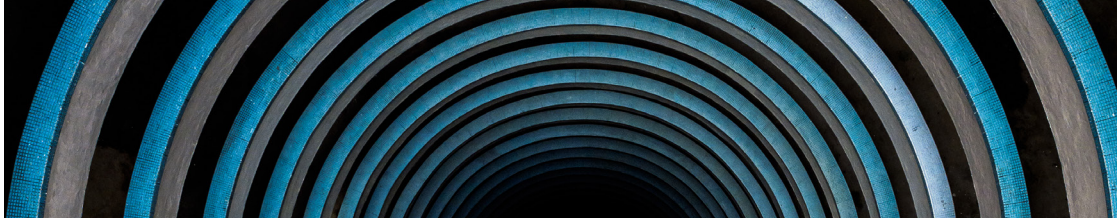
S&P Global
Market Intelligence

451 Research
Business Impact Brief



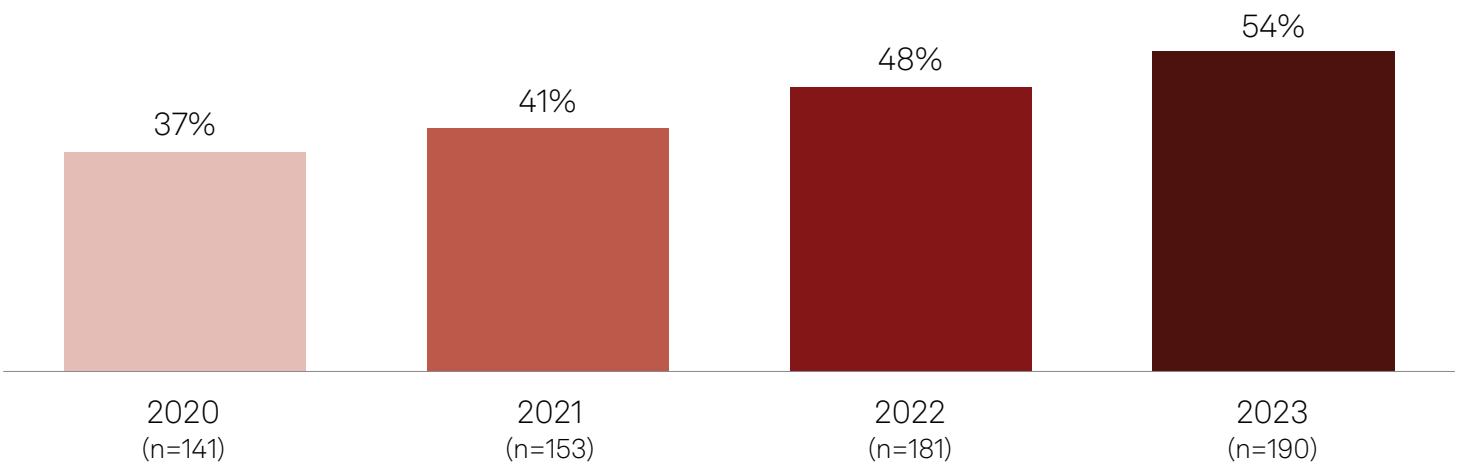
Building a cyber resilient future with inter-team collaboration

The Take

Recent trends such as accelerated digital transformation, the continued move to cloud and emerging AI technologies have increased organizational focus on security and resiliency. By their nature, these systems are dynamic and difficult to monitor, and it can take time to remediate the damage when incidents occur. This increases the risk of security incidents, data loss, litigation and compliance violations. In our survey research, we have been following the increasing percentage of alerts that security teams are unable to investigate in a typical day; it has been increasing by roughly 6 percentage points per year despite increases in information security spending (see figure below).

It's clear that managing increasing alerts and longer remediation times coupled with skills shortages requires more than throwing money and tools at the problem; organizations must also improve processes and efficiencies to fully realize value from investments. Realizing this, many chief information security officers have turned their focus to response and recovery, which are critical since many alerts are not addressed for days or longer.

Percentage of alerts security teams are unable to investigate in a typical day, 2020-2023



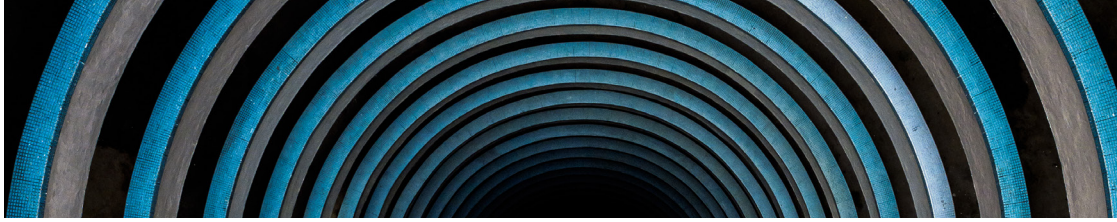
Q. What percentage of SIEM/security analytics alerts are you unable to investigate in a typical day?
Base: Respondents who currently use SIEM security analytics.
Sources: 451 Research's Voice of the Enterprise: Information Security, Vendor Evaluations 2020, 2021; Security Operations 2022; Security Analytics & SecOps 2023.

