Machine Learning, Analytics, and Open Source Boost Cybersecurity

Study: IT leaders say visibility is lacking and they would welcome new platforms

CIO Strategic Marketing Services

SPONSORED BY:

cloudera

intel

Today's global enterprises are hyperconnected. Employees, partners, and customers access corporate systems at any hour of the day or night, from anywhere in the world. Meanwhile, the Internet of Things (IoT) is bringing countless new devices onto corporate networks. Together, these trends greatly increase the threat surface that must be defended against hackers and cybercriminals.

Cybersecurity is at the top of the priority list for IT leaders, and with good reason. Breaches can be devastating to a company's finances and reputation. Threats such as phishing, viruses, and distributed denial of service (DDoS) attacks are increasing in number and sophistication. This is true across all industries, particularly the public sector, financial services, retail, and healthcare. And the cost of protecting critical data is putting pressure on corporate budgets.

A new IDG Research survey identifies specific cybersecurity challenges and delivers insight into how IT leaders are responding.

Cybersecurity challenge: SIEM gaps

Many organizations have responded to cybersecurity challenges by deploying a security information and event monitoring (SIEM) system to detect, investigate, and respond to threats. However, many are finding that they fall short in certain respects. The deficiency most often cited (by 45% of the survey respondents) is the frequency of false-positive alerts—when the SIEM system raises the alarm for a breach when, in fact, there is none. (See chart)

"The biggest challenge is the amount of time people have to spend to make it a valuable tool. They need to review all the logs and alerts, pick out false alarms, and respond where needed," says Jason Gherardini, vice president of IT at real estate firm J.F. Shea.

Cybersecurity challenge: visibility

Visibility is a distinct challenge for many organizations implementing cybersecurity strategies. "The biggest challenge is not knowing what I don't know," says Gherardini.

The survey details several problems caused by lack of visibility:

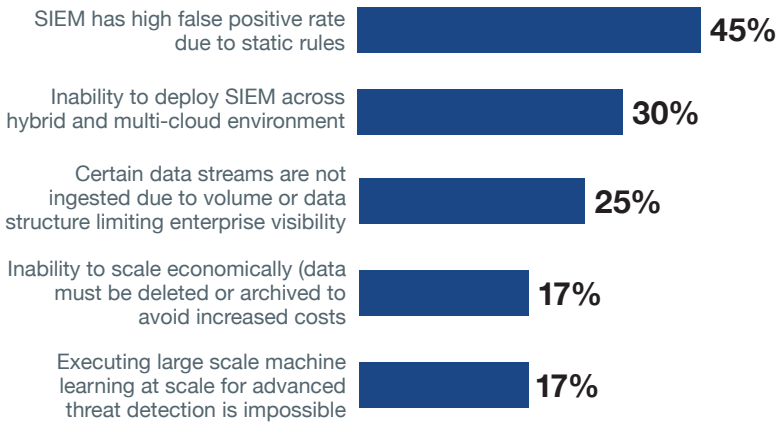
- Incomplete information for investigation and response to security events (51%)
- Inability to create reliable threat detection models with enriched data (43%)
- Inability to search across complete historical data (42%)
- Limited contextual data (34%)
- Long mean time—weeks or months—to incident response (15%)

Cybersecurity response: Machine learning

To detect security threats faster and more accurately, a significant majority (70%) are using machine learning to analyze data streams and detect anomalies for incident responders and to automate threat response.

One of the main benefits of machine learning is breaking down large amounts of data to detect advanced threats and root out false positives.

Issues with Traditional SIEM



Source: IDG Research

"The information we receive from lots of sources is like a fire hose. We need to boil that down to something that's reasonable and targeted," says Stash Jarocki, director of information risk and security at food and drug retailer Albertson's.

Larger organizations—those with more than 5,000 employees—are more likely to use machine learning for threat response automation (42%) than are organizations with fewer than 5,000 employees (17%), according to the survey. This finding suggests that smaller organizations could gain by leveraging machine learning if they could find a platform suited to their needs.

Cybersecurity response: open source

A strong majority of the respondents (72%) are using open source software for cybersecurity. The top reasons: to democratize cyber analytics and gain access to community knowledge, libraries, and experiences as well as to break vendor lock-in by owning the systems that manage the data.

"You get value from open source," says John Nelson, security officer with U.S. Expediters. Nelson has implemented open source software broadly at his company, including for machine learning, and is interested in applying it to cybersecurity.

Additional benefits of using open source technology for cybersecurity are the ability to scale economically on commodity hardware or in the cloud (33%), to improve scalability with regard to data volume and variety (27%), and to enable ISV applications to easily integrate into a platform (18%).

Cybersecurity response: New analytics platforms

IT leaders are facing the challenge of defending their organization from cybersecurity threats with an open mind: 61% of the survey respondents said they are highly likely to evaluate new analytics platforms over the next 12 months. "An analytics engine to process all that data, root out false positives, and find the anomalies: That would pique my interest," says Jarocki. And interest in new platforms is greater at higher levels within organizations. In fact, 83% of the vice president and higher survey respondents said they are extremely or very likely to evaluate new platforms.

The Cloudera Solution

Cloudera empowers cybersecurity innovators to proactively secure the enterprise by accelerating threat detection, investigation, and response through machine learning and complete enterprise visibility.

Cloudera's cybersecurity solution, based on Apache Spot, enables anomaly detection, behavior analytics, and comprehensive access across all enterprise data, using an open, scalable platform. Building on Cloudera's scalable, open platform enables organizations to build custom solutions as well as deploy packaged applications on top of one shared, enriched data set.

Using the diverse open source community to accelerate shared innovations while changing the economics of cybersecurity enables organizations to come together to fight back against cyberthreats.

Conclusion

As cybersecurity threats increase in variety and number, cybersecurity leaders face the daunting challenge of protecting corporate data. Although many have deployed SIEM systems as a defense, these systems produce too many false positives and cannot be deployed across hybrid and multi-cloud environments. And they cannot scale to the volume of data required for modern threat detection, investigation, and response.

In addition, insufficient visibility and enriched data impede threat detection and investigation. Increasing the amount of data accommodated by SIEM systems, and applying machine learning can address these issues. Many organizations, particularly larger ones, are benefiting from them. Open source is proving to be a key enabler for cybersecurity technologies, including machine learning. As IT leaders search for new platforms to help defend their organizations, many will find that open source machine learning technologies deliver the benefits they seek.

For additional information, go to www.cloudera.com/cybersecurity