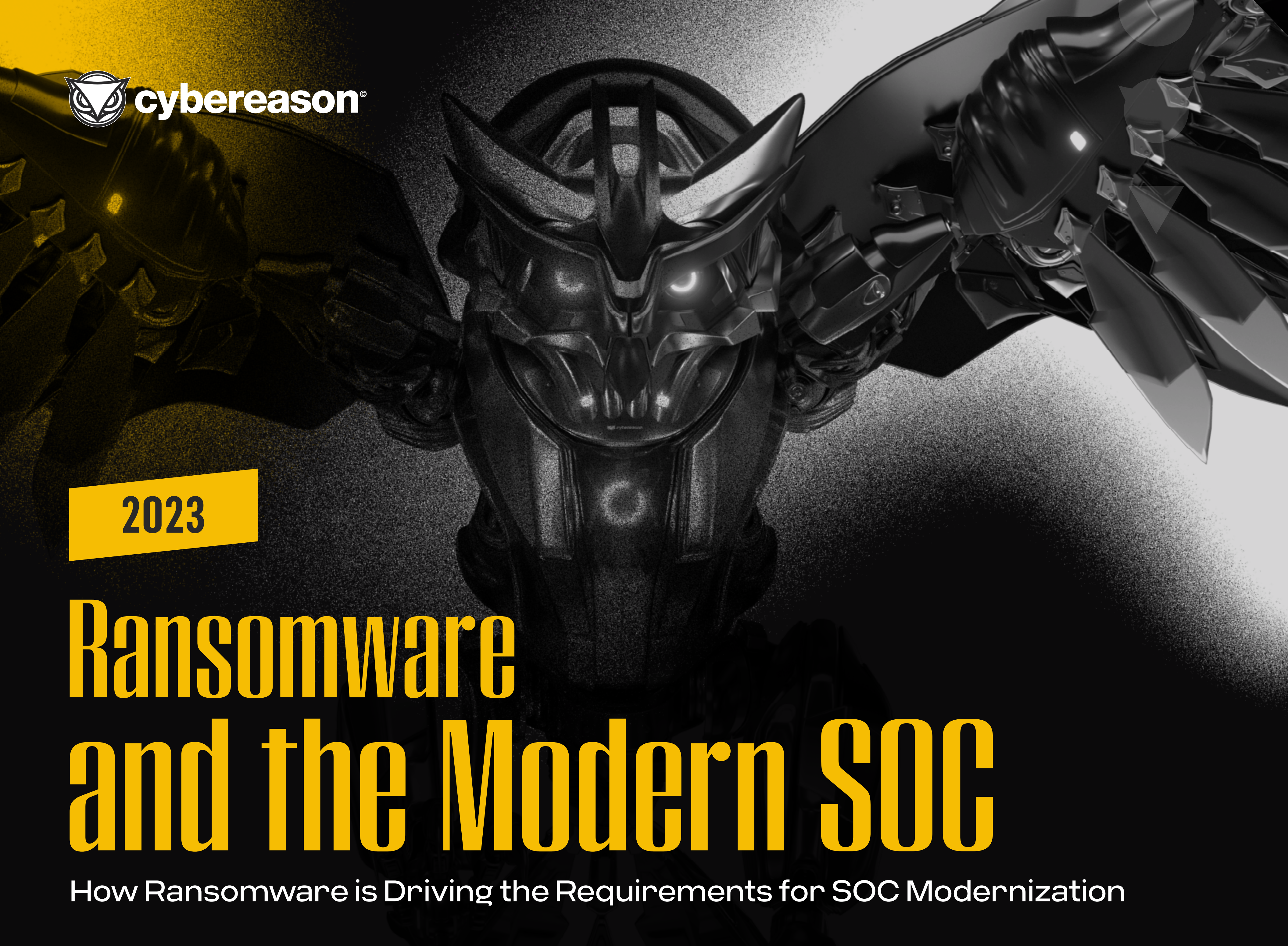


cybereason

2023

Ransomware and the Modern SOC

How Ransomware is Driving the Requirements for SOC Modernization

Contents

Introduction

Security Operations Centers (SOCs) of all sizes and levels of sophistication are in a constant stranglehold stemming from workforce shortages, lack of visibility and automation, tool sprawl, and alert overload. The status quo of constantly battling to stay ahead of adversaries, show a return on security investments, and ensure that hard-to-come-by staff is not overworked to the point of burnout is untenable.

