How to Better Guard Against a Security Breach

While making progress in setting strategies and policies to anticipate security breaches, many organizations are unable to fully utilize security and event data.

Perimeter defenses alone are no longer sufficient to ensure protection of enterprise data. In a world of increasingly sophisticated and persistent cyber attacks, business and IT leaders are ramping up investments in a wide range of security solutions. However, a recent IDG Research Services survey indicates many lack confidence in their company's ability to detect or mitigate a sophisticated IT security breach.

Decision makers say that compliance issues and improved business continuity are the primary drivers behind approval of enterprise security projects, and the survey finds many are making progress when it comes to documenting security policy and forming comprehensive strategies. But the survey, conducted on behalf of HP ArcSight, also reveals that barely half of the respondents are confident in their ability to utilize event logs to meet compliance requirements or detect suspicious behavior.

The survey polled IT and business decision makers who are involved in the purchase of IT security solutions and services at their organizations. The base provides a broad representation from companies with fewer than 250 workers to more than 5,000, spanning a range of industries.

Highly Motivated

Achieving and maintaining compliance with government or industry regulations is a top driver behind funding approval for IT security projects, according to 60% of respondents. Improving business continuity is the next top driver, say 55%.

Indeed, compliance has long been a factor in justifying investments in security information and event monitoring (SIEM), says Eric Schou, director of product marketing for HP ArcSight. "But the core reason a SIEM is purchased today is for security use cases," he adds.

Remarkably, 90% of respondents indicate they made progress over the past 12 months in documenting IT security policy, with more than half saying their progress is either complete (26%) or significant (36%). Most of those (70%) have invested in SIEM technology, which, according to Gartner Inc.[1], "aggregates event data produced by security devices, network infrastructures, systems and applications."

Despite their investments in SIEM and the notable progress in developing strategy and policy, barely half (51%) of survey respondents that utilize security and event log data have strong confidence in their ability to detect or mitigate breaches. That may reflect the continuing focus on perimeter protection and firewall technologies—the top priority for coming investments, according to 56% of survey respondents. Interestingly, that's despite the growing industry-wide recognition that building higher fences is no longer a viable security strategy in the face of sophisticated cyber assaults.

Many enterprises "are investing, typically, in the same things they invested in last year and the year before," says Schou. "They are spending money on 'blocking technology' rather than looking in a different way at adversaries who have proven they are extremely good at getting past the security perimeter."

That said, according to the Ponemon Institute's 2014 cyber crime study, U.S. businesses that deployed security intelligence technologies including SIEM realized significant benefits. "Findings suggest companies using security intelligence technologies were more efficient in detecting and containing cyber attacks. As a result, these companies enjoyed an average cost savings of $5.3 million when compared to companies not deploying security intelligence technologies."[2]

The 59 U.S. companies reporting data experienced 138 discernible cyber attacks *each week*, according to Ponemon. The average annualized cost to counter those attacks was $12.7 million. But, says Ponemon, "Companies deploying security intelligence systems experienced a substantially higher ROI, at 30%, than all other technology categories presented."

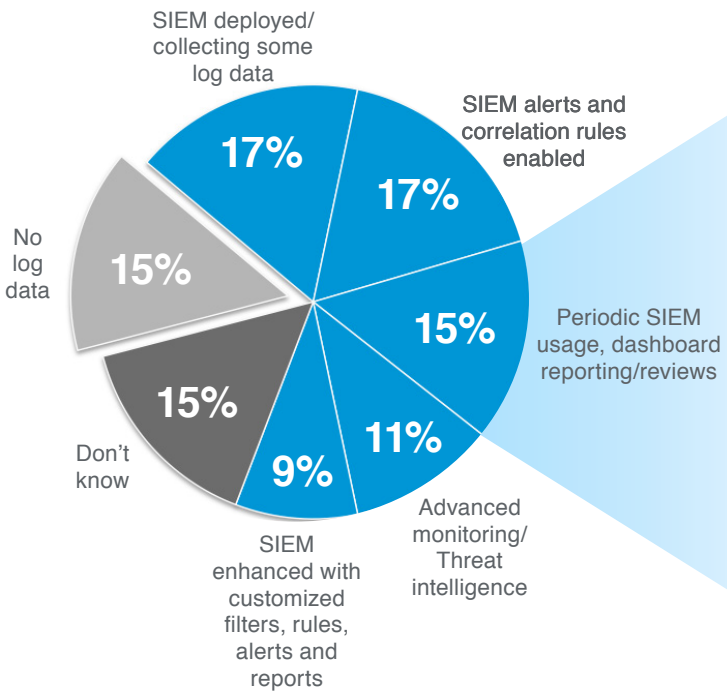
Getting to the Next Level

While organizations have invested in people, processes and technology designed to prevent malicious access to networks and endpoints, utilization of SIEM as a security bulwark tends to be perfunctory, with only 20% indicating they are using their solutions in an advanced or customized manner.