One way to become more efficient is to improve collaboration between cybersecurity and IT operations teams. Historically, they operated as separate groups, and in many organizations, a "throw the problem over the wall" culture still exists, where security teams focus on detection and analysis while IT operations performs remediation tasks.

The lack of inter-team collaboration can result in longer response and recovery times that can translate into system downtime, ransom payments and compliance issues. Changing this culture — even to the extent of team reorganization — and investing in tools that foster collaboration and simplify workflows can yield significant results by getting the business back online quickly with the least amount of impact to systems and data. Organizations should prioritize deployment of modern cyber-resilient architectures built upon tiered resiliency that address threats before, during and after an event. Alignment to the National Institute of Standards and Technology (NIST) 2.0 cybersecurity framework with a focus on detection, response and recovery is recommended. A cyber-resilient architecture should produce enhanced speed (for detection and recovery) and security (with built-in indelibility) and should be simple to deploy and manage.

S&P Global
Market Intelligence

451 Research
Business Impact Brief



Business impact

US NIST CSF 2.0 provides a set of six cybersecurity functions and desired outcomes to help organizations manage cybersecurity risks, including an emphasis on reducing silos and encouraging collaboration. Four of the key areas are "protect," "detect," "respond" and "recover."

Protect includes access management, protection and monitoring of devices, plus using automated backups and ensuring data is recoverable. While security and IT often collaborate on the first three items, backups are often left to the IT operations team. Security must be involved in defining and orchestrating backup and restoration processes and ensuring that recovery objectives are met when a loss occurs. Key considerations include: using tiered resilience when architecting cyber resiliency strategies; ensuring immutable and indelible data copies to ensure backup integrity; using certified clean storage for recoveries; utilizing cost-effective cloud storage for long-term and less-critical backups; and deploying cloud-based data backup. Ideally, the same system used for on-premises backups also supports cloud-based applications and data. Consider designing a system that supports partial recovery of critical systems before full recovery completes.

Detect includes monitoring networks, systems, facilities and users to quickly identify and stop cybersecurity attacks early. It's a key area for collaboration. For example, many security teams fail to realize the security value of data continually passing through backup systems, which can indicate malware and ransomware activity and changes in user and entity behavioral patterns. These signals can provide clues that aid in early detection of security incidents. IT teams can aid security teams by providing additional sources of telemetry that, when correlated with other signals, can improve early detection.

Respond includes actions taken when a cybersecurity incident is detected and requires further investigation. Collaboration can help today's overwhelmed security and IT teams determine the scope of an issue and quickly shut down affected resources before an attack spreads, reducing its severity. Another common response is to initiate recovery as quickly as possible to minimize business impact.

Recover includes steps taken after a critical incident has occurred. The ability to initiate rapid recovery begins with the design and implementation of backup systems, where security and IT not only collaborate on system architecture design and implementation, but also participate in recovery drills to ensure both teams are prepared to rapidly restore after incidents — from a single machine to an organization-wide outage.

Looking ahead

It's clear that security and IT operations teams can benefit by working closely with one another. Collaborating on system design, implementation and operations can ensure rapid recovery when a critical outage occurs, minimizing its impact on the business. Many organizations have embarked on this strategy and are realizing benefits.

One example is decreased cyber insurance premiums and improving the odds of obtaining (and keeping) insurance. Acquiring and retaining cyber insurance has become increasingly difficult, complex and expensive due to losses from high-profile attacks. The rise in payments has led some insurance providers to decline coverage for ransomware attacks, and carriers have become more specific about what they will cover. In 451 Research's Voice of the Enterprise: Cyber Insurance 2023 study, 68% of cyber insurance policyholders reported that it is more difficult to meet the requirements of their policies than it was 12 months ago, and only 43% of respondents indicated cyber insurance is in place at their organization. Some carriers are requesting audits or proof that policyholders meet certain criteria before issuing a policy — and proving the ability to rapidly recover from an attack is likely a major consideration.

It would behoove organizations to take a hard look at their information security spending with an eye toward decreasing detection, response and recovery times while improving the relationships between IT operations and security cohorts. This can ensure that both organizations function in lockstep across all phases of the security life cycle. It is no longer a luxury; it is a necessity.