In a new Cybereason survey, 1,203 security professionals from eight countries and a dozen industries were asked to describe the challenges currently faced by their SOCs and how they impact their plans for modernization.

Nearly half of the respondents (49%) said ransomware is the most common incident type they deal with daily, followed closely by supply chain attacks (46%). Thirty-seven percent said daily alerts consumed most of their time, and 31% identified targeted attacks as a top daily concern.

1,203

SECURITY PROFESSIONALS

8

COUNTRIES

MOST COMMON INCIDENTS

RANSOMWARE	49%
SUPPLY CHAIN ATTACKS	46%
NORMAL DAILY SECURITY CONCERNS	37%
TARGETED ATTACKS	31%

Key Takeaways

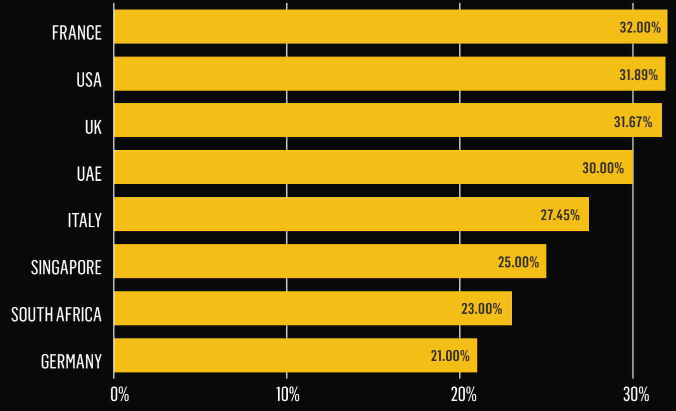
57% of respondents say resolving an incident takes 3 to 6 hours from discovery.

59% of respondents said it takes their company two hours to 1 day to resolve a ransomware incident. **19%** said resolving a ransomware incident takes 3 to 7 days.

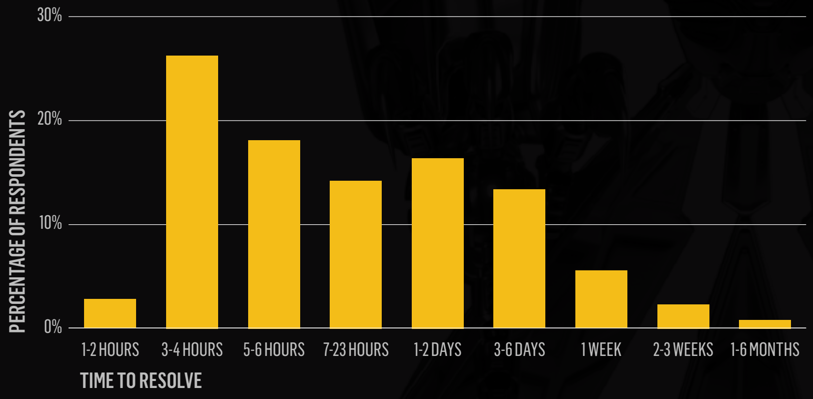
88% of respondents said they have missed a holiday or a weekend because of a ransomware attack.

More than a third of companies report receiving between **10,000 and 15,000** security alerts per day.

GLOBAL RESPONDENTS WHO SAID RANSOMWARE HAS INCREASED THE NEED FOR AUTOMATION AND FASTER RESPONSE



AVERAGE TIME IT TAKES TO RESOLVE A RANSOMWARE ATTACK



Ransomware & the Capabilities-Based SOC

The challenges identified thus far are enough to justify the investments needed to modernize today's SOC. However, it is essential to note that there is no longer one standardized SOC model that organizations can use. Today, building or modernizing a SOC is no longer about a centralized location with specific security tools. It's about delivering specific functions, capabilities, and outcomes needed by a particular organization.

