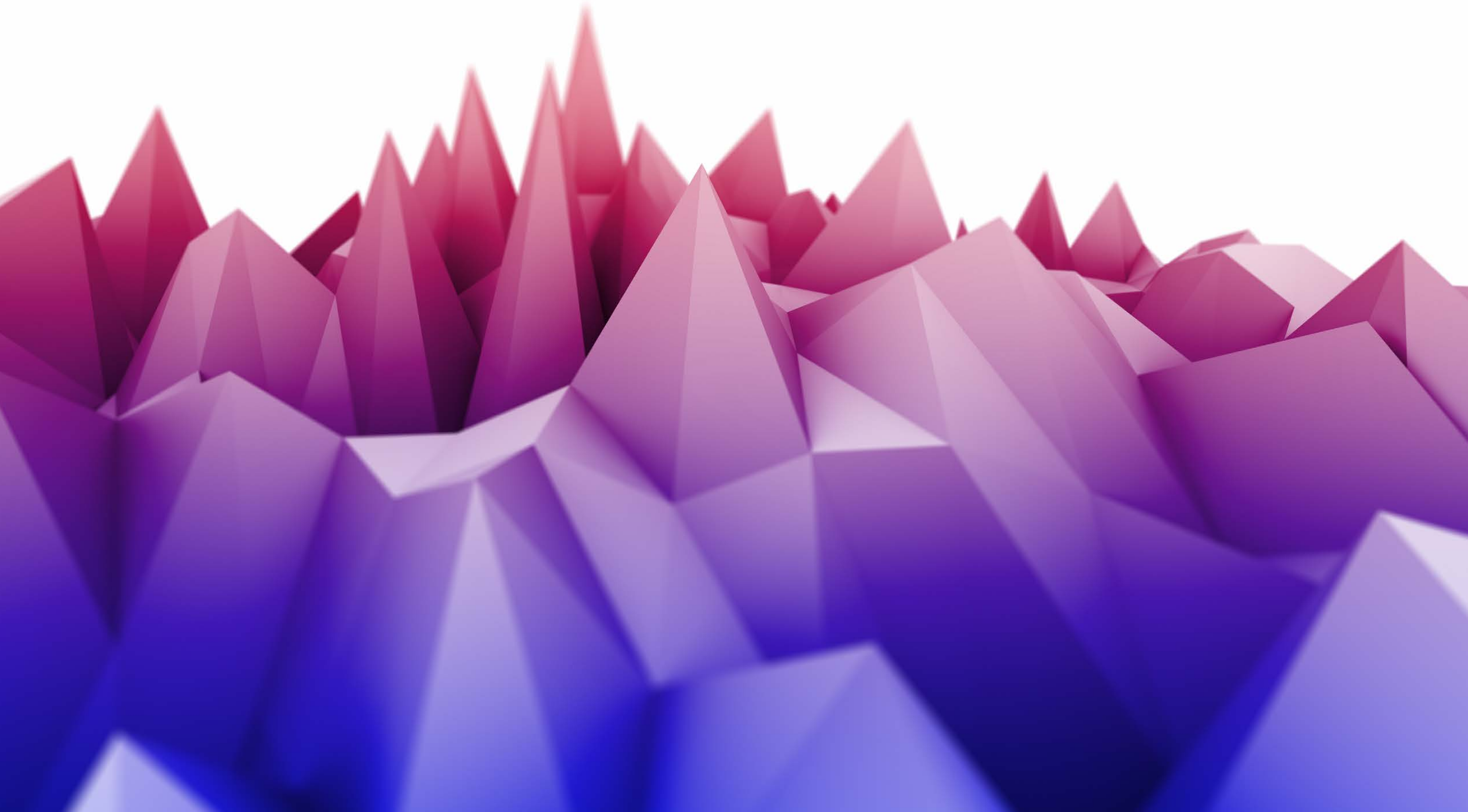
CyberRes

Research Report

2021 State of Security Operations

Insights from SecOps decision-makers around the globe, with research and recommendations to advance your SOC and reduce business risk.



Five Key CISO Highlights

79% of SOCs have increased their adoption of **advanced security technologies** during COVID-19 to combat evolving threats.

The biggest challenge for security operations teams in 2021 is monitoring security across a **growing attack surface**.

85% of respondents increased **monitoring controls** as a response to COVID-related workforce transformation, as well as complex remote access requirements.

A top priority is the effort to build repeatable processes backed by **Priority Intelligence Requirements (PIRs)**.

72% of SOCs believe **red teaming** to be essential, and conduct exercises at least twice per year to encourage vigilance.

Table of Contents

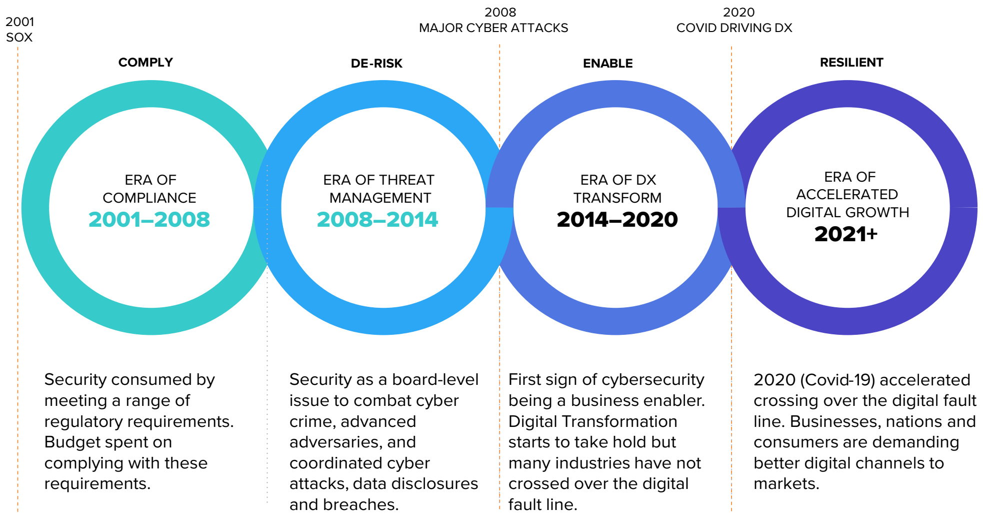
Executive Summary

How Has 2021 Changed Our Thinking?

The global pandemic turned the world on its head in 2020, and businesses—and the security teams that protect them—were no exception. While business IT spending declined by 3.2% in 2020,[1] adapting infrastructure to cater to remote work accompanied by a global increase in threat activity resulted in a 6.4% growth in overall security-related spending, and a forecasted growth of 12.4% in 2021.[2] Businesses increased their share of cloud-based infrastructure, applications, and business processes, driving a rapid expansion of security monitoring capabilities and tooling into cloud environments.

CYBER RESILIENCY IN 2021

THEN, NOW AND FUTURE



Security consumed by meeting a range of regulatory requirements. Budget spent on complying with these requirements.

Security as a board-level issue to combat cyber crime, advanced adversaries, and coordinated cyber attacks, data disclosures and breaches.

First sign of cybersecurity being a business enabler. Digital Transformation starts to take hold but many industries have not crossed over the digital fault line.

2020 (Covid-19) accelerated crossing over the digital fault line. Businesses, nations and consumers are demanding better digital channels to markets.

Figure 1. Cyber Resiliency in 2021

Not surprisingly, attackers exploited the chaos created by the pandemic. One incident response firm found that 51% of all security breaches included a ransomware component,[3] which increasingly used the two-pronged approach of stealing and then encrypting data to create more pressure on the victims to pay the ransom.[4] Meanwhile, the frequency of distributed denial-of-service (DDoS) attacks climbed by 25%, driven by inexpensive DDoS-as-a-service offerings.[5]

The CyberRes 2021 State of Security Operations survey took the pulse of global security teams that are defending against these attacks to see how their approaches to security have changed, how they plan to mature their security operations centers (SOCs) going forward, and how they are equipping their SOCs to handle advanced adversaries, expanding attack surfaces, and other key challenges, both now and in the future.

[1] Gartner. "Gartner Forecasts Worldwide IT Spending to Grow 6.2% in 2021." Press Release. 25 January 2021.

[2] Gartner. "Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021." Press Release. 17 May 2021.

[3] Lemos, Robert. "Ransomware Makes Up Half of All Major Incidents." Dark Reading. News Article. 9 December 2020.

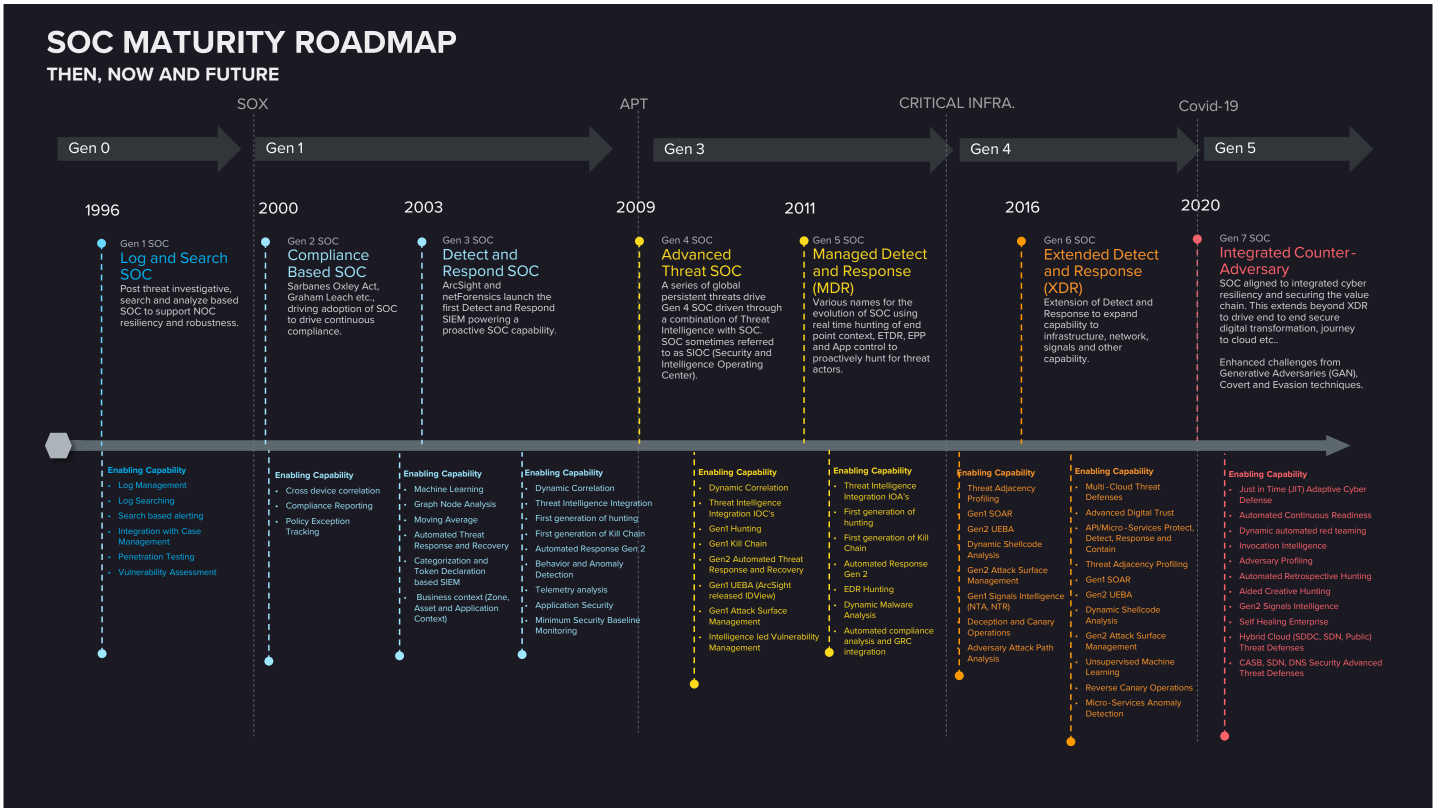
[4] Lemos, Robert. "Pay-or-Get-Breached Ransomware Schemes Take Off." Dark Reading. News Article. 26 January 2021.

[5] Vijayan, Jai. "DDoS Attacks Spiked, Became More Complex in 2020." Dark Reading. News Article. 30 December 2020.

SOC Journey

The design, development, and management of a digital, cloud, and business aligned SOC can be a complex task—with everything from acronyms, methods, integration models, and edge considerations (IoT, IIoT) to regulatory requirements and privacy implications. SOCs that operate for multi-nationals need to consider the balance between end-to-end visibility and the need to comply with data sovereignty and labor requirements.

Even though various credible frameworks and platforms have come to the market over the last few years (e.g., MDR, XDR, etc.), these methods and capabilities are evolutionary, and should still be centered on best practices that have evolved over the last two decades. A major goal of the State of Security Operations Report is to align where we have been, where we are, and where we believe we are going, in terms of challenges (and their business impact), technology, people, and processes. The below is a high-level view of the SecOps journey, from the mid-90s to today, and to what we expect in the future.



SOC MATURITY ROADMAP

THEN, NOW AND FUTURE

Gen 1 SOC
Log and Search SOC
Post threat investigative, search and analyze based SOC to support NOC resiliency and robustness.

