451 Research

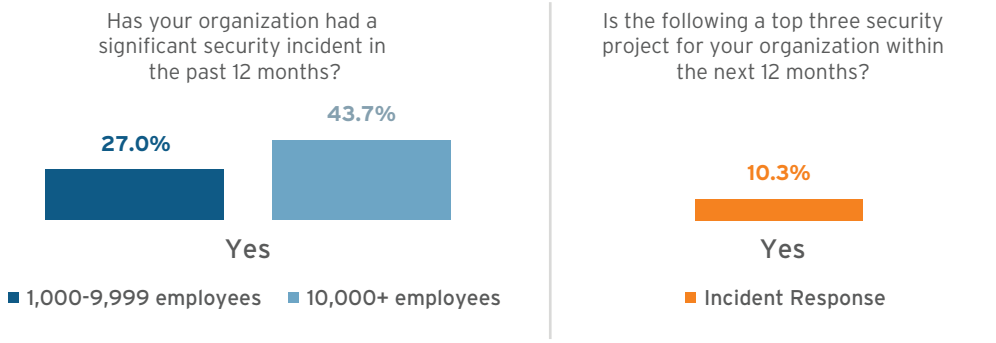
Business Impact Brief

Security Focus on Prevention and Detection Over Incident Response Leaves Enterprises Vulnerable

The 451 Take

For years many organizations have taken a preventive-based approach to cybersecurity focused on controls such as firewalls, antivirus and intrusion prevention systems – often placing too much confidence in the ability of these tools to protect the business. There's now a growing industry realization that while preventive tools can consistently stop many known threats, they often fail to defend against newer, more sophisticated cyberattacks, making it only a matter of time before an organization will be compromised. According to a recent 451 Research Voice of the Enterprise survey, over 43% of large enterprises have experienced a significant security incident in the past year.

Despite Significant Security Incidents at Many Organizations, Incident Response Is Rarely Prioritized



Source: 451 Research, Voice of the Enterprise: Information Security, Organizational Dynamics 2017

This number is likely much higher, since many organizations may not know they have been – or currently are – compromised. Unable to completely defend against an increasing number of cyberthreats, some businesses have shifted their attention to detection capabilities in the hope of minimizing the impact of compromise by rapidly identifying threats that have bypassed the preventive tools in place.

While both prevention and detection are necessary to protect the enterprise, organizations often overlook the importance of incident response (IR). In a 451 Research VotE survey, only 10.3% of enterprises cited IR as an immediate priority – placing it well below other, largely preventive, security initiatives. Yet as well-publicized security breaches have shown, poor incident response often makes a bad situation worse, resulting in lost business, bad publicity, lawsuits and brand erosion. Poor or slow IR not only increases risk, but can severely impact a company's bottom line.

Simply having an IR plan is not enough, though. Manual processes typically limit the efficiency and effectiveness of IR approaches. For IR to be effective, organizations must invest in capabilities for integrated and intelligent automation, process orchestration, knowledge management and case management to enable timely and accurate response, collaboration, investigation and remediation of incidents across the enterprise.

New approaches to IR aim to align, automate and orchestrate the people, processes and technology required to effectively respond to and mitigate threats while still allowing organizations to be dynamic and agile in adapting to attacks. Such platforms provide an intelligence-led approach to IR, enabling organizations to address incidents quickly and accurately.

Business Impact Brief

Business Impact

IMPROVED RESOURCE ALLOCATION AND MINIMIZED SKILL GAPS. Understaffed and under-skilled security teams face time-consuming manual tasks that detract from more strategic response efforts and slow the IR process. Fatigue and human error can make the response worse than the security incident itself. Automating low-complexity, high-volume tasks and enabling subject-matter experts to push knowledge to frontline engineers can help mitigate these challenges and better leverage human capital.

FASTER RESPONSE AND REMEDIATION. As the attack surface grows and threats become more sophisticated and multidimensional, security teams need more time to understand and respond to events with manual efforts. With automation and orchestration, security teams can proactively gather threat intelligence, event logs and contextual alert data to support data-driven decision-making, reducing the time required to assess and respond to events.

IMPROVED CROSS-FUNCTIONAL TEAMWORK. IR is complex work that requires more than just skilled security pros in a SOC. While it may be the SOC team's responsibility to handle incidents, they rely heavily on IT operations teams for much of the work to resolve an incident. This requires the teams to come together quickly when an attack occurs. Collaboration tools, standardized and automated response procedures, and knowledge capture/sharing enable faster response and remediation.

ABILITY TO ADAPT TO AN INCREASINGLY COMPLEX LANDSCAPE. Organizations are rapidly deploying new technologies. Hybrid cloud infrastructures are now standard for many enterprises, resulting in a wide array of distributed workloads, interconnects, access controls and logging capabilities, making security incidents more difficult to remediate and investigate. Incorporating automation and orchestration into IR brings the ability to analyze incidents quickly, determine the systems affected and identify the resources required for remediation.

MEET COMPLIANCE AND REGULATORY REQUIREMENTS. Most organizations operate under one or more regulatory schemes (e.g., PCI, HIPAA, GDPR) as well as various laws with provisions on IR. Many of these requirements focus on notification, evidence handling, reporting and specific timing of when response events must occur. An IR platform can better equip enterprises to address compliance concerns.

Looking Ahead

Hacking has evolved from isolated activity into a large, profitable and organized business. Ransomware is now a lucrative, low-risk business model for cybercriminals, and the rise of destructive malware is destabilizing businesses and state organizations. Digital transformation and emerging technologies are introducing new risks more quickly than enterprises can understand or react. A majority of organizations say they lack critical security expertise and resources. This is the current state of cybersecurity, and it's only going to get worse.

Cybercriminals will acquire the capabilities to do more damage more quickly. Leveraging AI, automation and ML, they will launch fully autonomous attacks able to adapt and make decisions that counter preventive and detection controls in real-time. These attacks will be harder to detect, more disruptive and more costly. Although enterprises will deploy new intelligence-based security capabilities, attackers will maintain the lead, and organizations will continue to be breached.

IR will remain a critical component for a defense-in-depth strategy as enterprises mature in their response to security incidents. Specialized, intelligent and automated IR tools will be required to meet new regulatory obligations and fill the security expertise and staffing gaps.

RESOLVE SYSTEMS™

Resolve Systems is the leading security incident response automation and orchestration platform. With powerful and adaptive automation, out-of-the-box standards-based playbooks, and ability to orchestrate response enterprise-wide, security teams are able to quickly investigate, respond and resolve incidents. Learn about our agile automation platform and how to accelerate incident response by visiting our *Security Incident Response Page*. Headquartered in Irvine, California with operations in EMEA and APAC, Resolve Systems is owned by Insight Venture Partners.