ANOMALI

iSMG INFORMATION SECURITY MEDIA GROUP

How to Operationalize Your Threat Investigations and Response

Automation, machine learning, and global visibility can help improve detection and response to cyberthreats.

Introduction

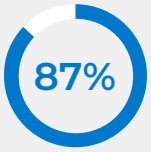
The proliferation of cyberattacks has become an existential threat for businesses no matter where or how they operate in the global economy. Cunning threat actors engineer shape-shifting cyberattacks that pose potentially grave risks to organizational operations, data security, systems uptime, and revenues.

Everything is on the line, and companies can't afford to get it wrong.

Yet the complexities of detecting and responding to intrusions remain an incredible challenge for most. In a recent Anomali-sponsored Harris Poll survey, 87% of enterprise security decision makers said their organizations have experienced a successful cyberattack in the past three years that resulted in damage, disruption, or a breach to their business.[1] Separately, consider that more than half (52%) of organizations admit their security environment has become more difficult to manage over the last two years, according to a global survey of security leaders conducted by market research firm Enterprise Strategy Group (ESG).[2] Top reasons include highly skilled threat actors, an ever-expanding attack surface, public cloud adoption, and a massive number of security alerts, many of them false.

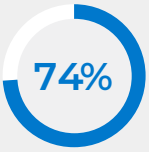
Rising challenges are not surprising, given that the frequency and technical sophistication of cyberattacks rises every year. At the same time, the financial costs of compromise continue to climb. Globally, the average total cost of a data breach reached a highest-ever at $4.35 million in 2022, according to IBM Security's Cost of a Data Breach Report 2022.[3] Financial losses were far greater in the U.S., where costs associated with data breaches soared to $9.44 million in 2022 — more than twice the global average.

Security by the numbers



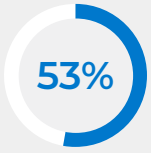
Nearly 90% of organizations have experienced a cyberattack in the past three years.

Anomali



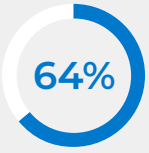
Three out of four organizations have increased their cybersecurity budgets and 78% are re-evaluating their cybersecurity strategies.[4]

Anomali



Just over half of decision makers feel their organizations are very effective at sharing threat intelligence information across internal resources.

Anomali



Nearly two thirds of organizations say keeping up with security requirements has become more difficult, up from **49%** a year ago.[5]

Splunk

$4.35 million

The average total cost of a data breach in 2022, highest ever.

IBM

$9.44 million

Average cost of a breach in the U.S., highest of any country.[6]

IBM

Source[1]: Anomali Cybersecurity Insights Report 2022
Source[2]: The Role of XDR in SOC Modernization - ESG Research from Anomali
Source[3]: Data Breach Reports

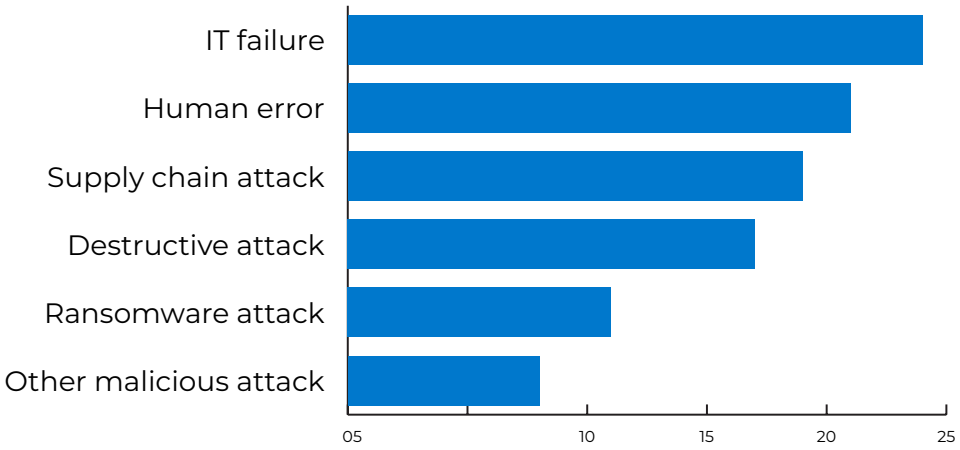
Source[4]: Anomali Cybersecurity Insights Report 2022
Source[5]: State of Security 2022
Source[6]: Data Breach Reports

Cybersecurity challenges get more complex

It's easy to see why securing digital assets is an increasingly formidable undertaking. Today's security tech stacks are extensive, intensely complex, and often not integrated with key cybersecurity tools and systems across the ecosystem.