Gen 2 SOC
Compliance Based SOC
Sarbanes Oxley Act, Graham Leach etc., driving adoption of SOC to drive continuous compliance.

Gen 3 SOC
Detect and Respond SOC
ArcSight and netForensics launch the first Detect and Respond SIEM powering a proactive SOC capability.

Gen 4 SOC
Advanced Threat SOC
A series of global persistent threats drive Gen 4 SOC driven through a combination of Threat Intelligence with SOC. SOC sometimes referred to as SIOC (Security and Intelligence Operating Center).

Gen 5 SOC
Managed Detect and Response (MDR)
Various names for the evolution of SOC using real time hunting of end point context, ETDR, EPP and App control to proactively hunt for threat actors.

Gen 6 SOC
Extended Detect and Response (XDR)
Extension of Detect and Response to expand capability to infrastructure, network, signals and other capability.

Gen 7 SOC
Integrated Counter-Adversary
SOC aligned to integrated cyber resiliency and securing the value chain. This extends beyond XDR to drive end to end secure digital transformation, journey to cloud etc..

Enhanced challenges from Generative Adversaries (GAN), Covert and Evasion techniques.

Enabling Capability
- Log Management
- Log Searching
- Search based alerting
- Integration with Case Management
- Penetration Testing
- Vulnerability Assessment

Enabling Capability
- Cross device correlation
- Compliance Reporting
- Policy Exception Tracking

Enabling Capability
- Machine Learning
- Graph Node Analysis
- Moving Average
- Automated Threat Response and Recovery
- Categorization and Token Declaration based SIEM
- Business context (Zone, Asset and Application Context)

Enabling Capability
- Dynamic Correlation
- Threat Intelligence Integration
- First generation of hunting
- First generation of Kill Chain
- Automated Response Gen 2
- Behavior and Anomaly Detection
- Telemetry analysis
- Application Security
- Minimum Security Baseline Monitoring

Enabling Capability
- Dynamic Correlation
- Threat Intelligence Integration IOC's
- Gen1 Hunting
- Gen1 Kill Chain
- Gen2 Automated Threat Response and Recovery
- Gen1 UEBA (ArcSight released IDView)
- Gen1 Attack Surface Management
- Intelligence led Vulnerability Management

Enabling Capability
- Threat Intelligence Integration IOA's
- First generation of hunting
- First generation of Kill Chain
- Automated Response Gen 2
- EDR Hunting
- Dynamic Malware Analysis
- Automated compliance analysis and GRC integration

Enabling Capability
- Threat Adjacency Profiling
- Gen1 SOAR
- Gen2 UEBA
- Dynamic Shellcode Analysis
- Gen2 Attack Surface Management
- Gen1 Signals Intelligence (NTA, NTR)
- Deception and Canary Operations
- Adversary Attack Path Analysis

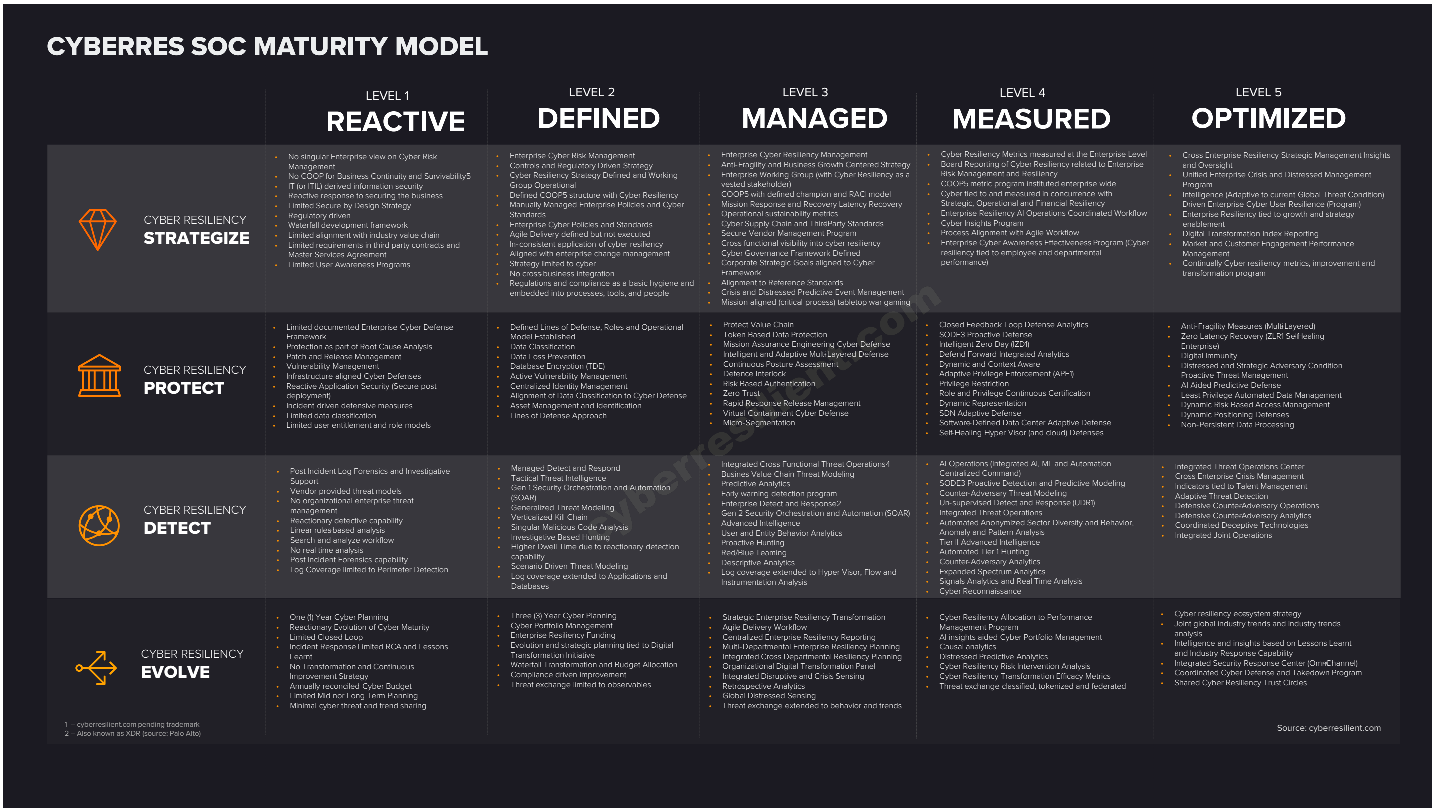
Enabling Capability
- Multi-Cloud Threat Defenses
- Advanced Digital Trust
- API/Micro-Services Protect, Detect, Response and Contain
- Threat Adjacency Profiling
- Gen1 SOAR
- Gen2 UEBA
- Dynamic Shellcode Analysis
- Gen2 Attack Surface Management
- Unsupervised Machine Learning
- Reverse Canary Operations
- Micro-Services Anomaly Detection

Enabling Capability
- Just in Time (JIT) Adaptive Cyber Defense
- Automated Continuous Readiness
- Dynamic automated red teaming
- Invocation Intelligence
- Adversary Profiling
- Automated Retrospective Hunting
- Aided Creative Hunting
- Gen2 Signals Intelligence
- Self Healing Enterprise
- Hybrid Cloud (SDDC, SDN, Public) Threat Defenses
- CASB, SDN, DNS Security Advanced Threat Defenses

Figure 2. SOC Maturity Roadmap—Image can be clicked on to view a full-size version

SOC Maturity

To address business resiliency, secure digital transformation, and deliver an elastic workforce, enterprises need to address modern threats, reduce business risk, and suppress operational impact. Security operations has come a long way since it first emerged in the mid-90s. We have gone through a NOC to SOC 2.0 (an integrated NOC and SOC), EDR, MDR, XDR and beyond. This has created a state where organizations can vary wildly in their SOC maturity, depending on the frameworks, technologies, and strategies they adopt.



CYBERRES SOC MATURITY MODEL

	LEVEL 1 REACTIVE	LEVEL 2 DEFINED	LEVEL 3 MANAGED	LEVEL 4 MEASURED	LEVEL 5 OPTIMIZED
CYBER RESILIENCY **STRATEGIZE**	• No singular Enterprise view on Cyber Risk Management • No COOP for Business Continuity and Survivability5 • IT (or ITIL) derived information security • Reactive response to securing the business • Limited Secure by Design Strategy • Regulatory driven • Waterfall development framework • Limited alignment with industry value chain • Limited requirements in third party contracts and Master Services Agreement • Limited User Awareness Programs	• Enterprise Cyber Risk Management • Controls and Regulatory Driven Strategy • Cyber Resiliency Strategy Defined and Working Group Operational • Defined COOP5 structure with Cyber Resiliency • Manually Managed Enterprise Policies and Cyber Standards • Enterprise Cyber Policies and Standards • Agile Delivery defined but not executed • In-consistent application of cyber resiliency • Aligned with enterprise change management • Strategy limited to cyber • No cross-business integration • Regulations and compliance as a basic hygiene and embedded into processes, tools, and people	• Enterprise Cyber Resiliency Management • Anti-Fragility and Business Growth Centered Strategy • Enterprise Working Group (with Cyber Resiliency as a vested stakeholder) • COOP5 with defined champion and RACI model • Mission Response and Recovery Latency Recovery • Operational sustainability metrics • Cyber Supply Chain and ThirdParty Standards • Secure Vendor Management Program • Cross functional visibility into cyber resiliency • Cyber Governance Framework Defined • Corporate Strategic Goals aligned to Cyber Framework • Alignment to Reference Standards • Crisis and Distressed Predictive Event Management • Mission aligned (critical process) tabletop war gaming	• Cyber Resiliency Metrics measured at the Enterprise Level • Board Reporting of Cyber Resiliency related to Enterprise Risk Management and Resiliency • COOP5 metric program instituted enterprise wide • Cyber tied to and measured in concurrence with Strategic, Operational and Financial Resiliency • Enterprise Resiliency AI Operations Coordinated Workflow • Cyber Insights Program • Process Alignment with Agile Workflow • Enterprise Cyber Awareness Effectiveness Program (Cyber resiliency tied to employee and departmental performance)	• Cross Enterprise Resiliency Strategic Management Insights and Oversight • Unified Enterprise Crisis and Distressed Management Program • Intelligence (Adaptive to current Global Threat Condition) Driven Enterprise Cyber User Resilience (Program) • Enterprise Resiliency tied to growth and strategy enablement • Digital Transformation Index Reporting • Market and Customer Engagement Performance Management • Continually Cyber resiliency metrics, improvement and transformation program
CYBER RESILIENCY **PROTECT**	• Limited documented Enterprise Cyber Defense Framework • Protection as part of Root Cause Analysis • Patch and Release Management • Vulnerability Management • Infrastructure aligned Cyber Defenses • Reactive Application Security (Secure post deployment) • Incident driven defensive measures • Limited data classification • Limited user entitlement and role models	• Defined Lines of Defense, Roles and Operational Model Established • Data Classification • Data Loss Prevention • Database Encryption (TDE) • Active Vulnerability Management • Centralized Identity Management • Alignment of Data Classification to Cyber Defense • Asset Management and Identification • Lines of Defense Approach	• Protect Value Chain • Token Based Data Protection • Mission Assurance Engineering Cyber Defense • Intelligent and Adaptive Multi-Layered Defense • Continuous Posture Assessment • Defence Interlock • Risk Based Authentication • Zero Trust • Rapid Response Release Management • Virtual Containment Cyber Defense • Micro-Segmentation	• Closed Feedback Loop Defense Analytics • SODE3 Proactive Defense • Intelligent Zero Day (IZD1) • Defend Forward Integrated Analytics • Dynamic and Context Aware • Adaptive Privilege Enforcement (APE1) • Privilege Restriction • Role and Privilege Continuous Certification • Dynamic Representation • SDN Adaptive Defense • Software-Defined Data Center Adaptive Defense • Self-Healing Hyper Visor (and cloud) Defenses	• Anti-Fragility Measures (Multi-Layered) • Zero Latency Recovery (ZLR1 Self-Healing Enterprise) • Digital Immunity • Distressed and Strategic Adversary Condition Proactive Threat Management • AI Aided Predictive Defense • Least Privilege Automated Data Management • Dynamic Risk Based Access Management • Dynamic Positioning Defenses • Non-Persistent Data Processing
CYBER RESILIENCY **DETECT**	• Post Incident Log Forensics and Investigative Support • Vendor provided threat models • No organizational enterprise threat management • Reactionary detective capability • Linear rules-based analysis • Search and analyze workflow • No real time analysis • Post Incident Forensics capability • Log Coverage limited to Perimeter Detection	• Managed Detect and Respond • Tactical Threat Intelligence • Gen 1 Security Orchestration and Automation (SOAR) • Generalized Threat Modeling • Verticalized Kill Chain • Singular Malicious Code Analysis • Investigative Based Hunting • Higher Dwell Time due to reactionary detection capability • Scenario Driven Threat Modeling • Log coverage extended to Applications and Databases	• Integrated Cross Functional Threat Operations4 • Busines Value Chain Threat Modeling • Predictive Analytics • Early warning detection program • Enterprise Detect and Response2 • Gen 2 Security Orchestration and Automation (SOAR) • Advanced Intelligence • User and Entity Behavior Analytics • Proactive Hunting • Red/Blue Teaming • Descriptive Analytics • Log coverage extended to Hyper Visor, Flow and Instrumentation Analysis	• AI Operations (Integrated AI, ML and Automation Centralized Command) • SODE3 Proactive Detection and Predictive Modeling • Counter-Adversary Threat Modeling • Un-supervised Detect and Response (UDR1) • Integrated Threat Operations • Automated Anonymized Sector Diversity and Behavior, Anomaly and Pattern Analysis • Tier II Advanced Intelligence • Automated Tier 1 Hunting • Counter-Adversary Analytics • Expanded Spectrum Analytics • Signals Analytics and Real Time Analysis • Cyber Reconnaissance	• Integrated Threat Operations Center • Cross Enterprise Crisis Management • Indicators tied to Talent Management • Adaptive Threat Detection • Defensive Counter-Adversary Operations • Defensive Counter-Adversary Analytics • Coordinated Deceptive Technologies • Integrated Joint Operations
CYBER RESILIENCY **EVOLVE**	• One (1) Year Cyber Planning • Reactionary Evolution of Cyber Maturity • Limited Closed Loop • Incident Response Limited RCA and Lessons Learnt • No Transformation and Continuous Improvement Strategy • Annually reconciled Cyber Budget • Limited Mid nor Long Term Planning • Minimal cyber threat and trend sharing	• Three (3) Year Cyber Planning • Cyber Portfolio Management • Enterprise Resiliency Funding • Evolution and strategic planning tied to Digital Transformation Initiative • Waterfall Transformation and Budget Allocation • Compliance driven improvement • Threat exchange limited to observables	• Strategic Enterprise Resiliency Transformation • Agile Delivery Workflow • Centralized Enterprise Resiliency Reporting • Multi-Departmental Enterprise Resiliency Planning • Integrated Cross Departmental Resiliency Planning • Organizational Digital Transformation Panel • Integrated Disruptive and Crisis Sensing • Retrospective Analytics • Global Distressed Sensing • Threat exchange extended to behavior and trends	• Cyber Resiliency Allocation to Performance Management Program • AI insights aided Cyber Portfolio Management • Causal analytics • Distressed Predictive Analytics • Cyber Resiliency Risk Intervention Analysis • Cyber Resiliency Transformation Efficacy Metrics • Threat exchange classified, tokenized and federated	• Cyber resiliency ecosystem strategy • Joint global industry trends and industry trends analysis • Intelligence and insights based on Lessons Learnt and Industry Response Capability • Integrated Security Response Center (Omni-Channel) • Coordinated Cyber Defense and Takedown Program • Shared Cyber Resiliency Trust Circles