Achieving real-time situational awareness with a SIEM solution requires the ability to centrally collect and analyze information from thousands of devices and applications in order to detect unusual or unauthorized activities as they occur. But the volume of log alerts can often overwhelm an organization's ability to respond to or investigate potential breaches and other security lapses.

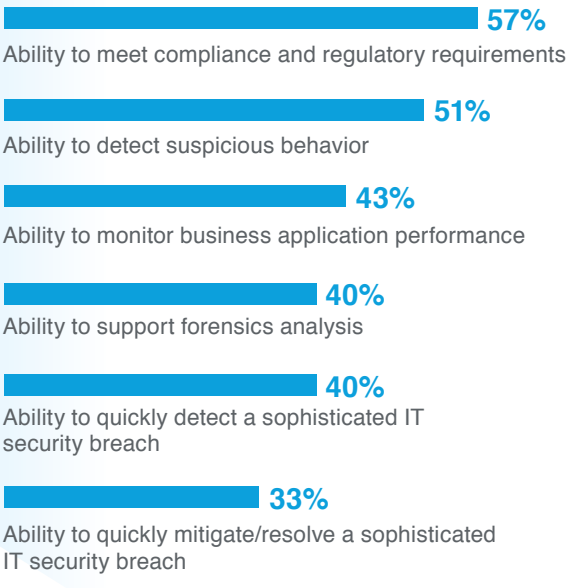
Organization's deployment of SIEM (security information and event monitoring)

DEPLOYMENT OF SIEM



CONFIDENCE IN UTILIZING LOGS TO PERFORM

% Extremely/Very Confident; Of those that have log data



SOURCE: IDG Research Services

Furthermore, midsize companies that in the past may have been less exposed to cyber threats are now viewed by criminals as softer targets and need to be as adept as larger organizations that have invested major resources in security infrastructure and personnel. No matter the size, few can afford to continually grow security teams and budgets, so organizations need greater analytical capabilities to prioritize and respond to those alerts that are most likely to represent a threat. That takes a "big data–like" approach that can sift through massive volumes of event log data to detect and even predict security lapses, says Schou.

Enterprises are seeking simpler management interfaces and more relevant, actionable information and advanced threat detection capabilities. "It can't be something that takes weeks and weeks to figure out," Schou says. In response, he adds, the industry is concentrating on providing SIEM solutions that are more use-case focused and prescriptive, and that can be up and running and producing results in a short period of time.

Such an approach is critical to alleviating the lack of confidence in addressing threats that IT and business leaders expressed in the IDG study. A more advanced, analytical solution that can deal with sophisticated threats will ensure that organizations can respond quickly and effectively when, as seems inevitable, cyber attackers are able to find their way around perimeter defenses.

For more information, please go to:
hp.com/go/arcsight

COMBATING THE DELUGE

After investing in people, processes and technology to prevent malicious access to networks and end-points, enterprises find themselves overwhelmed by a growing deluge of alerts.

That was the situation in 2001 when ArcSight brought to market technology designed to provide security event analysis and correlation, which was quickly adopted by larger enterprises to help deal with growing threats. The technology now resides within an industry category known as security information and event management (SIEM) and HP subsequently acquired ArcSight.

Today, HP ArcSight serves companies of all sizes with a big data analytics approach that generates actionable intelligence that can reduce the cost of a breach and help minimize risk to business. Using thousands of different types of device and application connectors, HP ArcSight ESM (enterprise security management) provides a central point for analysis of daily business operations, and its real-time correlation capabilities can detect unusual or unauthorized activities as they occur.

Rather than waiting weeks or longer for analysts to wade through reams of log data and assess what is happening, administrators, managers or auditors can utilize personalized dashboards and on-demand or scheduled reports to gain insight and take action on the actual threat.

[1] SOURCE: Kelly M. Kavanagh, et al, "Magic Quadrant for Security Information and Event Management," 25 June, 2014.
[2] SOURCE: "2014 Cost of Cyber Crime Study: United States," October 2014. Ponemon Institute