Companies often deploy dozens of disconnected cybersecurity solutions and tools, which create torrents of data that can muddy visibility into enterprise-wide activities and threats. What's more, security teams must normalize data to make it compatible with multiple disparate security solutions. That's no small feat: ESG's research shows that 80% of organizations collect, process, and analyze security operations information from more than 10 data sources.[7]

Types of breaches



Source: IBM Security, Cost of a Data Breach Report 2022

Average cost and frequency of data breaches by initial attack vector

$4.91 M	Phishing
$4.89 M	Business email compromise
$4.55 M	Third-party software vulnerability
$4.50 M	Stolen or compromised credentials
$4.18 M	Malicious insider

Source: IBM Security, Cost of a Data Breach Report 2022

Source[7]: The Role of XDR in SOC Modernization - ESG Research from Anomali

Cybersecurity challenges get more complex, continued

Compounding matters is that companies have been slow to adopt automation. Manual processes are sluggish, inaccurate, and inefficient. This contributes to employee burnout, and higher breach costs. Nonetheless, 44% of companies say spreadsheets and email remain their most-used threat-research tools, according to the SANS 2022 Cyber Threat Intelligence Survey.[8]

The overnight transition to remote work during the COVID-19 pandemic also expanded the universe of security risks. That's because virtual employees may access an organization's internal resources and cloud systems using unsecured personal computers, smartphones, and home networks. With less direct interaction and training, employees are more susceptible to phishing and ransomware scams, which have spiked immediately and dramatically since the onset of the pandemic.

The pandemic also convinced many workers to reassess their personal and professional priorities. The result? Millions quit their jobs, a phenomenon known as the 'Great Resignation' that has tightened the talent squeeze for skilled IT and security workers. In 2021, a record 47.8 million U.S. workers abandoned their positions, according to the U.S. Bureau of Labor Statistics.[9] Deepening the concern: 72% of tech and IT workers said they were considering quitting within 12 months, according to TalentLMS.[10]

Finally, increased interconnection among an organization's systems and those of its trusted contractors, vendors, and other third parties can create an on-ramp for threat actors to attack your supply chains. Cybercriminals target these third parties, which may have weaker security standards than the primary company, by infiltrating partner systems to get a foothold on the primary organization's systems. Effective cybersecurity requires that organizations secure and protect their entire ecosystem of relationships.

Source[8]: Sans 2022 Cyber Threat Intelligence Survey
Source[9]: SHRM Interactive Quit Level by Year
Source[10]: Tech Employeess Great Resignation Statistics

Detection in action:
Identifying the Log4j vulnerability

To understand the criticality of automated processes in threat detection, consider the Log4j vulnerability, an exploit of a critical remote-code execution that was discovered in November 2021.[11]

In attempting to identify the Log4j vulnerability, a company will ingest a staggering volume of data. In one recent example, the business aggregated 200 million indicators of compromise and analyzed them against 2.5 billion events from 500 data sources. A volume of data this vast cannot be quickly or efficiently manually vetted.

But quickly identifying and remediating Log4j attack indicators can be vastly accelerated by adopting machine learning (ML) and process automation. Threat researchers can augment Log4j data and boost accuracy by gaining context on observed vulnerabilities, geolocation of attackers, and other threat intelligence.

ML and automated processes can empower threat specialists to correlate a massive amount of security telemetry and global intelligence to determine the presence of Log4j within minutes — or even seconds. The technology can then pivot to ML-generated mitigation strategies and detection signatures to inoculate systems against existing and future breaches. ML can also automate dissemination of machine-readable threat intelligence to the organization's security controls.

Source[11]: Using Anomali to Determine Apache Log4J Vulnerability Impact

Tech tools and techniques to improve threat intelligence management

Enterprise-wide threat detection and response demands broad and deep visibility into disparate security tools and gargantuan volumes of data.