1 – cyberresilient.com pending trademark
2 – Also known as XDR (source: Palo Alto)

Source: cyberresilient.com

Figure 3. SOC Maturity Model—Image can be clicked on to view a full-size version

These varying frameworks have primarily evolved from some key fundamentals and critical topics:

- **Cyber resiliency:** To align with enterprise, digital and cyber resiliency goals, the SOC needs to map its operational capabilities, threat models, risk, and performance metrics to see how each helps to secure the value chain. Terms for SOC evolution (EDR, MDR, etc.) may come and go, but the fundamentals of securing the value chain will be a persistent determinant of SOC alignment with the business.
- **Securing what matters:** Security operations teams need to focus their efforts around protecting critical business functions and processes, the digital supply chain, and the 'crown jewels'.

- **Modernization:** SOCs need to address both current and modern threats that could impact operational resiliency. For example, how can SOAR, automation, and AIOps play a role in the modern SOC to counter advanced adversaries that have evolved with automated tactics and procedures.
- **Going beyond Detect and Respond:** Securing the business requires a tightly orchestrated SOC that extends its view beyond simple detection and response. An effective SOC considers all of the activities listed in the NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover.

Highlights of the Report

The following are highlights of the 2021 State of Security Operations report:

- **Growth during COVID-19:** Security operations teams have evolved and expanded during the COVID-19 pandemic. 85% have increased their budgets, 73 % have increased their staffing, and 79% have increased their adoption of advanced security technologies.
- **Technology Adoption and Investment Trends:** Organizations globally are accelerating investments in unified data lakes, attack surface management, red teaming, and various forms of advanced analysis. On average, 38% of respondents are planning to adopt these solutions over the next 12 months.
- **The Essential Cloud:** Roughly 85% of companies have increased their adoption of cloud security technologies. As a result, 99% of organizations now use the cloud for IT security operations. On average, nearly two-thirds of their IT security operations software and services are already deployed in the cloud.
- **AI vs Advanced Threats:** 59% of respondents say improving detection of advanced threats is the top use case for AI, machine learning, and automation.
- **Threat Intelligence:** 82% of companies have increased their adoption of threat intelligence (TI) in the past year. The top two priority investments surrounding TI are: 1. Setting up a Threat Intelligence Platform (TIP), and 2. Building a repeatable process backed by priority intelligence requirements (PIRs).
- **The Talent War:** 97% of respondents report the need for additional skilled staffing on their security operations teams. The greatest need is in attack detection and analysis.
- **Outsourcing for Support:** 92% of organizations outsource a portion of their SecOps functions. On average, six to seven functions are outsourced to some degree.
- **Top Challenges in 2021:**
    1. Monitoring security across a growing attack surface—Selected by 40%
    2. Expanding workloads to cloud/hybrid environments—Selected by 37%
    3. Preemptively detecting threats to reduce exposure—Selected by 32%

Introduction

Objective

The CyberRes 2021 State of Security Operations report offers a close look at the changes, trends, challenges, and strategies of security operations (SecOps) teams around the globe. Specifically, we wanted to hear from security executives, directors, managers, and other SecOps decision makers. Pulling primarily from the results of the 2021 State of Security Operations survey, this report leverages data from over 500 security operations leaders and decision makers to offer an informative assessment of the current state of SecOps and its expected state in the near-future.

Going beyond the survey results, this report also offers implications and insights into security operations. Watch for our “C-Level Insight” highlight boxes, which include special recommendations for CISOs, CSOs, and other executives. These insights stem from a team of experts at CyberRes and Micro Focus who have either current or past C-Suite experience in security operations.

Methodology

CyberRes developed a 20-question survey, not counting additional qualifier questions and demographic questions, through a respected web-based survey distribution service provider. The survey was promoted to a database of IT decision makers, managed by the service provider.

To ensure accurate responses, the survey was translated into multiple languages appropriate for the seven countries where the survey was distributed. Responses were collected from May 15 until May 31, 2021.

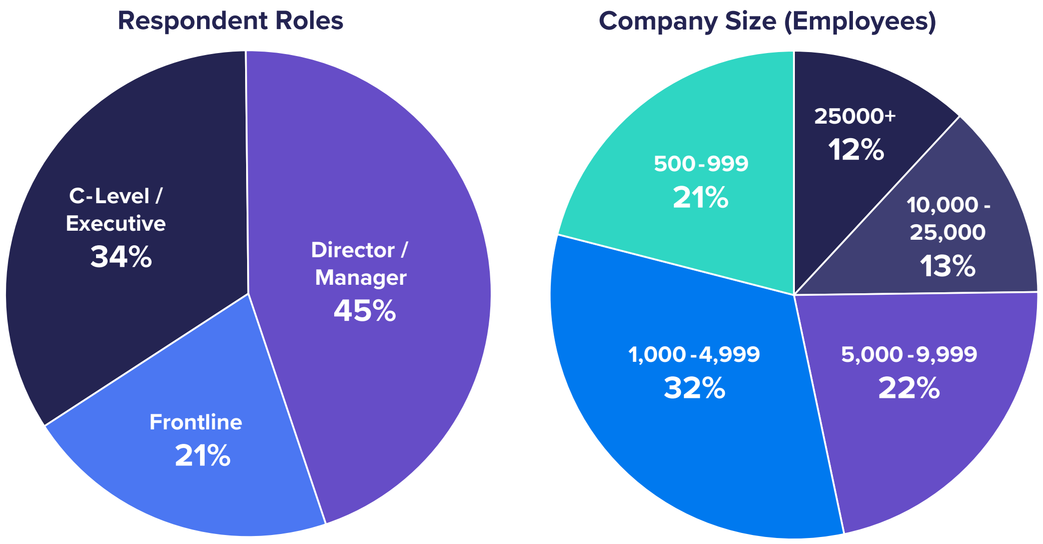
The margin of error for this research study is 5%, using a standard 95% confidence level.

To further ensure data reliability, CyberRes and our survey distribution partner applied many survey best practices including:

- Randomized available survey responses, where appropriate, to avoid bias
- Eliminated responses from people who were going through the survey too quickly
- Eliminated responses from people who provided contradicting answers to “filter” questions
- Eliminated incomplete survey responses
- Included “Don’t Know” responses where appropriate so respondents did not feel a need to “guess”
- Eliminated responses from people who did not match the survey’s target audience (in terms of job role, company size, involvement in decision making, etc.)

Demographics

The 2021 State of Security Operations survey gathered responses from 520 respondents across seven different countries, varying company sizes, and 16+ different industries. By design, respondents were all from companies with 500+ employees, and were all at least moderately involved in decision making for security operations at their organizations, with 8% reporting they were moderately involved, 28% reporting that they were very involved, and 64% reporting that they were extremely involved.


Respondent Roles

Company Size (Employees)

Figure 4. Key demographics of survey respondents

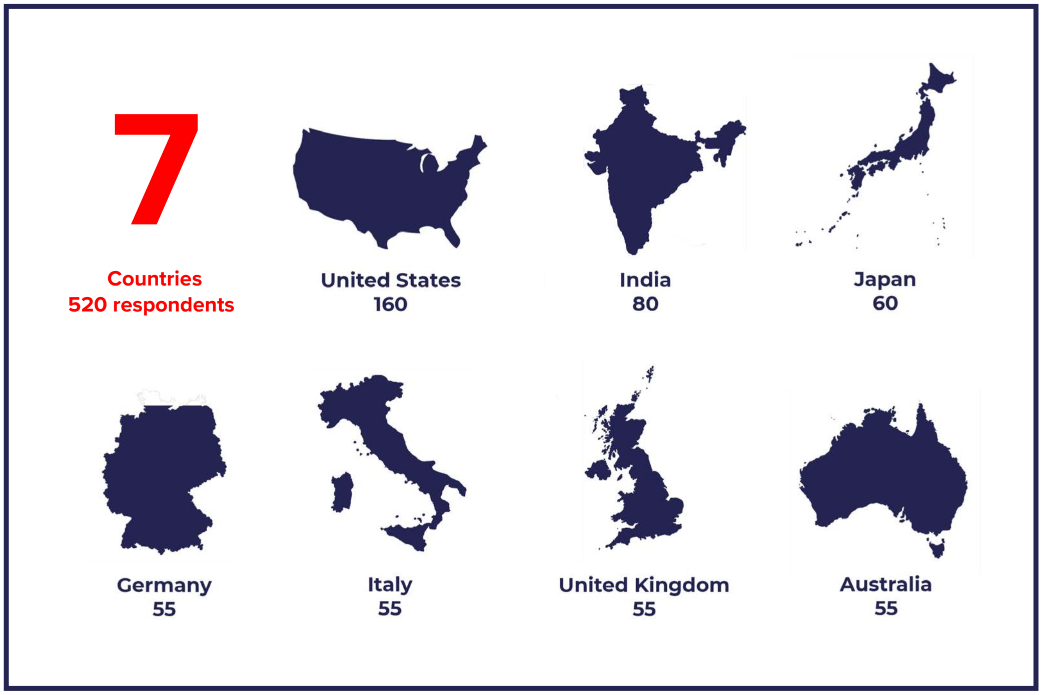


Figure 5. Respondent countries, and number of respondents from each country

Respondents represented the following industries: Airlines & Aerospace (including Defense), Automotive, Business Support & Logistics, Construction Machinery & Homes, Education, Entertainment & Leisure, Finance & Financial Services, Food & Beverages, Government, Health Care & Pharmaceuticals, Insurance, Manufacturing, Retail & Consumer Durables, Technology & Electronics, Telecommunications & Internet, Utilities/Energy & Extraction, and more.

About CyberRes

CyberRes is a Micro Focus line of business. We bring the expertise of one of the world's largest security portfolios to help our customers navigate the changing threat landscape by building both cyber and business resiliency within their teams and organizations. CyberRes is part of a larger set of digital transformation solutions that fight adverse conditions so businesses can continue to run today, keep the lights on, and transform to grow and take advantage of tomorrow's opportunities.

Section 1: Business Impact

Businesses faced significant change and hurdles in the past year, and that trend is still continuing today. The ability of a security operations team to protect against attacks and gain visibility into threats could mean the difference between an organization that can stay resiliently focused on its day-to-day operations, and an organization whose resources are squandered by a costly security breach. Not investing enough and experiencing a breach can create huge negative impact. Investing in the right security and focusing on smart processes can protect the business and reduce risk, while efficiently and effectively leveraging budget.

The 2021 State of Security Operations survey found that companies faced a dramatically changing landscape that impacted their business in a myriad of ways. Respondents reported that their organizations are now at a point where they, on average, have nearly two thirds of their security operations software and services deployed in the cloud. Additionally, nearly 70% had to expand their Bring Your Own Device (BYOD) policies in order to adapt to the sudden rise in remote work, and the insufficient supply of company-issued devices to support that remote work. Each change had a big impact on the attack surface, as we'll cover more below. But these are just two examples of the major changes SecOps teams have experienced in the past year.