More than 58 percent of survey respondents said their SOC spends most of its time responding to ransomware and supply chain attacks that can lead to ransomware incidents. When asked how ransomware impacted their plans for SOC modernization, survey respondents specifically pointed to four requirements:

38% New detection capabilities that have better detection efficacy

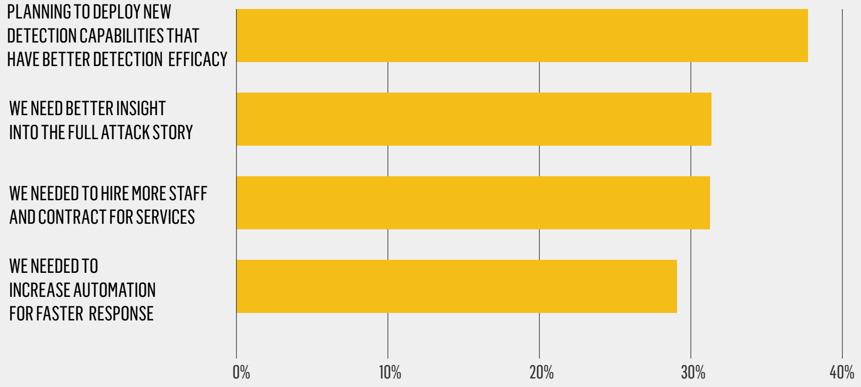
31% Better insight into the full attack story

31% More staff and contracts for services

29% More automation for faster response

Building, modernizing, or operating a SOC are evolutionary processes that change as the business, its needs, and the threat landscape change. The trajectory for the post-COVID era SOC is clear: The modern SOC will be a decentralized, capabilities-based organization that leverages industry-leading detection, prevention, visibility, and automation technologies, all of which are often augmented by managed services.

Q1 HOW, IF IN ANY WAY, HAS RANSOMWARE CHANGED YOUR SOC SKILLS?



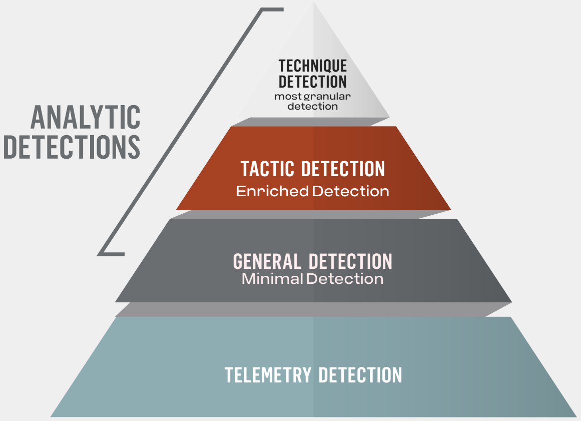
Need for New Detection Capabilities

Thirty-eight percent of survey respondents said they plan to deploy new threat detection capabilities with better detection efficacy.

Regardless of size and sophistication, a modern SOC can leverage focused threat detection and response capabilities driven by business risks and priorities.

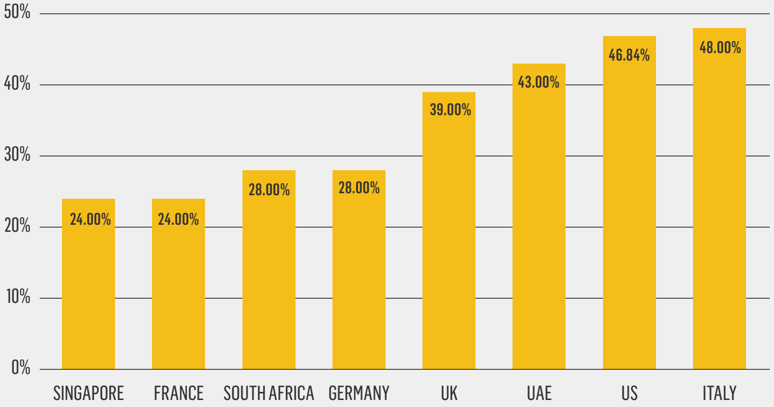
Traditional endpoint security solutions rely on limited Indicators of Compromise (IOCs) - the artifacts from previously-known attacks. Modern detection capabilities go beyond IOCs, leveraging Indicators of Behavior (IOBs) to detect the subtle signs of an attack. These chains of behavior reveal an attack at the earliest stages by surfacing malicious human and machine activity to uniquely expose and end never-before-seen attacks before they escalate to a major breach event.

