC) teams struggle to prioritize the ever-growing list of potential indicators of compromise (IOCs) while addressing the burden of dealing with false positives that can compromise the efficiency of SOC analysts. This data deluge has the greatest impact on SOC layer 1 analysts where the volume of events is rendering the manual processes used at this level untenable.
- **Proliferation of security toolsets.** Owing to the buildup of security tools in the SOC, chief information security officers (CISOs), and more specifically the head of security operations, face the laborious task of integrating a mix of new and old tools into a cohesive system. The result of this buildup is a patchwork of tools that are not well integrated and severely limit the ability to have a holistic view across an organization's security controls.
- **Scarcity of qualified security expertise.** Organizations have found it difficult to build an effective staff to manage their security posture largely because of the lack of in-house security expertise. Organizations looking to build the requisite capabilities in-house can also find it costly to continuously maintain knowledge levels for their in-house staff, given the constantly evolving threat landscape. This has forced security operations teams to incorporate outside expertise to augment existing in-house security resources.
- **Limited visibility across the security infrastructure.** Visibility is severely limited in an architecture where technology silos exist. For organizations looking to gain a holistic picture of their security posture, they must move from a siloed architecture to one that provides end-to-end visibility. In addition, the lack of visibility across platforms has increased the amount of time it takes to detect and remediate a security breach.
- **Lack of a comprehensive security preparedness plan.** Organizations that neglect to develop a detailed security strategy that encompasses a security awareness plan, an incident response plan, and a process for measuring the effectiveness of their security operations face increased chances of suffering a security breach.

As security operations teams look to build a resilient operations center that provides a comprehensive and cohesive approach to identifying, protecting, and responding to security breaches, they must reevaluate their security operations requirements and devise new strategies to increase the effectiveness of their security operations. The changes needed to make these improvements require a mix of technology- and process-related enhancements.

Transformation Puts Security in the Spotlight

In addition to the challenges confronting security operations teams, organizations must also consider the security impact of any business transformation initiative. These initiatives often force organizations to consider the security ramifications and their impact on achieving the desired business outcome. Traditionally, security has been an afterthought that was "wrapper" implemented after the strategy had been formulated instead of a well-integrated, multilevel solution. This is beginning to change as business leaders push for security to be considered early in the strategy planning process so that steps can be taken to mitigate risk and remove obstacles to achieving business transformation objectives before the strategy is executed. Tying security risk to business risk has created even more complexity for security leaders because now they must think about mitigating risk, an iterative process that includes the following tasks:

- Planning to identify security vulnerabilities
- Assessment of existing security posture
- Implementation of security controls to address vulnerabilities
- Documentation of processes and procedures, including incident response plans
- Conducting regular exercises to practice security processes and procedures
- Identification of procedural gaps or technology issues

IDC believes that as organizations consider the current cybersecurity challenges they are facing and rethink their risk management strategies as a part of any transformation initiatives they are pursuing, they will look to make improvements in their overall security strategy and focus specifically on technologies, processes, and procedures within their security operations.

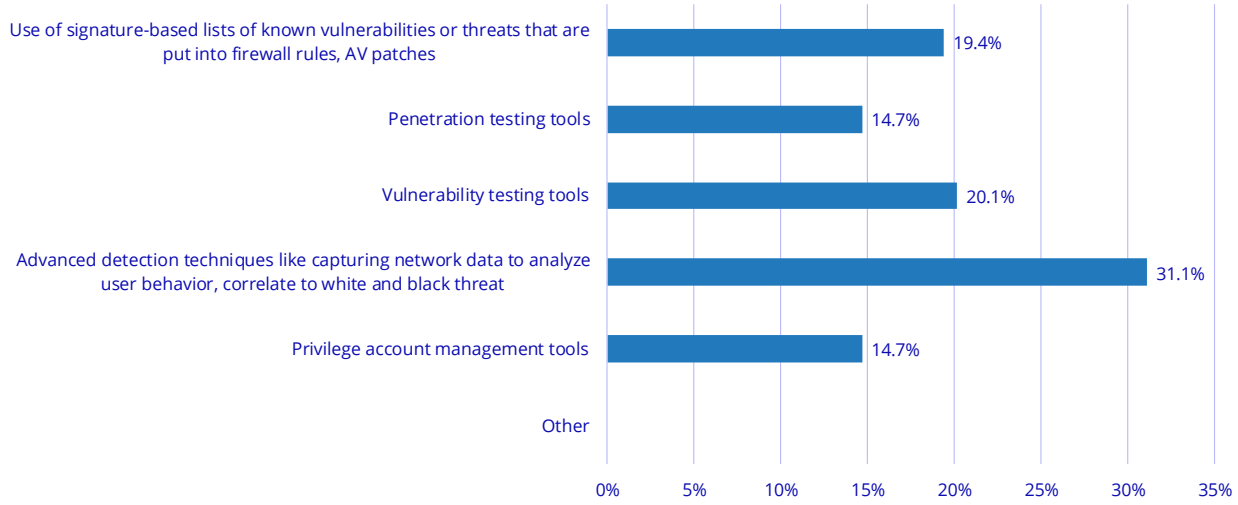
Next-Generation Security Operation Center Model