C-Level Insight: Remote Work and Behavioral Analytics

"Identity and access control has proven to be remarkably resilient for monitoring and analytics, despite the shift from working in the office to working remote. The applications used by employees remained relatively static and independent of worker location. Investments in the monitoring and detection of behavioral anomalies on application access data will continue to bear fruit as every company goes through their pandemic and post-pandemic journey."

—Stephan Jou, CTO Security Analytics, Interset, CyberRes

Security Deployment and Investment Accelerated Due to COVID-19

How has the COVID-19 pandemic changed the way security operations is run at your organization?

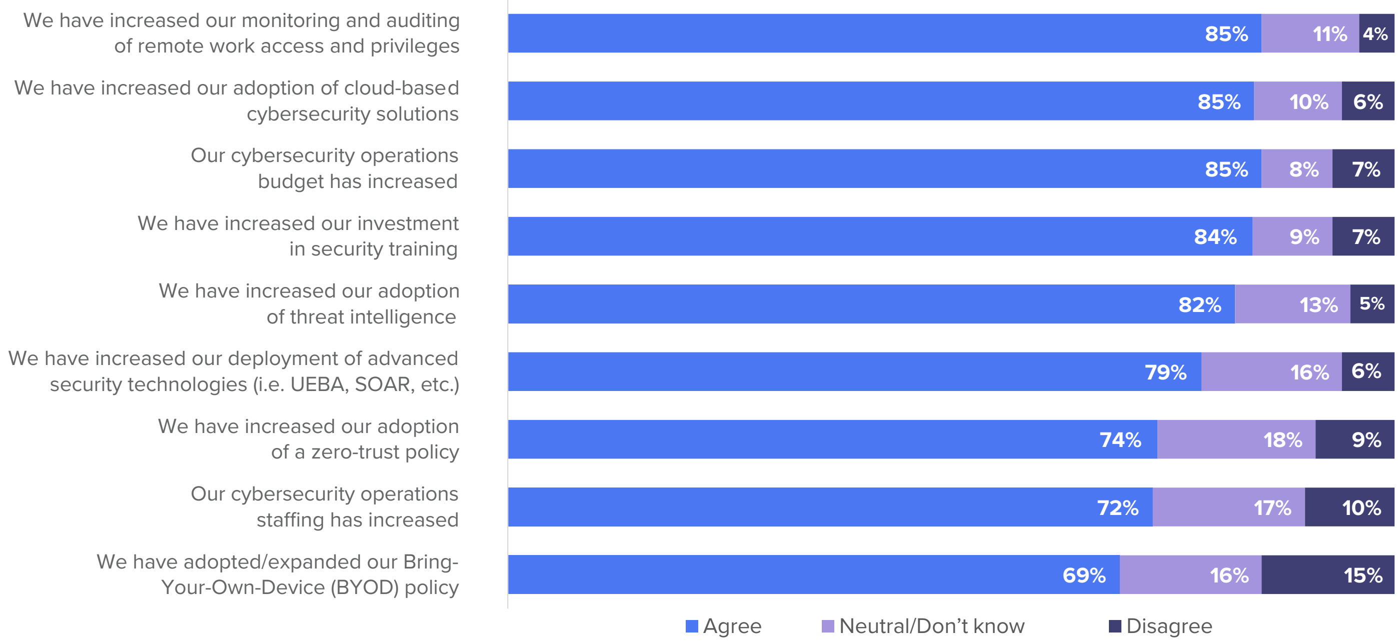


Chart 1. COVID-19's effect on security operations

Initially, businesses expected the pandemic to lead to an economic recession that would affect all of their functional units. According to a survey by McKinsey & Company conducted early in the pandemic, more than 70% of leaders predicted a decline in their security budgets for the year.[6] In reality, our data suggests that budgets grew during the period, driven by a widespread need to continue doing business in a rapidly shifting IT environment.

According to our survey, 85% of respondents say their companies increased their security budgets, with the same percentage saying that their company also increased monitoring and auditing of remote workers' privileges. The shift to a distributed workforce meant that security could no longer focus solely on the perimeter. It had to focus on granular access controls, device and user identities, and behavioral anomaly detection as well. Little surprise then that approximately the same share of companies—85%—increased their adoption of cloud-security services and technologies.

Another top change was that 84% of companies increased their investment in security training. With all the drastic changes to the IT environment during COVID, and the simultaneous rise in cyberthreats (especially phishing) across the globe, companies took the time to train their existing security staff and increase security training for employees. More than half of cybersecurity workers say that their organizations are at risk because of a lack of trained cybersecurity staff, with expertise in cloud-computing security as the skillset most in demand.[7] More than a quarter of organizations (28%) reach out to other departments to find potential cybersecurity recruits.[8]

For the most part, these changes are all positive. Security initiatives have evolved with the increased adoption of both BYOD and zero-trust policies, along with increased staffing efforts, increased adoption of advanced security technologies, and increased adoption of threat intelligence. Moreover, the pandemic underscored that security operations' goal should be to empower the business. Security teams could not just say 'no' to employees working remotely—they had to help employees working from home so they could be both secure and productive. At the same time, security teams also had to evolve to match the times and make remote security operations work efficiently, raising the specter that the days of in-person security operations centers (SOCs) may begin to wane.

C-Level Insight: Are the Days of the In-House SOC Waning?

"Dedicated, in-house SOC facilities are designed for maximum productivity and comfort, for both analysts and engineers. And depending on how many bells and whistles these command hubs contain, they often present a 'wow factor' for touring prospects and customers. However, the impact of COVID-19 has forced many SecOps teams to do their threat detection and response in completely remote settings. As the months have passed, SecOps leadership have been learning that virtually everything they do can be accomplished remotely and are finding it easier to retain skilled resources now that working remote is acceptable. So, are the days of the in-person SOC waning? I think the answer may be: 'Yes'."

—Stan Wisseman, Chief Security Strategist for North America, Micro Focus. Former CISO

Top Challenges of the Year

Companies faced many security challenges in the past year with the abrupt arrival of the COVID-19 pandemic. With remote work came a growing attack surface and a greater need for the cloud, so it's little surprise that the top challenges for respondents were monitoring the security of an increasingly distributed workforce and infrastructure, and expanding workloads to the cloud. We should note that, while the coronavirus pandemic accelerated the move to the cloud—and the attendant worries of monitoring that vast attack surface—the challenge of a growing attack surface had begun much earlier with the ever-expanding use of Internet-of-Things (IoT) devices, bring-your-own-device (BYOD) policies, and a progressive adoption of cloud technologies.

[6] Anant, Venky et al. "COVID-19 crisis shifts cybersecurity priorities and budgets." McKinsey & Co. Blog Post. 21 July 2020.
[7] "Cybersecurity Workforce Study 2020." (ISC)2. Whitepaper. p 15. 11 November 2020.
[8] "Cybersecurity Workforce Study 2020." p 26.

Which of the below do you consider to be the top challenges facing your cybersecurity operations team in 2021? Select up to three.

	Global	Australia	Germany	India	Italy	Japan	United Kingdom	United States
Monitoring security across a growing attack surface	40%	49%	36%	46%	49%	40%	38%	32%
Expanding workloads to cloud/hybrid environments	37%	36%	36%	46%	29%	20%	40%	40%
Pre-emptively detecting threats to reduce exposure	32%	31%	49%	24%	42%	30%	35%	27%
Investigating / validating / prioritizing security incidents	32%	36%	27%	25%	38%	32%	36%	31%
Taking advantage of cyber-security threat intelligence	30%	24%	20%	26%	29%	32%	27%	37%
Lacking skilled security operations personnel	29%	27%	26%	23%	36%	45%	27%	26%
Finding time for strategy and process improvement	29%	26%	29%	33%	24%	20%	27%	33%
Keeping up with the volume of alerts (“alert fatigue”)	26%	29%	16%	31%	22%	28%	20%	27%
Having too many unintegrated point solutions	24%	22%	31%	28%	15%	17%	26%	25%
Doing too many processes manually	21%	20%	29%	15%	16%	27%	24%	21%

Chart 2. Top SecOps challenges in 2021

Another top challenge (at 32%) was pre-emptive threat detection. As security operations centers (SOCs) continue to mature, they are advancing their objectives and making more concerted efforts to stop threats before they can cause damage, rather than simply detecting and responding to threats retroactively.

Roughly 32% of respondents also said that their cybersecurity operations teams were concerned with their struggles in investigating and prioritizing security incidents, selecting that as one of their top challenges for the year. And not far behind this was “taking advantage of threat intelligence”, which nearly 30% of respondents reported as a top challenge.

Another interesting insight comes from the opposite end of the results spectrum: for years now, a significant proportion of companies have been pursuing increased automation within their SOCs. According to this survey, “doing too many processes manually” was the least-selected top challenge for security operations teams, suggesting that a fair number of organizations have already been able to address this issue through automation and other means.

Differences in Top Challenges by Country and Industry

Respondents in different countries faced different challenges. Companies in the United States and the United Kingdom worried most about the speed with which they were deploying infrastructure and workloads into the cloud, while businesses in Australia and Italy were most concerned with monitoring security across their growing remote and cloud infrastructure.

C-Level Insight: Optimize and Simplify

“In a post-COVID era, many CISOs and security organizations are re-examining their strategies, looking for ways to optimize and reduce complexity. The majority of SOCs manage responses from multiple consoles, being fed by a vast portfolio of disconnected tools, collecting information from an expanding threat surface. CISOs are realizing that ‘more tools’ doesn’t necessarily mean ‘more security’. It’s about consolidation, rationalization, simplification, and automation.”

—Jim Foote, Global Chief Security Technologist, Micro Focus. Former CISO and CSO

Companies in India considered these two challenges equally problematic, with 46% of respondents listing each as a top challenge. Finally, Japan's top challenge seems to be a lack of skilled talent (45%), while Germany appears to be struggling the most with pre-emptive threat detection (49%).

Section 2: Technology

Technology and tools are critical to the success of security operations centers (SOCs). A survey of 4,800 IT security and privacy professionals found that two security practices—a proactive refresh of technology and a well-integrated technology stack—most significantly correlated with successful security outcomes.[9]

Security practitioners need to modernize their SOCs with solutions that enable them to address both established and contemporary threats that could impact operational resiliency. But modernizing the SOC doesn't mean implementing every new technology that comes along. Security professionals must stay aware of attackers' tactics, how they are evolving, and what security tools and features are needed to keep up.

Adoption of Security Technologies

The vast majority of organizations increased their adoption of advanced security technologies during the coronavirus pandemic, with 79% of respondents agreeing or strongly agreeing that their company increased deployment in the past year—unsurprising, since 85% of respondents also agreed that their security budgets had increased.

Which of the following security operations technologies are currently in use or planned for acquisition (within 12 months) by your organization?

	Currently in use	Planned for acquisition	No plans
Security information and event management (SIEM)	71%	24%	5%
Log management	69%	23%	7%
Advanced Signals Analysis (i.e. Network Traffic Analysis)	61%	31%	7%
Security orchestration, automation and response (SOAR)	61%	29%	8%
Advanced Threat Hunting Technologies	57%	34%	8%
Threat Intelligence Workbench, TIPS and/or CTX	53%	34%	11%
Attack Surface Management (i.e. EDR and ETDR)	52%	37%	11%
User and Entity Behavior Analytics (UEBA)	51%	36%	11%
Dynamic Malcode Analysis	49%	36%	12%
Unified Security Data Lake	48%	39%	11%
Pen Testing / Red Teaming Tools	44%	39%	15%
Advanced Shellcode Analysis	42%	38%	17%

Chart 3. Adoption of security technologies

C-Level Insight: The Key to a Successful Data Lake

"As a fan of analytics, AI, and ML, I am pleased to see a consolidated effort across the survey respondents to have a unified security data lake. Key to a successful data lake is not only consolidating the data, but also normalizing it. Do your best to clean the data as it enters the lake: examples include a consistent naming convention for users, servers and endpoints, and making sure timestamps are all in the same time zone. Ensuring your data lake is as clean as possible will pay huge dividends when you report and analyze that data later on. There is no analytics strategy without a data strategy."

—Stephan Jou, CTO Security Analytics, Interset, CyberRes

[9] "The 2021 Security Outcomes Study." Cisco. Whitepaper. 1 December 2020. p 12.

The adoption of security technologies is led by a set of solutions that are critical to security operations: security information and event management (SIEM), log management, and network traffic analysis systems. More recent supplementary technologies for holistic security efforts come next: security orchestration, automation and response (SOAR), user and entity behavior analytics (UEBA), threat intelligence solutions, advanced threat hunting, and attack surface management (ASM). These five solutions range in adoption, from a low of 51% of respondents to a high of 61%.

On the bottom rungs of the adoption ladder are those technologies that typically require a mature security operations team or a skilled application-security team. Cutting-edge technologies such as dynamic malcode analysis and advanced shellcode analysis—as well as a couple of highly-useful but perhaps undervalued technologies such as unified security data lakes and penetration-testing / red-teaming tools—were all adopted by less than half of respondents' companies. Yet, those technologies also have the highest likelihood of being acquired in the next year, with each expected to reach 80% adoption if security teams are able to execute on their plans. Of particular interest are those solutions considered to be "Gen 5 SOC" technologies, such as signals, shellcode, and dynamic malware analysis, as well as ASM. These tools are designed to address modern adversaries and threat actors, and are expecting 36% of respondents, on average, to adopt them over the next year.