Solutions that are highly effective against today's threats—especially sophisticated threats like ransomware—must be able to detect malicious activity immediately without waiting for additional processing time or human analyst intervention.



Analytic detections are built from a broader data set and are a combination of technique + tactic detections. SOC teams are in desperate need of this nuanced view of what took place for enriched detections.

Q2 RESPONDENTS PLANNING TO DEPLOY NEW DETECTION TECHNOLOGIES DUE TO RANSOMWARE



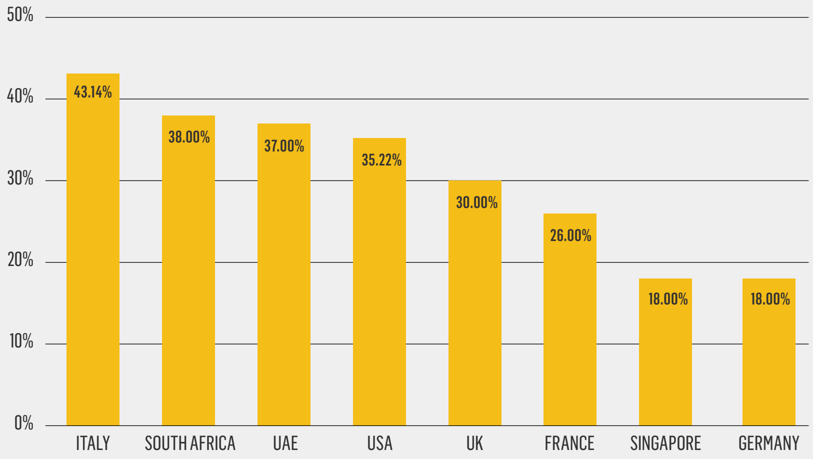
Need for Better Insight Into Full Attack Story

Thirty-one percent of survey respondents said the threat of ransomware has exposed their need for better insight and visibility into the full attack story.

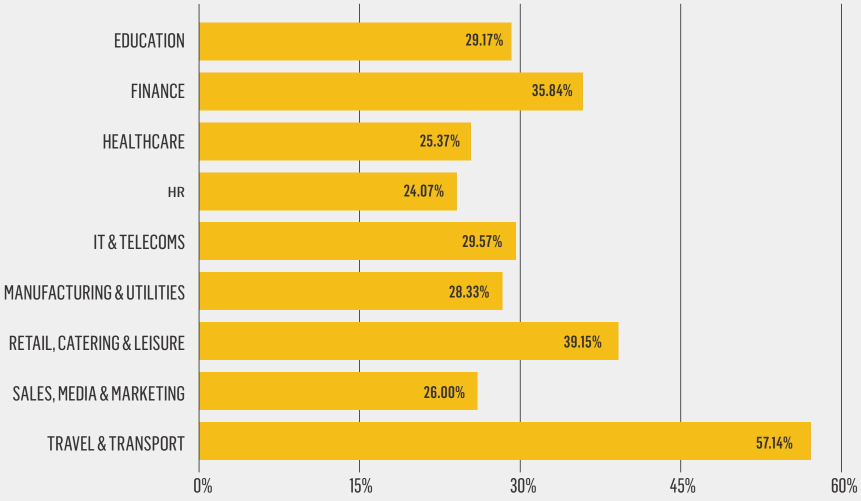
Assessing the ability of solutions to provide visibility quantifies their effectiveness at providing the full context of an attack, uncovering where it originated, what was affected, the timeline of events, and the granular details of the attack chain.

Leveraging an operation-centric approach means the full attack story from A-Z is contained in a single screen, including all impacted users and devices. This unique understanding of data relationships means that the full context of an attack accompanies every detection within a malicious operation, including all users, devices, identities, and network connections.