IDC believes that a new security operation model is needed to address the challenges stemming from the evolving threat landscape. The new model will reduce the reliance on manual processes and incorporate advanced technologies that enable deep insight through machine learning and artificial intelligence, as well as a more proactive approach to security management that includes proactive threat hunting and threat detection. In a recent survey conducted by IDC, respondents cited advanced detection techniques as the most effective method for threat detection (see Figure 1).

FIGURE 1

Methods Believed to Be Most Effective at Threat Detection

Q. Which methods do you believe are the most effective in detecting a threat in your environment? Please rank order their effectiveness, where 1 is the most effective, 2 the next most effective, and so forth.



n = 402

Base = all respondents

Notes:

Data is shown only for answers that ranked first.

This survey is managed by IDC's Quantitative Research Group.

Data is not weighed.

Use caution when interpreting small sample sizes.

Source: IDC's *MSSP Survey,* 2018

Artificial intelligence, machine learning, and automation are critical in today's SOC. These technologies are essential in handling the volume of alerts coming into the SOC and accelerating the time to detect and respond to a security breach. However, while these technologies help alleviate the staffing shortages and speed up identification and response efforts, the problem that organizations face is the lack of in-house experience to implement and manage artificial intelligence and machine learning.

IDC believes that owing to the lack of security expertise in many security teams, inexperience with advanced technologies, and the overall complexity of embedding security into digital transformation initiatives, security teams will increasingly seek help and work with outside firms that have demonstrated frameworks for enabling secure business transformation.

Cisco Business Critical Services for Security Operations

To help security operations leaders accelerate transformation and innovation across the IT landscape, Cisco reimagined the Business Critical Services (BCS) portfolio with the introduction of the three-tiered Life Cycle offers targeted to address unique SecOps requirements, as well as those of the architecture, engineering, network operations, and developer operations teams. The Essentials tier includes services essential to strengthening the security posture of an organization, while the Advantage tier of services allows an organization to accelerate its transformation initiatives and pursue innovation without the inherent risk. The newest tier, Premier, offers IT roles more flexible access to insights so customers can move with the speed of the business to create successful multidomain solutions. In addition, to help IT teams speed transitions and address skills gaps, Cisco and CX Specialized Partners are offering two additional add-on services: Specialized Teams and Expert as a Service. With Specialized Teams, customers can subscribe to a team of experts provided for a 12-month period or longer to address priority projects and unexpected events. Customers seeking to augment teams to cover long-term projects can subscribe to Expert as a Service to fulfil their technology requirements.

With services that can be aligned to the needs of the head of security operations, the Essentials and Advantage offerings enable security operations teams to speed the value they receive from their existing and future security investments.

By leveraging Cisco's expertise across various security technologies such as network security, endpoint, email, and identity access management, SecOps leaders gain access to Cisco's mature security detection and prevention methodologies, security tools, and deep artificial intelligence/machine learning–driven insight into their organization's security posture to make more informed decisions on how to protect, detect, and defend against attacks. The security operations services offered through BCS range from consultative advice in the security strategy planning process to forensic analysis and incident response.

Cisco Business Critical Services is a suite of cross-architecture subscription services that help customers ensure optimal performance of the network infrastructure through Cisco's expertise, analytics, and automation. The adoption of BCS not only allows customers to increase the value from their investments but also helps them reduce costly, redundant, and error-prone manual tasks through predictive and preventive analytics, which increases the efficiency of maintaining their environments.