While this year's survey looked at a different population than the 2020 State of Security Operations Report,[10] our current research suggests an increase in the adoption of SIEM (5%), SOAR (5%) and Log Management (10%). These solutions are fundamental to SecOps, suggesting that more companies are beginning to tackle security operations, or perhaps that some companies with existing security operations teams are just now beginning to realize the value of these core solutions.

Digging deeper into this year's survey, we found that companies with less than 1,000 employees were less likely to have implemented a SIEM solution. Just over half of these small companies had a SIEM, compared to about three-quarters of those companies with more than 1,000 employees. This provides further evidence that larger companies see SIEM as foundational to a true security operations center and have taken the steps necessary to implement it. Small companies were also much less likely—only 35%—to have more advanced capabilities, such as red teaming / penetration testing tools, compared to larger companies. Mid-size companies (up to 10,000 employees) had such capabilities in 43% of cases, while 55% of large companies (more than 10,000 employees) had adopted them.

Technology adoption also varied by country, with Japan and Italy in particular showing higher adoption of various technologies. Japan leads in the adoption of a unified security data lake (63%), red teaming tools (58%), and threat intelligence solutions (64%). Italy leads in advanced shellcode analysis (60%), advanced threat hunting solutions (69%), and dynamic malcode analysis (64%).

C-Level Insight: Taking a Holistic Approach to Analytics

"Don't ignore SIEM's role in your analytics strategy. AI/ML is best thought of as an automation and detection tool for use cases that would be difficult-to-impossible for humans to do alone. This includes use cases like advanced attacks and insider threats, as the data patterns detectable by AI/ML are voluminous and subtle, vary between user-to-user and endpoint-to-endpoint, and are not easily representable via standard SIEM rules or policies. That said, AI/ML alone is not a replacement for SIEM technologies, which are great at capturing 'known threats', and are very efficient at standard detections. A holistic approach is required."

—Stephan Jou, CTO Security Analytics, Interset, CyberRes

[10] "2020 State of Security Operations" CyberEdge, sponsored by Micro Focus. Research report. 19 October 2020. p 6.

Threat Intelligence

Security operations teams are the primary consumers, and producers, of threat intelligence. While definitions of threat intelligence vary, the SANS Institute defines cyber threat intelligence (CTI) as "analyzing information about threats and producing guidance to determine what steps must be taken in response to those threats."[11] Threat intelligence can range from large reports on specific adversary groups to indicators of compromise that are machine-readable and consumable. Machine-readable threat intelligence often follows certain standards, such as Structured Threat Information Expression (STIX) format or the YARA language,[12] while communicating such information is often done through services supporting the Trusted Automated Exchange of Intelligence Information (TAXII).

What would you say is the highest priority area of investment for Threat Intelligence at your organization?

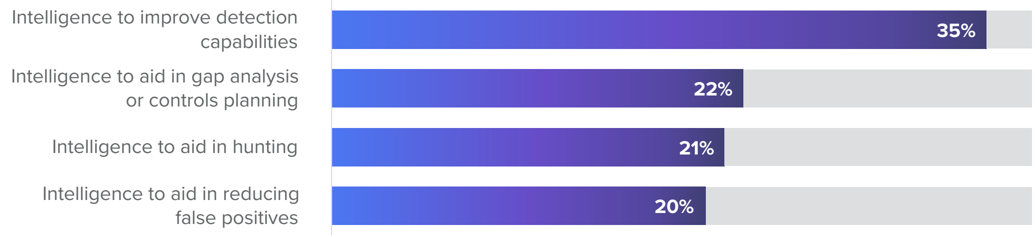


Chart 4. Priority objectives for Threat Intelligence

The majority of companies use threat intelligence to some extent, but the reasons vary. By far, the largest share of respondents (35%) prioritize the use of threat intelligence to improve threat detection, while the remaining companies are split fairly equally in prioritizing the use of threat intelligence to detect defensive gaps in controls, aid in threat hunting, and reduce false positives.

Which of the following are your highest priority areas of investment for intelligence over the next two years? Select up to three.

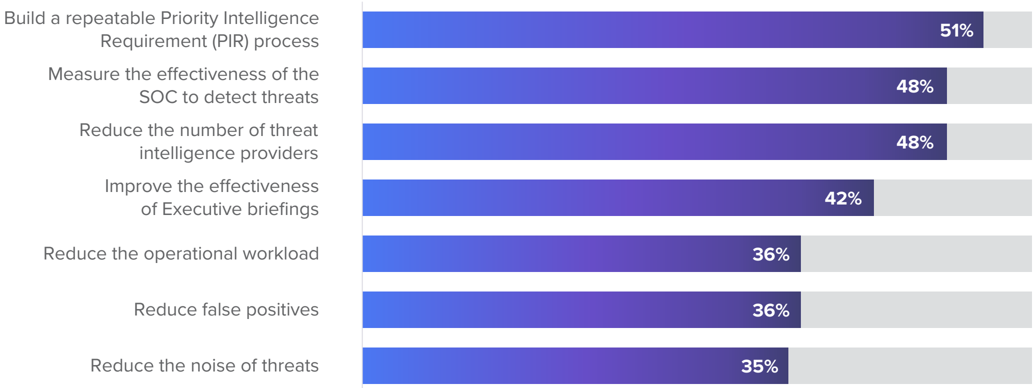


Chart 5. Priority Threat Intelligence investments

C-Level Insight: Instill the C-Suite and Board with Confidence

"An integrated threat intelligence program is necessary for protecting, detecting, responding, and recovering from current and active threats. One of the more subtle benefits of a threat intelligence program is the confidence it reinforces with the Board/C-Suite, when they inevitably email the CISO saying 'Hey, I got a news alert today about this current threat...' and the CISO is able to respond 'We've been aware of it for a week, and here is what we've done.'"

—Jim Foote, Global Chief Security Technologist, Micro Focus. Former CISO and CSO

[11] Lee, Robert M. "2020 SANS Cyber Threat Intelligence (CTI) Survey." SANS Institute. p 4. February 2020.`

[12] YARA stands for Yet Another Ridiculous Acronym, a less than descriptive name for what is essentially a way of communicating malware and exploit indicators.

Businesses are investing in threat-intelligence tools, with an aim to create order from the chaos caused by having too many threat intelligence providers, a lack of repeatable processes, and various other issues. More than half of those surveyed (51%) aim to invest in building a repeatable process backed by priority intelligence requirements (PIRs), which are a list of requirements that security groups need to do their job. A little less than half of companies ranked "measure the effectiveness of the SOC to detect threats" as a top-three priority for investment in threat intelligence, while a similar amount aim to reduce the number of threat intelligence providers used within their SOCs.

What are the highest priority intelligence-technology investments you plan to deploy over the next two years? Select up to three.

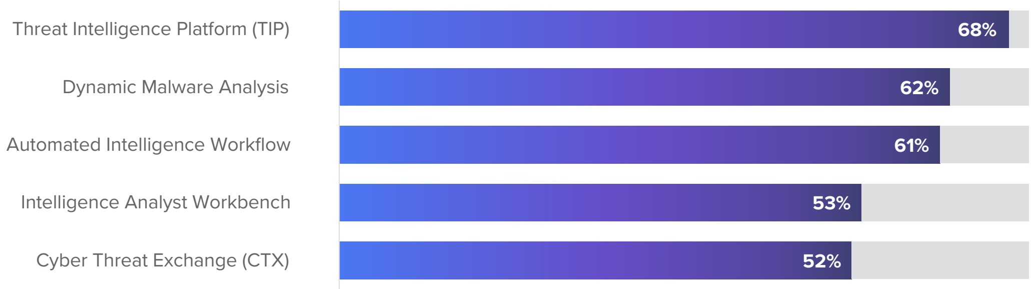


Chart 6. Priority Threat Intelligence technology investments

Companies have shared some of their specific goals for threat-intelligence investments. When asked about their top three priority investments in this area over the next two years, more than two-thirds indicated that they plan to invest in a threat-intelligence platform, while 62% plan to purchase the capability to analyze malware dynamically. Finally, about 61% will invest in tools to automate the intelligence workflow.

Role of AI/ML in Security Operations

Machine-learning (ML) and artificial intelligence (AI) technologies can automate the processing, filtering, and synthesis of data, and have been increasingly integrated into security tools. Most companies see these techniques as valuable, although in some cases they can be overhyped.

In cybersecurity, businesses have prioritized using AI/ML techniques to improve the detection of advanced threats—unsurprising, since the primary reason for adopting threat intelligence appears to be driven by the same goal. Nearly 60% of respondents placed this goal in their top-three primary roles for automation, ML, and cognitive security. The second and third most-selected roles were: improving the detection of data loss and exfiltration, and improving the detection of insider threats.

C-Level Insight: Any Threat Intelligence Is Better than None

"For the reduction of false positives, having any threat intelligence provider is better than no threat intelligence provider. There have been studies that show surprisingly little overlap between the various threat intelligence vendors, so I would recommend not overthinking this if you don't already have a provider."

—Stephan Jou, CTO Security Analytics, Interset, CyberRes

C-Level Insight: Preemptive Detection with Threat Intelligence

"Over the years, our SOC has seen the growing need to leverage the threat intelligence produced by the cybersecurity community. Having preemptive detection techniques, and then acting promptly, has become part of the DNA at our SOC, and we have deployed not only technology but processes and procedures to be able to identify, detect, protect, and respond as quickly as possible."

—Ramsés Gallego, International CTO, CyberRes

What are the primary roles you see automation, machine learning, and cognitive security technologies (e.g. deep learning) playing in your cyber operations? Select up to three.

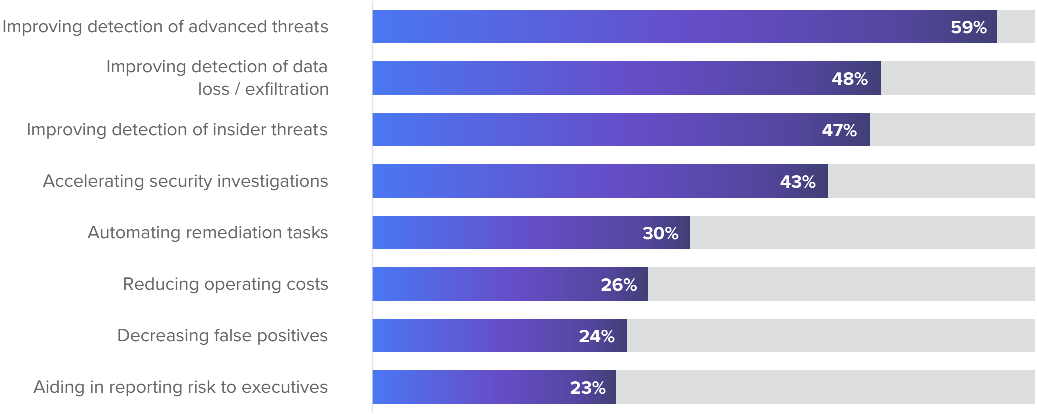


Chart 7. Roles of automation, machine learning and cognitive technologies

With the massive shift to remote work in the last year, the focus on insider threats has increased significantly. As employees began working from home and adapting to a new way of life, their schedules, workplaces, and overall behavior increased in flexibility and unpredictability. This has made technologies like behavioral analytics, backed by unsupervised machine learning, increasingly important as SOCs seek to maintain cyber resilience during periods of significant change. The ability to continually establish and update the baseline behavior of users and entities allows security teams to better monitor, understand, and secure their organizations and remote workforce.

Companies continue to struggle with the fear that they may be missing signs of an attack, especially when faced with the reality that attackers are slipping past too many of the security measures that have already been put in place. Digging into our data we found that the manufacturing sector, for example, marked data exfiltration and insider threats as higher concerns, likely because there is a greater risk within that sector of employees stealing and selling their company's prized intellectual property.

The Essential Cloud

Companies continue to face challenges with pushing workloads into the cloud. As noted in the Business Impact section, increasing cloud adoption was the second most significant security challenge facing respondents, after the challenge of monitoring a growing attack surface. Almost all security operations teams are worried about cloud security, with 96% professing to be "moderately concerned" about the security of public cloud, nearly two-thirds worried about data loss, 62% concerned about data privacy, and nearly half (46%) worried about workers accidentally exposing credentials.[13]

C-Level Insight: Look into Unsupervised Machine Learning

"One way we've found to amplify the reach and capabilities of our cyber analysts is by using unsupervised machine learning, which learns by observation rather than by example, allowing us to confidently detect anomalies and abnormal behaviour in our network. We find it critical to nurture the skills of our people, but we also find that those skills are completed and complemented by advanced technologies that expand the team's visibility. This allows them to focus on value-added tasks and on executing the right response, while solutions enhance our detection."

—Ramsés Gallego, International CTO, CyberRes

[13] Cybersecurity Insiders. "2021 Cloud Security Report." (ISC)2. Whitepaper. p 2. 20 June 2021.

That said, our research suggests that 85% of organizations have increased their adoption of cloud-based security solutions (also noted in the Business Impact section). Practically all organizations (99%) now have at least some part of their security operations solutions deployed in the cloud, and a notable 90% have at least one third of their security operations deployed in the cloud.