Q3 RESPONDENTS BY COUNTRY WHO SAY THEY NEED BETTER INSIGHT INTO FULL ATTACK STORY



Q4 RESPONDENTS BY INDUSTRY WHO SAY THEY NEED BETTER INSIGHT INTO FULL ATTACK STORY



Need for More Staff and Services

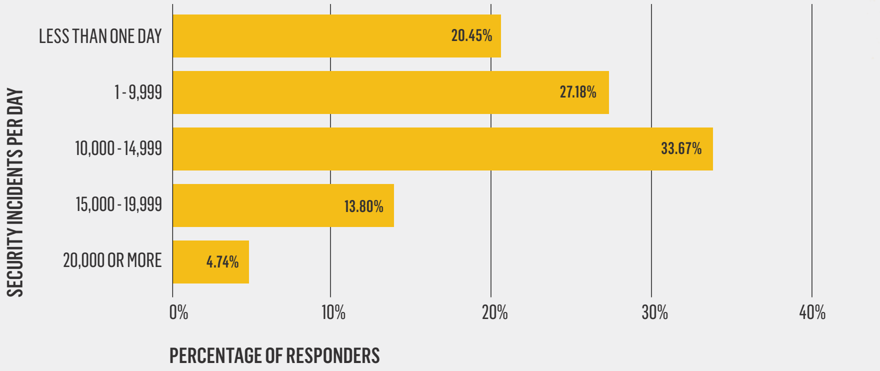
More than one-third of respondents said their SOCs receive between 10,000 and 15,000 security alerts per day.

Information overload remains the primary contributor to the problem of alert fatigue. Security Information and Event Management (SIEM) platforms are designed to err on the side of too much visibility rather than miss an alert that later becomes critical and leads to a serious security event. This means an oversensitive SIEM will issue an alert for anything resembling suspicious activity, and security analysts are left to dig through the noise to find actual malicious activity.

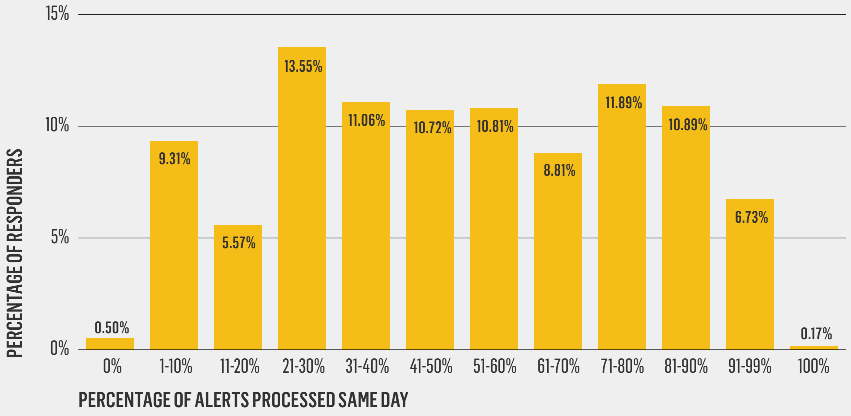
The global cybersecurity talent crisis has impacted SOC teams worldwide and compounded the alert overload problem. The cyber industry is dealing with a mass shortage of qualified staff, with negative employment and roughly 3.5 million unfilled cyber positions globally. The most skilled Tier III analysts are extremely difficult to source and even more challenging to retain. Not surprisingly, information overload and the pressure analysts feel to ensure they detect malicious activity has led to burnout and high staff turnover.

These challenges have generated increased interest in Managed Detection and Response (MDR) services. MDR removes the burden and arduous process of alert triaging and prioritization and gives time back to security teams to conduct remediation and focus on other priorities. As a stand-alone security solution or an additional layer of security to an existing SOC, MDR immediately matures any organization's security posture.

Q5 HOW MANY, IF ANY, SECURITY INCIDENTS DOES YOUR SOC RECEIVE ON AN AVERAGE DAY?