Most organizations start with security information and event management (SIEM) systems and network traffic-analysis solutions. But these technologies process and store huge volumes of data that tend to generate false threat alerts, which creates additional work for security teams and can hinder their ability to respond quickly.

Organizations can solve this by implementing a platform that integrates automation and processes. Extended detection and response (XDR) solutions, for example, collect data across an organization and can automate processes, which can have a profound impact. Leveraging big data management and artificial intelligence, XDR can supplement existing SOC technologies to prioritize alerts based on risk, improve detection and forensic investigations, and reinforce security controls to prevent future attacks. XDR is most often used to fill gaps within the security stack, while improving the efficacy and efficiency of threat detection and response.

Another foundational element is cyberthreat intelligence (CTI). CTI comprises curated information about relevant threat actors and their tactics, techniques, and procedures (TTPs). CTI is housed on a threat intelligence platform (TIP), which orchestrates and automates intelligence workflows by aggregating, processing, and disseminating information. These platforms can automatically correlate inputs to help rapidly generate comprehensive information about adversaries. This context can empower threat specialists to deftly investigate, validate, and respond to cyberthreats using centralized, collaborative processes.

Undoubtedly, manual investigation and validation of threat alerts and correlation with intelligence is time-consuming and resource-intensive. A threat intelligence management solution that automates processes and integrates machine learning (ML) can make all the difference. ML is a subset of artificial intelligence (AI) that harnesses algorithms to parse information and evaluate individual indicators of compromise (IOCs) that are relevant to a specific organization.

Threat Data Sources

- Third-party premium feeds from security vendors.
- Open-source feeds from security researchers and vendors.
- Threat-sharing groups such as Information Sharing and Analysis Centers (ISACs).
- Open-source analysis platforms for malware information.
- Community knowledge bases such as the MITRE ATT&CK framework.

Tech tools to improve threat intelligence, continued

ESG's research shows that 90% of businesses are automating security operations processes.[12] And the benefits are clear: A threat intelligence management solution can automate processes and fuse the strengths of machine learning to generate fast, efficient, and accurate threat intelligence that feeds detection and response. Automation of key tasks can also help organizations reduce human error, relieve "alert fatigue" among threat teams, and make data-driven judgment calls. In addition, automation can help security teams focus on more proactive security practices, such as threat hunting. A Threat Intelligence Management solution can automate processes to combine all available, relevant data, enrichments, and other context and displays this information in ways that provide value, such as in dashboards, rulers, alerts, and notes, enabling analysts to:

- Explore threats.
- Provide investigation workflows.
- Understand the broader context and implications of threats.
- Share information.

Taking it step further, automating threat detection and response with XDR can fill any remaining gaps. XDR solutions can unite existing security technologies on a central platform to amplify visibility and ultimately stop adversaries and attacks. Using XDR solutions can assist security analysts to:

- Quickly determine the scope of an attack and respond based on historical security telemetry and global intelligence about threat actor tactics, techniques, and procedures (TTP).
- Move from reactive to proactive, reducing both the cost of incident management and the potential damage of a cyberattack.

Reduce mean time to detection (MTTD) and response (MTTR)

No organization can detect and deflect all intrusions. But identifying events quickly can lessen the impact — and the cost — of a breach.

It is estimated that attackers can evade detection for as long as 140 days, on average. Security decision makers admitted in Anomali's Cybersecurity Insights report that they are not meeting detection and response goals. For example, among respondents surveyed, the average MTTD for a data breach was 3.1 days, which lags behind their average goal of 2.1 days.

To fast-track detection, Anomali recommends:

- Pay close attention to both MTTR and MTTD metrics. It's crucial to be fanatic about reducing these metrics, as shorter dwell times reduce your risk of damage and disruption.
- Work to break down silos and collaborate cross-functionally to ensure effective detection and response processes.

Source[12]: The Role of XDR in SOC Modernization - ESG Research from Anomali

Know your enemy with MITRE ATT&CK

A core component of threat intelligence management is knowing your adversary, how they plan to attack you, and using that information to improve responses and prevent future incidents. That's where the MITRE ATT&CK Framework can help. ATT&CK is an acronym for Adversarial Tactics, Techniques, and Common Knowledge, which is a behavioral-based threat model that classifies and describes cyberattacks based on real-world experience. It's designed to help network defenders quickly detect incidents and understand attack techniques, then use that knowledge to prioritize defense.