While these results may not come as a surprise to some people, it should be critically apparent to all that the cloud is essential to security operations, with most organizations (95%) taking a hybrid approach. Only 1% of organizations still have their security operations fully on premises, while only 4% are fully deployed in the cloud. Organizations should determine which of their solutions and workflows would be better run from the cloud and which would be better managed on premises.

Respondents shared that, on average, their organizations now deploy almost two-thirds (64%) of their security operations infrastructure in the cloud. In a country-by-country comparison, we find that Australia has shown the highest adoption of cloud-based security (69%), while Italy is on the opposite end of the spectrum (47%).

C-Level Insight: Integrating SecOps with Cloud-Native Tools

"SOC security processes are being integrated with cloud-native tools to drive visibility, detection and response. I expect this will increase to help to keep costs in check, remain agile, and obtain faster time to value, especially as workloads continue to shift to the cloud."

—Stan Wisseman, Chief Security Strategist for North America, Micro Focus. Former CISO

Approximately what percentage of your organization's cybersecurity operations software and services are presently deployed in the cloud?

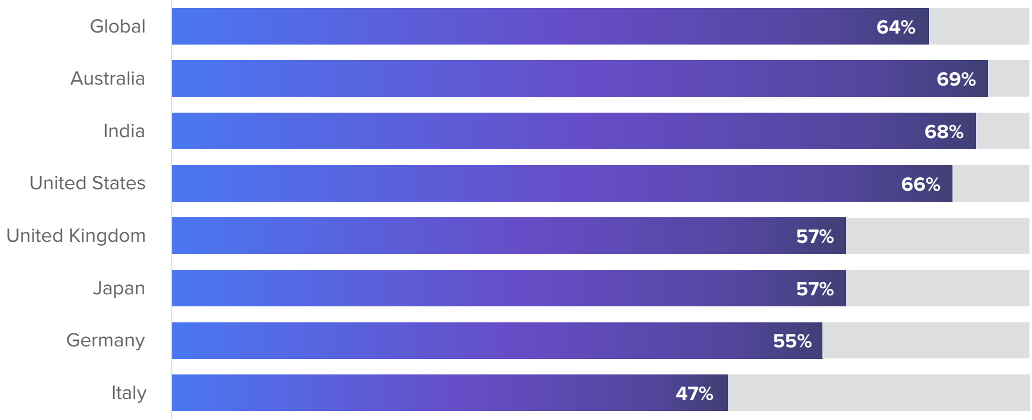


Chart 8. Percentage of security operations solutions deployed in the cloud, averaged across companies

While the pandemic has forced many companies to accelerate their plans to move to the cloud, companies are still facing several challenges. As noted by Cybersecurity Insiders, a lack of staff or expertise is holding back 39% of companies, while the risk of data loss is holding back 34%. Legal and compliance concerns are prompting 32% to reconsider a particular cloud move.[14]

[14] Cybersecurity Insiders. "2021 Cloud Security Report." p 7.

Digital Twins in Security Operations

Automated attack simulations became a component of cybersecurity more than two decades ago. Simulated attacks can be used to find vulnerabilities, verify patched assets, and model threats. A simulation that uses actual staged or production applications, however, can have unwanted impacts on a company's operations and development cycle.

Enter the concept of the digital twin. Originally, academics and engineers embraced the concept of simulated "mirror worlds" more than three decades ago,[15] recognizing a need for the pervasive simulation of products in the manufacturing and scientific world. This concept evolved into the "digital twin," a virtual representation of a real-world asset that can be used in simulations. In 2010, NASA revealed its intention to, by 2025, develop digital twins for simulations that model spacecraft and find unwanted interactions between physical systems prior to manufacture.[17] Software development and cybersecurity have begun to adopt more reliability and production concepts from manufacturing. Among them, simulating interactions between assets using digital twins. In 2018, Gartner named "digital twins" as a Top-10 Strategic Technology Trend,[17] vaulting the concept further into cybersecurity methodology.

In the 2021 State of Security Operations survey, we defined a digital twin as "a dynamic virtual replica of a physical environment or system, that uses sensor-based data to conduct real-world modelling and simulations." A number of technologies can be associated with incorporating digital twins and simulations into the security operations center (SOC). We asked respondents which of the following technologies they had adopted or were planning to adopt in a digital twin environment.

Which of the following SOC Digital Twin technologies have you adopted or are planning to adopt in the next two years?

	Currently in use	Planning to adopt	No plans
Security orchestration, automation and response (SOAR)	55%	37%	7%
Automated threat intelligence platform(s)	52%	39%	8%
Automated retrospective threat hunting	49%	40%	9%
Machine-aided workload (Bots)	46%	39%	13%
Automated cognitive research engine(s)	45%	41%	12%
Automated ERM	44%	43%	11%
Robotic Process Automation (RPA)	41%	43%	14%

Chart 9. Adoption of SOC Digital Twin technologies

[15] "Siemens and General Electric gear up for the internet of things." The Economist. Online Article. 3 December 2016.

[16] Shafto, Mike et al. "DRAFT Modeling, Simulation, Information, Technology & Processing Roadmap—Technology Area 11." National Aeronautics and Space Administration. Draft PDF Report. November 2010. p TA11-5.

[17] "Gartner Identifies the Top 10 Strategic Technology Trends for 2019." Gartner. Press Release. 15 October 2018.

Previously in this report, we remarked on the significant strides in the adoption of SOAR, automated threat intelligence, and automated retrospective threat hunting. But we can now see that nearly all automation technologies are expected to see over 85% adoption in the next two years, assuming that respondents are able to execute on their plans.

When asked about the role of SOC Digital Twin technologies within security operations, more than two-thirds of companies (68%) believed they would drive better instrumentation and performance metrics, with respondents placing that goal in their top-three choices, while 67% expected the technologies to improve analyst performance.

What roles do you see SOC Digital Twin technologies playing in security operations? Select up to three.

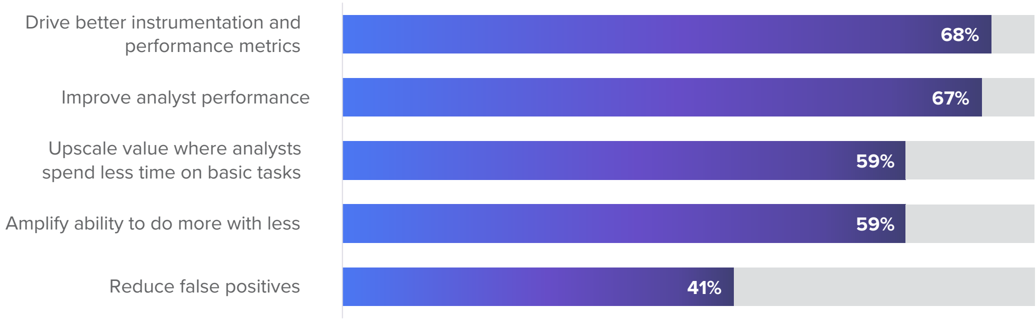


Chart 10. Role of SOC Digital Twin technologies

Cyber Range and Scenario Simulation

If digital twins are data representations of objects, cyber ranges are the virtual environment in which simulations using those objects are carried out. While such simulations are time consuming, they are necessary to get ahead of threats and adversaries, as well as to test out infrastructure to ensure that it can perform while under attack.

The concept has seemingly been embraced by companies worldwide. A plurality of companies—43%—have a cyber range and conduct readiness drills at a frequency dictated by risk management, with results tied to overall cyber-readiness reporting. By tying results to overall reporting, companies can regularly update their understanding of their security posture and adapt their threat modeling to match the actual threat level of certain types of attacks.

C-Level Insight: Cyber Range Simulations for Cyber Resilience

"Tabletop exercises have historically been fairly academic, scripted, and predictable, yet they still provide meaningful insights to security, IT, and business teams. Using a cyber range simulation is as close as you can get to an actual attack done in real time within a simulated environment. Leveraging a scenario-based cyber range simulation will be a critical next step in maturing a company's overall cyber resilience."

—Jim Foote, Global Chief Security Technologist, Micro Focus. Former CISO and CSO

C-Level Insight: Keeping Your Team Trained and Up-to-Date

"Our SOC has built a cathedral of protection upon a several key foundations including XDR, UEBA, cyber ranges, and keeping our team trained. Our SOC's monthly exercises and drills allow our team to be constantly trained on, and up-to-date with, techniques that help us to safeguard what matters most."

—Ramsés Gallego, International CTO, CyberRes

Do you have a cyber range, and conduct readiness drills at a frequency dictated by risk management, with results tied to overall board cyber-readiness reporting?

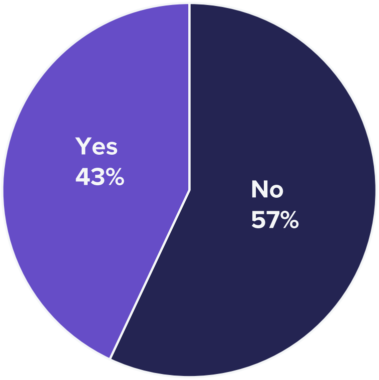


Chart 11. Cyber range use, readiness drills, and reporting

The adoption of cyber range technology and the commitment to readiness varies by country. Following the same frequency and reporting qualifiers mentioned above, India led the group in adoption and use of cyber ranges with 64% responding positively, while the United States followed with 53%, and Australia trailed with 47%. Next was the UK with 38%, Italy with 31% and Japan with 25%. Finally, Germany reported the lowest adoption and use of cyber ranges, with only 20% saying they conduct readiness drills with a cyber range at a frequency dictated by risk management, and with results reported to the board.

Section 3: People

Having the right security technologies and services is essential, but having the right people is the key to getting the most out of those assets. Unfortunately, acquiring knowledgeable security professionals continues to be a challenge. The United States, for example, has less than half of the necessary cybersecurity professionals that the market needs, estimated at about 370,000 workers.[18]

As a result, many companies do not have the skilled labor necessary to make the most of their security technologies and keep attackers at bay, while damaging attacks, such as ransomware, continue to grow exponentially. Large cities are particularly feeling the shortfall, with companies in New York, Baltimore, and Atlanta only able to hire about half the number of security professionals they need.[19]

[18] Saleh, Yustina et al. "Build (Don't Buy): A Skills-Based Strategy to Solve the Cybersecurity Talent Shortage." Emsi. PDF Report. July 2020. p 5.

[19] Saleh. "Build (Don't Buy): A Skills-Based Strategy to Solve the Cybersecurity Talent Shortage." p 5.

The Talent War Continues

While many of the world's businesses were forced to reduce their staff throughout 2020, security operations teams were actually able to increase their headcount. In the 2021 State of Security Operations survey, more than 72% of organizations indicated that their staffing had increased, with only 10% seeing a decline. Companies in the United States and India experienced the greatest increases, with 86% of organizations hiring more staff in both countries, while Japan and the United Kingdom faced the smallest gains of 37% and 62%, respectively.

Any gains in increased hiring, however, have been offset by greater staffing demands due to the year's growing number of cyberattacks, an expanding attack surface, and increased adoption of remote work. Attacks reported to the FBI more than tripled, while about two-thirds of workers in technology-focused industries began working from home, increasing the number of devices and locations that needed to be secured.[20] Most companies recognize the importance of retaining cybersecurity professionals, and so many workers were re-tasked during the pandemic to help out IT as the sudden shift to remote work caused chaos with business infrastructure. In fact, almost half of cybersecurity professionals were pulled from security duties to help out with IT.[21]

Which aspects of your cybersecurity operations would benefit the most from an increase in skilled staffing? Select your top three.

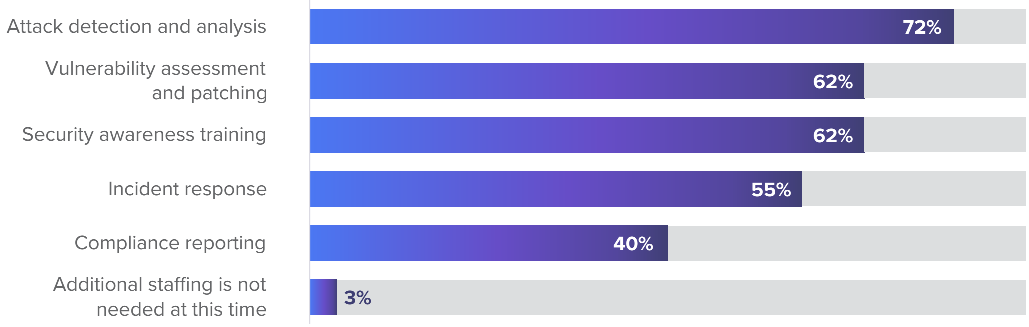


Chart 12. Areas in need of additional skilled staffing

As such, staffing continues to be a source of pain for companies. Among the challenges identified by the survey, almost 1 in every 10 organizations identified a lack of skilled cybersecurity staff as their biggest challenge in 2021, with nearly 30% listing it as a top-three issue. Only 3% of organizations reported that they do not need additional staffing at this time.

C-Level Insight: Grow Your Security Talent Internally

"As a former CSO, I have found it much quicker and more cost effective to grow security talent internally by cross-pollinating with the IT and product teams, than to try to acquire security talent off the streets. Many employees in technology roles aspire to pivot their skills into security but may leave their current company for an opportunity to make that move. Investing in training people beyond the security teams is good for security, for the company, and for the technical teams. It unlocks potential and may provide a career path for someone who is truly capable but is unsure of the pathway into security. It's a win/win."