BCS has developed an IT role approach designed to more accurately address the specific requirements of buyers/users to ensure that they are receiving the appropriate insight and analytics, training, expertise, and support necessary to meet their business, technology, and operations objectives to build more resilient, adaptive, and transformative IT.

The BCS framework is offered across all of Cisco's architectures and will be available at three tier levels – Essentials, Advantage, and Premier. Each tier provides a set of services that address the needs of key IT roles, and the various levels of the role, while providing more tailored solutions for companies with unique requirements. Each tier has three core fundamental components; each tier provides guidance throughout the technology life cycle through continuous customer engagement and value tailored to key IT roles.

Guidance Throughout the Technology Life Cycle

As companies pursue digital business models, the technology investments needed to support this move and the broader security issues that these digital strategies must address have created skills, process, and technical challenges that can slow digital transformation efforts. For security operations teams, the move to cloud as the core of IT, the need to support a broader array of endpoint devices, data protection, and privacy concerns have added to the complexities involved in security management.

Cisco addresses these challenges by providing expert guidance along the transformation journey. Cisco's experts provide advice aimed at accelerating their customer's life-cycle journey through onboarding and implementation to adoption and optimization to new technology transformations. Cisco's experts provide guidance, best practices, and proven methodologies focused on industrywide solutions to guide an organization through every stage of its life-cycle journey. Trusted experts share their valuable insight through a series of sessions including interactive technical webinars, 1:1 coaching sessions, experts assigned to a specific team, expert leader workshops, and expert reviews and recommendations. These experts employ use case best practice sharing and 1:1 personalized coaching engagements to optimally support you along your life-cycle journey. As enterprises are at various stages of their transformation, the breadth of Cisco's Business Critical Services provides the flexibility to meet customers wherever they are on their transformation journey while providing support throughout the full life cycle.

Key highlights of the BCS framework include:

- Interactive technical webinars focused on specific use cases
- 1:1 coaching sessions
- Experts assigned to a specific team
- Expert leaders for workshops
- Expert reviews on various life-cycle topics

Continuous Engagement

To enable continuous engagement along the technology life cycle, Cisco experts meet with their Business Critical customers for up to 24 times per year, depending upon the tier selected and deliverable requested, to assess the state of their Cisco technology. Couple this with the other expert resources and customers can have over 40+ engagements per year. Cisco experts leverage innovative technologies, such as machine learning, artificial intelligence, and diagnostic tools, derived from over 30 years of technology leadership. These experts combine data-driven insights with their knowledge of a company's IT environment to maximize the time to value of an organization's technology investments. IDC believes Cisco's BCS experts will prove extremely valuable in this area. The volume of log data that security analysts must analyze has increased exponentially. Having a Cisco expert available to help analyze and prioritize the events that action should be taken on will be highly valued by security operations teams that are already struggling with the deluge of data they must analyze. In addition, their expert teams help customers predict operational risk and engage in knowledge transfer coaching to improve the security teams' skill sets, reducing the time it takes to deploy, detect, and remediate.

Value for Each IT Role

Another important value proposition for BCS is the specific value that is delivered to key IT roles. IT roles in a customer's organization are empowered with continuous access to trusted Cisco experts, along with analytics, insights, and automation to change that equation, helping customers achieve higher performance, speed adoption, and accelerate transformation. While the BCS framework addresses the needs of key IT roles, within security operations, the ability to provide specific guidance that helps accelerate threat detection and response is critical to minimizing the impact of a security breach. Table 1 shows a summary of the value that is delivered to key IT roles through the BCS framework.

TABLE 1

BCS Value for IT Roles

IT Role	BCS Value
Security operations	Teams can improve the organization's security posture to protect, detect, and defend against cybersecurity incidents across the enterprise. Business Critical Services consultative support can provide customers with an improved security posture to proactively protect and defend from known and unknown threats. According to Cisco, SecOps services can help reduce monetary impacts from cyberattacks by 99%.
Architecture	Teams can quickly build a strategy to implement innovative technology that aligns IT strategy with business intent. Architects will benefit by gaining the agility and insight they require for successful transformation while lowering risk to transform. According to Cisco, BCS for architects can deliver transformations 50% more successfully and create new revenue streams more securely.
Engineering	Teams can de-risk technology transitions and design and accelerate deployment of new IT solutions to increase business agility. Cisco's design and deployment guidance helps address ever-changing business requirements. According to Cisco, these services for engineers can offer more effective software upgrades, lower deployment costs, and 47% reduction in testing time.
Network operations (NetOps)	Teams can maintain a secure, always-on customer network using predictive analytics, industry standards, and best practices. The service provides network and IT managers the ability to predict and resolve issues and increase performance, driven by analytics and automation. According to Cisco, BCS for NetOps offers operational gains and can reduce downtime by up to 74%.