The MITRE ATT&CK Framework uses analytics to collect log and event data to help quickly identify unusual systems behavior. The framework helps organizations understand what attack actions adversaries have taken in the past to predict future intrusions. This knowledge base can be augmented with an organization's historical intelligence and external threat intelligence sources.

Best practices to improve threat intelligence management

- Prioritize collaboration across security silos and threat detection activities.
- Use data classification and retention to help limit information vulnerable to breaches.
- Continuously monitor networks, endpoints, third parties, and remote employees to identify suspicious activity and threats.
- Use multifactor authentication and strong encryption to safeguard information, particularly for remote workers.

Best practices to improve cybersecurity resiliency

- Monitor and protect remote employees by deploying endpoint detection and response (EDR) and identity and access management (IAM) solutions.
- Create and test incident response plans.
- Perform red team exercises to understand real-world security vulnerabilities.

Stop cybercriminals and attacks

Cybercriminals are working overtime to design and deploy the next round of complex cyberattacks. Organizations must be equally diligent in deploying a solution that stops cyberattacks — and cybercriminals.

Using and investing in the right tools requires recognizing that while legacy solutions will continue to play a role in defensive strategies, they can no longer be relied upon solely to detect and respond to evolving threats. According to Anomali's 2022 Cybersecurity Insights survey, seven out of 10 (69%) organizations still use firewalls to detect threats in the network. In addition:

- 59% use Threat Intelligence and another 38% plan to invest.
- 48% use XDR and 44% plan to invest.
- 43% use the MITRE ATT&CK Framework and 47% plan to invest.

The Anomali Platform is a cloud-native threat detection and response solution that helps scale security operations and enables threat specialists to strengthen defense capabilities. Anomali fuses the world's largest repository of global adversaries, techniques, and indicator intelligence with precise detection capabilities to continuously detect current threats and prevent future attacks. Our intelligence-driven, cloud-native detection and response solution helps fortify defense capabilities and enhance return on security investments. The Anomali Platform is comprised of differentiated offerings including:

1. **Threat Intelligence Management:** ThreatStream, automates the collection and processing of raw data to create actionable intelligence and eliminate noise to speed threat detection, streamline investigations, and boost analyst productivity. Anomali ThreatStream integrates with existing security infrastructure to operationalize threat intelligence and improve organizational efficiencies.
2. **Threat Detection Management:** Match, an intelligence-driven detection engine helps organizations detect and respond to threats in real-time by automatically correlating all security telemetry against global active threat intelligence. Anomali Match provides precision attack detection that enables security teams to pinpoint relevant threats, understand criticality, and prioritize response.
3. **Threat Insights:** Lens, a powerful extension for browsers and Microsoft Office that quickly operationalizes threat intelligence by automatically scanning digital content to identify relevant threats and streamline researching and reporting. Anomali Lens uses natural language processing (NLP) to scan structured and unstructured internet content to help automate the identification of adversaries, malware, and cyberthreats.
4. **Exposure Management:** Gain visibility across your attack surface to identify risks and defend against targeted threats. The Anomali Platform correlates an organization's internal attack surface with its global threat landscape to prioritize investigation and response activities.

Improving resilience requires that organizations go beyond thwarting breaches. They must also stop attackers, now and in the future. The Anomali Platform can help you accomplish both. To learn more, visit Anomali.

Anomali is the leader in modernizing and scaling security operations, delivering breakthrough levels of security visibility and intelligence-driven threat detection and response. In a world filled with SIEM, SOAR, and XDR, the Anomali Platform amplifies visibility, integrating with existing security controls and enriching them with actionable context to stop adversaries. Anomali helps customers and partners transform their SOC platform by elevating security efficacy and reducing their costs with automated processes at the heart of everything. The solution is anchored in big-data management and boasts the world's largest repository of global intelligence that supports native-cloud, multi-cloud, on-premises, and hybrid deployments.

Learn more at www.anomali.com.

www.anomali.com | +1 844-4-THREATS (847328) | +44 8000 148096 (International Toll-Free)

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG INFORMATION SECURITY MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io