—Jim Foote, Global Chief Security Technologist, Micro Focus. Former CISO and CSO

[20] Brandenburg, Rico and Mee, Paul. "Cybersecurity for a Remote Workforce." MIT Sloan Management Review. Article. 23 July 2020.

[21] "(ISC)^2 Survey Finds Cybersecurity Professionals Being Repurposed During COVID-19 Pandemic." (ISC)2. Press Release. 28 April 2020.

The lack of skilled staff is causing major problems for security operations, with 72% of companies concerned that this shortage is affecting their ability to detect and analyze attacks. 30% listed this area as the aspect of their security operations that would benefit the most from an increase in staffing. Companies were also concerned that the lack of staff had inhibited their ability to provide security awareness training, as well as conduct vulnerability assessments and patching.

Should We Outsource?

Given the disruption caused by the ongoing talent war, most companies have considered outsourcing at least some of their security operations. While outsourcing allows companies to gain access to needed experts and to free up staff, many organizations continue to view outsourcing with distrust, especially for their security operations. Our survey found that companies generally prefer managing their security operations in-house as opposed to outsourcing it. However, hybrid management is clearly the most popular route, with the vast majority of organizations outsourcing tasks to some degree.

Fairly consistently across security functions, about 33% to 40% of organizations fully manage a particular function in house, while 52% to 60% of organizations take a hybrid approach ranging from mostly in-house to mostly outsourced. On average, about 6% of companies fully outsource a particular security function.

Further exploring the data, we found that only 8% of organizations fully manage all 10 of our surveyed functions in-house, with organizations managing only 3 to 4 functions fully in-house on average, and the rest outsourced to some degree. At the other end of the spectrum, less than 1% of organizations fully outsource all 10 of the measured security functions. In fact, nearly three-quarters (73%) of organizations don't fully outsource any of the functions. The average number of functions fully outsourced, per company, is between 0 and 1.

Which of the following cybersecurity functions does your organization manage in -house and which do you outsource (via MSSP, SaaS, etc)?

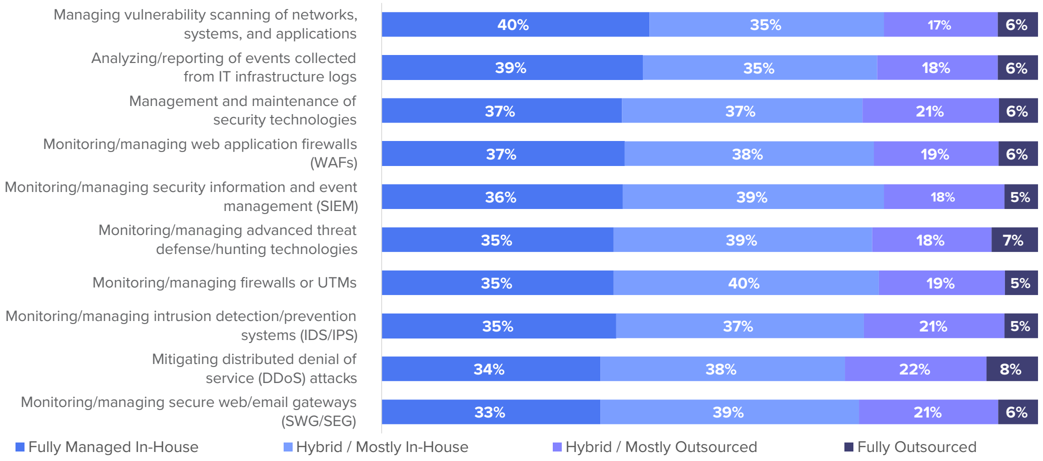


Chart 13. Distribution of SecOps function management (internal vs outsourced)

C-Level Insight: The Rising Need to Outsource

"For many organizations, growing SecOps complexities have made the cost of outsourcing SOC functions not only appealing but necessary. Many will first try to streamline and ease the internal operation, but once you add in the difficulty of sourcing top talent, it's easy to see why outsourcing often presents the path of least resistance. Most modern SOCs are hybrid SOCs… I expect we will continue to see growth in third-party outsourcing."

—Stan Wisseman, Chief Security Strategist for North America, Micro Focus. Former CISO

C-Level Insight: Consider a Blended Model

"'Outsource or in-source' is not an all-or-nothing proposition. Increasingly, CISOs are moving to a blended model, outsourcing low value things like system installation, configuration, maintenance, and upgrading to a partner. Others are moving to SaaS, which preserves their scarce, skilled resources to deliver against the primary mission: securing the company."

—Jim Foote, Global Chief Security Technologist, Micro Focus. Former CISO and CSO

However, the use of outsourcing to augment in-house processes with a hybrid approach is much more common. Nearly one in five companies (18%) outsource all 10 of their security functions to some extent.

This data from the survey suggests that, while some organizations are able to get by managing everything in-house and most are trying to keep at least the majority of their workload in-house, almost all companies (92%) are finding they need to outsource, at least partially, some of their SecOps functions. Yet, outsourcing hesitancy is still the rule: Only 24% have fully outsourced 1 to 3 security functions, and only 4% rely on more than three fully outsourced functions.

Automation Priorities

The shortfall in security workers can also be offset by adopting more automation as well as artificial-intelligence and machine-learning systems to reduce workloads. While only about half of companies have automated each of the particular security functions we surveyed, about 85% of companies will have adopted these individual functions in the next 12 months.

Which of the following automation activities are currently in place or planned for implementation within the next 12 months at your security organization?

	Currently implemented	Planning to implement	No plans
Automation of Risk Assessment	58%	33%	8%
Automation of Threat Hunting	53%	38%	7%
Automation of Intelligence Analysis	53%	38%	8%
Automation of Attack Surface Management	52%	40%	7%
Automation of Level 1 Triage	46%	39%	11%
Automation of Advanced Triage	45%	44%	10%

Chart 14. Implementation of automation activities

The priority for automation is risk assessment, followed by a near-tie between automation of threat hunting, intelligence analysis, and attack-surface management. There seems to be less focus on automation of triage, which is surprising since one of the most widely discussed reasons for security automation and AI is the replacement of Tier-1 analysts.

C-Level Insight: Combating the Growing Attack Surface

"The explosion of remote employees and external devices accessing organizations' networks and applications has led to a much larger attack surface. It's a serious issue when you consider how most organizations were already having a difficult time detecting and responding to cyber-attacks when they had fewer remote workers and on-site resources. SOC teams now have to prevent cyber threats for an infrastructure that has grown well beyond the confines of traditional security boundaries. That's why many are turning to machine learning to detect bad actors, and to automation to quickly neutralize threats."

—Stan Wisseman, Chief Security Strategist for North America, Micro Focus. Former CISO

Section 4: Processes

Establishing mature processes for handling security operations in a consistent and intelligent way is essential. Having an organized playbook and effective automation could mean the difference between a significant breach and a minor security incident. Nearly 30% of respondents considered “finding time for strategy and process improvement” to be a top challenge for their security operations teams, while 21% considered “doing too many processes manually” to be a top challenge. Clearly, security professionals see automation as an advantage and are seeking to implement it in a thoughtful way.

Evaluating Your Defenses

Arguably, the most important security operations process is the regular evaluation of defenses to ensure their effectiveness against current threats and to ensure that security controls continue to operate as expected. Simulation of defenses using a cyber range is covered in the Technology section of this report, but two other important components need to be discussed. Those components are: evaluating your company’s threat models, and using red-team exercises to evaluate defenses in real-world conditions.

The regular evaluation of threat models is important because threat models, like technologies, age quickly and can lose relevance. We asked respondents how often they evaluate their threat models for relevancy to business impact. Surprisingly, and to our relief, we found that most organizations (85%) are reporting that they evaluate their threat models at least once every six months. Nearly half, 44%, report that they continuously evaluate their threat models by linking them to threat intelligence.

How often are your security operations threat models evaluated for their relevance to business impact?

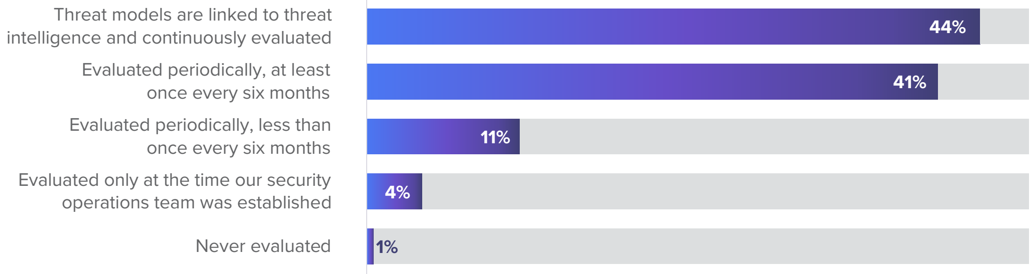


Chart 15. Frequency of threat model evaluation

Unfortunately, 11% of companies evaluate their threat models less frequently than every six months, and about 4% have not evaluated their models since their security operations teams were established. These organizations should refresh their threat models and establish a quarterly—or continuous—process to evaluate those models against current threats, to determine whether cybersecurity measures and security operations processes need to be updated.

C-Level Insight: Focus on Operational Efficiency

“Security is a journey, not an event. Security teams know this but often rely on audit or compliance programs to evaluate the effectiveness of their security programs. The problem is that these evaluations seldom touch on efficiency. It is as important to measure operational efficiency as it is effectiveness when building a culture of continuous improvement.”

—Jim Foote, Global Chief Security Technologist, Micro Focus. Former CISO and CSO

Similarly, we see a focus on evaluating defenses using human-centric exercises such as red teaming and penetration testing. About 72% of organizations are running exercises at least twice a year, and an additional 19% of organizations are at least conducting tests annually.

How often do you run independent red teaming exercises against your SOC?

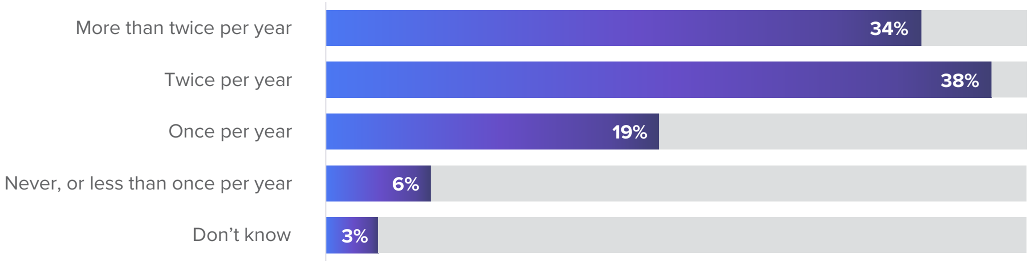


Chart 16. Frequency of red teaming exercises

However, about 6% only conduct such exercises less than once per year. These organizations should, at the very least, consider moving to an annual evaluation. An alternative approach would be to assess infrastructure components and security processes whenever there is a significant change in technology, process, or the threat landscape.

Forward-thinking security operations teams use red-team exercises to ensure a strong cybersecurity posture. More than 93% of those surveyed consider red teaming an essential activity for security operations. Almost half—44%—report their red-teaming results to the board for due diligence, while 33% share the results with the CISO as part of risk-and-readiness reporting. Finally, 16% of respondents do not share the results of their red teaming exercises with the CISO or the Board.

How essential is Red Teaming to the effectiveness of your organization's security operations center (SOC) readiness?

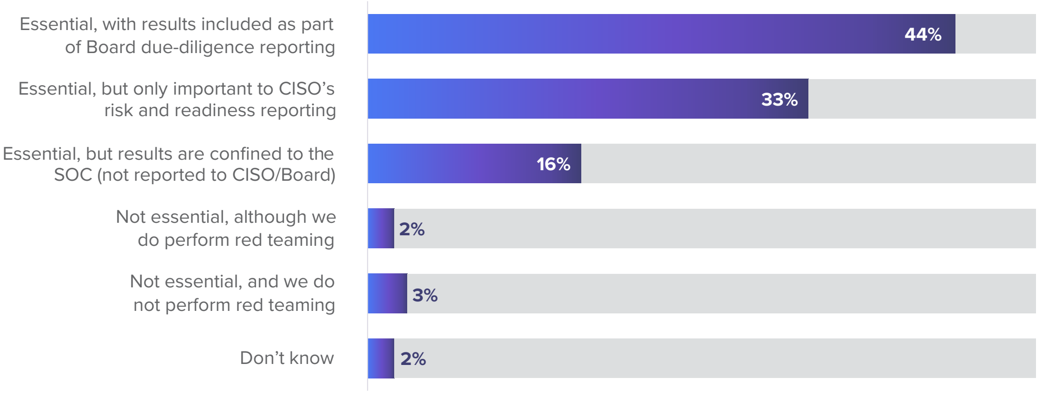


Chart 17. Importance, and reporting, of red teaming exercises

Automation Benefits for Security Processes

The benefit of any sort of automation is that the process is managed by the machine, reducing analyst workloads so they can focus on higher-value activities. About 30% of our surveyed SecOps decision-makers considered automating remediation tasks to be a top use case for automation, while almost a quarter (23%) considered automating the process of reporting risks to executives as a top use case. Furthermore, as you may recall from the Technology section, more than half of security professionals considered building a repeatable PIR process as a top priority for their intelligence-related investments over the next two years.