Source: IDC, 2020

The BCS framework is available at three tier levels:

- **Essentials.** This tier provides access to Cisco's intellectual capital and deep technical insights and analytics, mitigating cyber-risk and optimizing operational performance of key security controls. With remote access to Cisco experts who can act as an extension of a customer's existing operations staff, a customer's staff can prioritize actions that need to be taken to meet business objectives. These services also provide operational insight into and analysis of an organization's infrastructure and applications environment as well as recommendations on potential risks and vulnerabilities that need to be addressed.

The Essentials tier includes the following components:

- Operational insights
- Change window support
- Expert review workshops
- Ask the experts

The Essentials tier provides holistic visibility into an organization's environment to identify potential risks and offers an array of capabilities to build a comprehensive security strategy. Ask the experts provides a catalog of scheduled open enrollment or recorded webinar sessions aligned to Cisco's Customer Success Portfolio. These sessions provide access to Cisco experts who share insights and recommend best practices to help onboard, implement, use, adopt, and optimize Cisco solutions.

- **Advantage.** This tier includes all the Essentials' capabilities plus additional new services. The Advantage tier provides a richer set of high-touch advisory services, delivered onsite and remotely, to help increase technology adoption and accelerate transformation. By offering a "high touch" set of advisory services, the Advantage tier helps an organization develop a life-cycle approach to security management. In addition, the Advantage tier addresses the lack of skilled expertise that many organizations face by augmenting the customer's team with transformation guidance from Cisco experts. Accelerators guides successful technology adoption by letting customers choose technical sessions per year from a catalog of Cisco expert one-to-one technical sessions that are aligned to Cisco's Customer Success Portfolio.

  The Advantage tier includes all the Essentials components plus the following:

  - Expert incident review
  - Accelerators

- **Premier.** This tier offers more flexible access to insights to create successful multidomain solutions. With BCS Premier, key IT roles get the insights they need to move with the speed of the business with less risk and faster time to value. Through ongoing access to Cisco experts, analytics, insights, and automation, Premier enables organizations to successfully transition to and optimize core Cisco architectures by dynamically adjusting guidance to the most strategic initiatives. Further:

  - To speed transitions and address skills gaps, Cisco developed two new add-ons — Specialized Teams and Expert as a Service:
    - Specialized Teams can be added to the customer's contract, enabling Cisco and the customer to identify highly specified needs and quickly assemble the right experts to deliver a rapid, focused engagement.
    - Customers that want to augment their teams with a dedicated expert, like a solution architect, consulting engineer, or project manager, to cover long-term projects can have their requirements fulfilled through Expert as a Service.

CHALLENGES AND OPPORTUNITIES

The cybersecurity challenges that organizations face have created a level of complexity that has forced organizations to seek help from third parties with comprehensive security expertise and capabilities that allow them to address people skill, technology, process, and procedural issues. The transition of the SecOps model from reactive to proactive is critical and requires a completely new set of capabilities to drive effective security management.

There are several factors that will dictate what an organization will need to do to improve its security posture. These factors include the level of maturity of an organization's security operations, the skill level of an organization's security operations team, the security technologies currently in use, the potential cost of breaches, and the risk appetite of the business. These factors will largely dictate where an organization is on its security journey and highlight the requirements needed at each stage of the journey. Securing an organization's IT environment is a continuous process, and the ability to match security requirements to current and future needs is an essential component of an overall security strategy.

CONCLUSION

Organizations looking to develop comprehensive security strategy plans require a full set of solutions that address security needs holistically. The solutions start with security strategy planning but also include a broad array of offerings that address requirements for compliance, security operations effectiveness, and advanced technologies for threat detection. Through Business Critical Services Life Cycle tiers, Cisco has created a broad portfolio of capabilities that allow organizations to flexibly build their abilities to improve their security posture and resiliency while leveraging Cisco security expertise to help build a long-term security vision that is tied to an organization's business objectives.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com