Q6 PERCENTAGE OF ALERTS PROCESSED ON THE SAME DAY THEY ARE RECEIVED



Need for Increased Automation for Faster Response

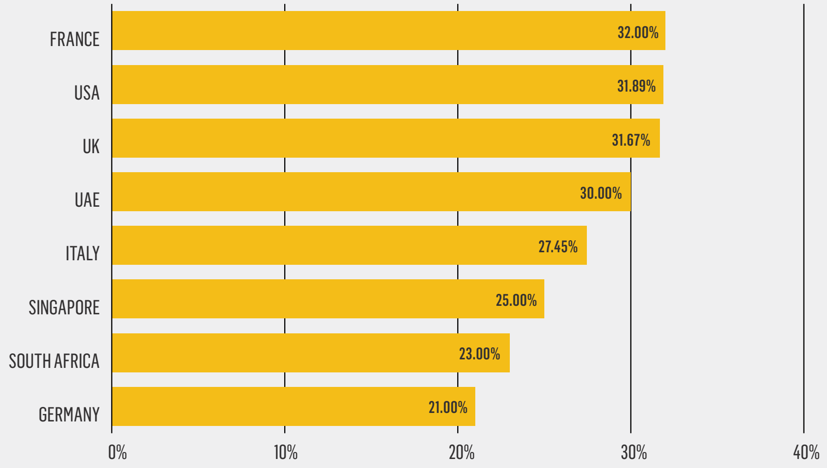
Twenty-nine percent of respondents globally said ransomware has increased their need for automation and faster response times.

Solutions that are highly effective against today's threats—especially sophisticated threats like ransomware—must be able to detect malicious activity immediately without waiting for additional processing time or human analyst intervention.

Incident response should be orchestrated and automated to all impacted endpoints and users through tailored response playbooks without needing an outside Security Orchestration, Automation, and Response (SOAR) solution.

This advanced and automatic analysis increases analyst speed and accuracy by reducing the noise of alerts with a focused deconstruction of the overall operation. With all the information an analyst needs to scope and respond to a malicious operation concisely presented, analysts can drastically reduce their Mean Time to Respond (MTTR).

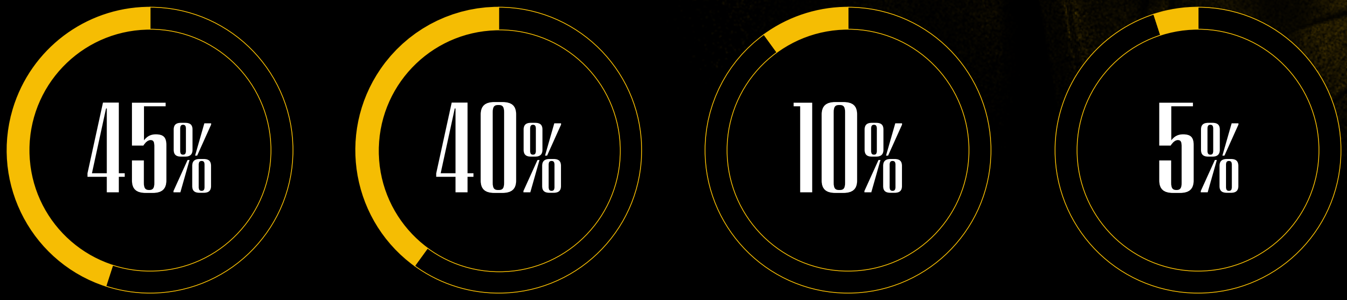
Q6 PERCENTAGE OF RESPONDENTS WHO SAID RANSOMWARE HAS INCREASED THEIR NEED FOR AUTOMATION



Note on Methodology

This report is based on a global survey of 1,203 cybersecurity professionals working at companies with 700+ employees. The survey was conducted between Sept. 27, 2022, and Oct. 4, 2022.

The seniority breakdown of respondents was as follows:



SENIOR MANAGERS/ PROFESSIONALS

DIRECTOR LEVEL PROFESSIONALS

BUSINESS OWNERS

MIDDLE MANAGERS/ PROFESSIONALS

ABOUT CYBEREASON

Cybereason is the XDR company, partnering with Defenders to end attacks at the endpoint, in the cloud, and across the entire enterprise ecosystem. Only the AI-driven Cybereason Defense Platform provides predictive prevention, detection and response that is undefeated against modern ransomware and advanced attack techniques. The Cybereason MalOp^{tm} instantly delivers context-rich attack intelligence across every affected device, user, and system with unparalleled speed and accuracy. Cybereason turns threat data into actionable decisions at the speed of business. Cybereason is a privately held international company headquartered in Boston with customers in more than 40 countries.

Learn more at **www.cybereason.com**