For most of the data, process generally ranks after capabilities in terms of importance, but security professionals do recognize that process is still critically important. Companies need to create and maintain efficient and effective processes to support their SOC analysts and to optimize the ROI of their security tools.

Threat-Modeling Frameworks

One area where an established process can improve security operations is in modeling threats. A formalized threat modeling framework, such as MITRE ATT&CK, can help organizations prepare for and respond to threats. We asked organizations what value they see in implementing a threat modeling framework. By far, most respondents use threat modeling frameworks to improve detection of advanced threats, which (as we have covered throughout this report) is very much a top-of-mind concern for SecOps decision makers.

Threat-modeling frameworks are also valued for their ability to identify gaps in security defenses, improve an organization's ability to remediate threats, and because they enable everyone to communicate about threats in a consistent way. Lower on the benefits list, but still chosen by at least 20% as a top-three benefit, were: improved training on how cyberattacks function, enhanced executive visibility into risk, increased understanding of cyber adversaries, and reduced overall threat exposure.

What do you view as the primary benefits of implementing a formalized threat modeling framework?

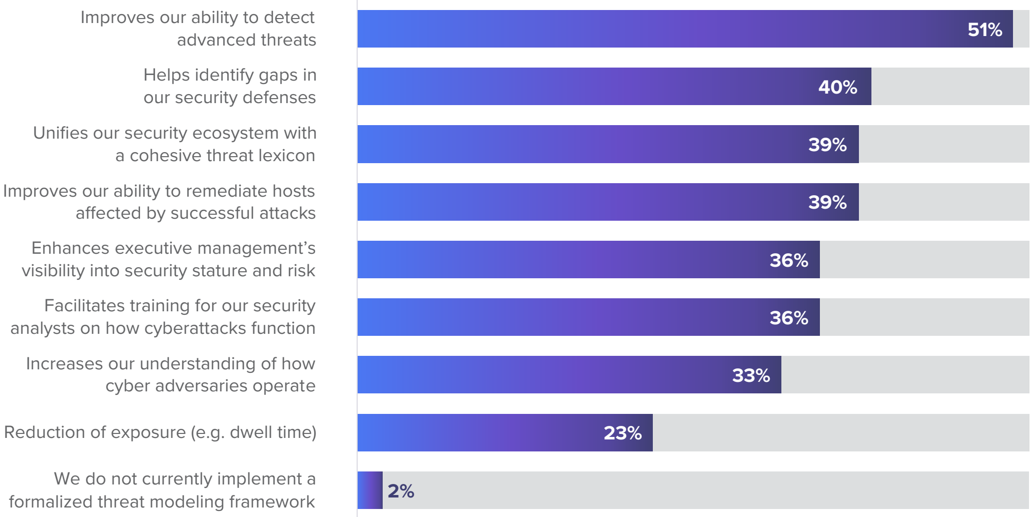


Chart 18. Benefits of implementing a threat modeling framework

Of the frameworks included in our survey, the one most frequently used by security organizations on a regular basis was the Cyber Kill Chain, a variant of the military's kill chain analysis technique, adapted by Lockheed Martin, with 44% adoption. Not far behind are several other popular frameworks, including the MITRE ATT&CK framework, used by 41% of organizations, and the STRIDE framework created by Microsoft, used by 40% of companies.

It is common for organizations to leverage multiple threat modeling frameworks across their security teams to maximize value. Roughly one-in-ten companies admitted to not using any of the referenced threat-modeling frameworks, or to not using any framework at all. Because most of the frameworks are open-source and can serve many functions, as shown earlier, we recommend that organizations look into implementing threat-modeling processes using at least one of the major frameworks listed.

What threat modeling frameworks does your security organization use on a regular basis?

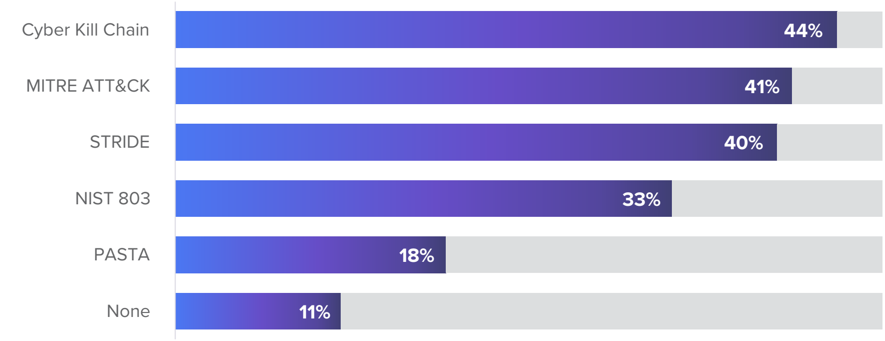


Chart 19. Usage of various popular threat modeling frameworks

C-Level Insight: Reduce Exposure with MITRE ATT&CK

"SOCs that are leveraging MITRE's ATT&CK framework, and products that integrate with its knowledge base, can reduce detection and exposure time to cyber threats. While the classic Lockheed Cyber Kill Chain still has value and continues to be broadly used, ATT&CK's list of techniques by tactics that doesn't propose a specific order of operations is more useful in the shift beyond traditional security to cyber resilience."

—Stan Wisseman, Chief Security Strategist for North America, Micro Focus. Former CISO

Attack Surface Management

Attack surface management (ASM) is the capability to discover, track, classify, and monitor assets in your network or used by your employees—from laptops to routers, and from software to cloud services. With 40% of companies considering the growing attack surface to be a major problem, finding technology and processes to reduce the footprint of your information technology and infrastructure is extremely important. Attack surface management (ASM) solutions are a relatively new technology, but more than half of respondents currently have such efforts in place within their organizations, and about another 40% intend to implement them in the next 12 months.

Attack Surface Management (ASM) tools attempt to find the weakest link under the assumption that "if you do not find it, the attacker will." From data discovery to hunting down rogue devices, to outdated software, attack surface management gives companies the peace-of-mind that a hardened system will not have a soft underbelly.

What do you consider the most applicable use case for the rollout of Attack Surface Management?

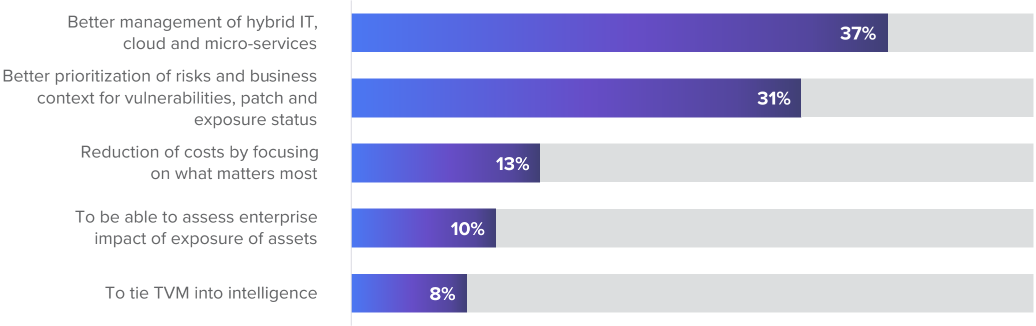


Chart 20. Use cases for Attack Surface Management

We asked respondents what they viewed as the most applicable use cases for the rollout of ASM. Results prioritized better management of hybrid IT, cloud and micro-services, aligning with what we've already seen in this report about cloud and remote work. Reduction of risks and reduction of costs ranked second and third, respectively, while less than 10% of companies gave priority to the use case of tying threat and vulnerability management (TVM) into intelligence. Interestingly, the results around this use case varied across certain countries. Not a single respondent from Japan considered the TVM use case to be a top application, while German respondents ranked it as their most relevant use case (26%). The next most-selected use case in Germany, with 24%, was the "management of hybrid IT, cloud, and micro-services" use case, which topped the list in all other countries.

C-Level Insight: Counter the Attack Surface with ATT&CK

"The attack surface has evolved and is always expanding. There are more threat actors using a variety of methods to grind our business to a halt. However, when our team is using the knowledge from MITRE ATT&CK, together with our SIEM solution, we are able to better recognize how we might be attacked, and we empower our professionals with insightful information on 'the hacking book'. Then, using the right SOAR technology, we are able to protect and defend our group of enterprises, both in a centralized and decentralized way."

—Ramsés Gallego, International CTO, CyberRes

Conclusions

Driven by the necessities of the pandemic, companies have moved to widespread implementation of remote work and a significant increase in the adoption of cloud infrastructure and services. As a result, security operations have evolved a great deal in the past year, testing the cyber resilience of SOCs around the globe. While many challenges have remained the same for security teams—such as the war for skilled security talent and a focus on advanced threats—other changes are a result of companies adapting to the year's unique circumstances. Among the most significant trends:

- As employees moved from the central office network to work from home, attack surface area and business risk increased.
- While business investment in technology declined during the year, investment in security—and especially cloud security—grew, defying early predictions.
- With more infrastructure in the cloud, companies increasingly need security solutions that support cloud monitoring. Organizations looking to expand their presence in the cloud should evaluate cloud-based security solutions to determine fit.

- Security operations centers (SOCs) continue to mature, by implementing foundational technologies and best practices while also looking to modernize their SOC by adopting more recent innovations.
- Threat modeling, attack surface management, and threat intelligence are increasingly influencing SecOps strategy and enabling informed approaches to defending business networks.

Given the volatile nature of the past 18 months, predicting the future may be a fool's errand, but barring another Black Swan event like the coronavirus pandemic, certain trends appear to be taking shape. While companies will bring people back to the office, remote work is here to stay and that requires certain changes to security operations. Here are the most likely trends:

- The number of knowledge workers working from home will double in the medium term, with about 51% working remotely by the end of 2021, up from 27% prior to the pandemic.[22]
- Companies need to secure their attack surface areas; more than half have not fully implemented security controls for their expansions in digital and cloud operations.[23]
- Until useful deterrence strategies are developed to dissuade cybercriminals in unreachable jurisdictions, companies will need to continue to focus on hardening every endpoint, pre-emptively detecting threats, and establishing a strong backup strategy to recover from ransomware.
- While the whiplash nature of the pandemic economy has resulted in a shrinking of the gap for cybersecurity workers, companies will continue to struggle to find and retain strong talent.

Every company should strive to improve the maturity of their security operations capabilities and the resilience of their SOCs. The 2021 State of Security Operations survey found some surprising strengths in organizations' security operations—the vast majority of companies ambitiously intend to adopt nearly every important security technology and process. However, if this year has taught us anything, it's that plans change and security teams need to have a prioritized list of security initiatives. CyberRes recommends that organizations:

1. Implement processes and tools for attack-surface management to reduce the weak points in your network, with a focus on securing the most critical business functions, processes, "crown jewel" assets, and the digital supply chain.
2. Augment security staff by automating processes to make them repeatable and quick-to-implement when needed. Beyond automation, organizations should also seriously consider the value of threat intelligence, machine learning, AI/cognitive technology, and (where necessary) outsourcing, to supplement their SOC teams and reinforce their resilience.
3. Adopt a threat-modeling framework, such as MITRE ATT&CK or the Cyber Kill Chain, and promote its use within your SOC to enhance threat detection, identify security gaps, and unify your security ecosystem.
4. Establish a process for regularly evaluating your defenses with the right tools, from red teaming to cyber ranges to digital twins, and report the results to your CISO and Board.

[22] "Gartner Forecasts 51% of Global Knowledge Workers Will Be Remote by the End of 2021". Gartner Press Release. June 22, 2021.

[23] Joyce, Sean et al. "The cyber-threat landscape: The digital rush left many exposed." PwC. Web Page. n.d.

5. Finally, organizations should seek to align with enterprise, digital and cyber resiliency goals, by having their SOCs map their operational capabilities, threat models, risk, and performance metrics to securing the value chain. This extends beyond simply detecting and responding. Terminology for SOC evolution (EDR, MDR, etc.) may come and go, but the fundamentals of securing the value chain will be a persistent determinant of SOC alignment with the business.

Next Steps

We hope you have found the results of this report to be both informative and instructive. The survey can be a starting point for your security operations teams to discuss the impact of the past 18 months, and where your company wants to be in the next 18 months.

For more information, we recommend you check out the companion webinar to this report, 2021 State of Security Operations: Insights and Implications, where CyberRes CTO Mark Fernandes shares his perspective on the survey results and their significance to SOCs globally. Additionally, CyberRes will soon be kicking off a multi-episode video series to discuss the report with various CyberRes guest speakers that have extensive SOC expertise. Be sure to subscribe to the ArcSight Unplugged YouTube channel to be notified the moment these videos are published.

Finally, we have created an assessment that will help you identify gaps in your cybersecurity posture, so you can understand how to prioritize them for your business. The assessment will help you by comparing your company's current security posture with others in the global community, allowing you to focus on the areas that most need improvement. Take the assessment now.

Your Voice: What Would You Like to See in the 2022 Report?

Help us shape the 2022 State of Security Operations report by taking a brief, 3-question survey. Let us know what you liked most about this year's report, which questions were most useful to you, and what you'd like to see in next year's report.

Take the survey.

Contact us at **CyberRes.com**

Like what you read? Share it.