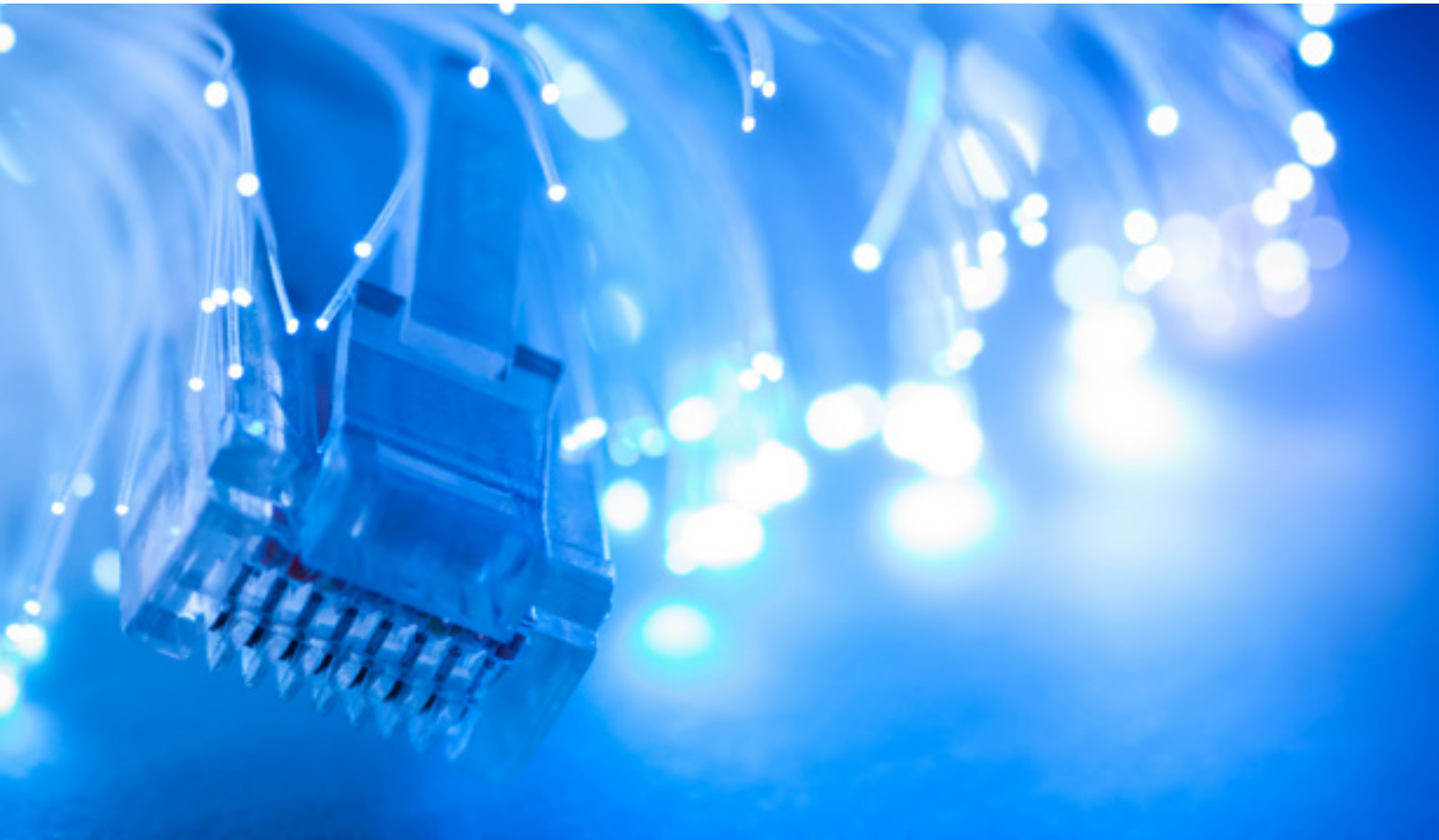
cybereason

Data Breaches

Don’t Blame Security Teams, Blame Lack of Context



The increased likelihood that an organization will be breached has security teams under greater pressure to fend off attackers. However, as stories about cyber attacks continue to appear in the news, the reality is even the best protected organizations are no match for highly motivated hackers.

Even though enterprises spend millions of dollars on cyber-security protection and detection solutions, the average breach goes undetected for 256 days, according to a Ponemon Institute study. Then, once an incident is discovered, it usually takes another month for security teams to investigate the attack's overall damage and magnitude. This significantly prolongs response time and has devastating financial impacts on a business. **The average cost of a data breach totalled $3.79 million in 2015, according to the study.**

Traditional tools cannot reveal if the alert was a localized event or a part of a far more dangerous hacking operation

Incompetence and negligence aren't why security teams fail to defeat complex hacking operations. Attacks succeed because security teams desperately lack threat context. Analysts are blinded by the thousands of daily alerts they receive from various security tools. Even the most sophisticated security teams are unable to comprehend an attack because most security products lack the capabilities to produce cohesive alerts.

When the Human Factor Fails

Since security tools produce a large amount of unwarranted alerts, security teams must manually investigate them, meticulously weed out false alerts and connect isolated malicious activities in order to reveal an attack. In an ideal world, where there is an abundance of highly skilled security experts, the need for manual investigation would be less detrimental. However, this security paradigm significantly weakens your defense for several reasons:

Isolated Alerting Equals Limited Remediation

Because traditional security systems issue alerts on individual events, security teams will also remediate isolated issues without taking historical evidence into consideration. For instance, IT will be alerted about a virus on a single endpoint and then clean that computer. However, they cannot tell if an employee brought the virus in from working at home or someone downloaded it from an email. Traditional tools do not reveal if the alert was a localized event or a part of a far more dangerous hacking operation. The inability to see individual events as part of something larger will make it very difficult for security teams to detect and remediate a cyber attack, giving hackers a major time advantage.

Alert Blindness

Security solutions rely on indicators of compromise (IOCs) to triggers an alert. These IOCs are based off very rigid predefined rules. For example, multiple failed log-in attempts will produce an alert. However, since security solutions lack the capability to automatically judge alerts by examining other evidence, a large amount of alerts are produced, many of which are false.

According to an industry report, 56% of organizations claim their security tools produce too many false positives. This issue leaves security analysts feeling rightfully uneasy. They are never completely sure if the problem was fixed or if something was missed.

Out of Context, Out of Touch

Nearly 70% of the organizations we work with say their security tools do not provide them with enough context about a threat. Because many security tools focus only on individual events instead of the entire IT environment, cyber attacks can go undetected for long periods of time. The key is to see a hacker's every move. This can only be achieved by having complete visibility into an IT environment and a technology that automatically connects isolated events to provide a more accurate picture for analysts. Technologies that can bring in context will allow you to tell if multiple security alerts came from the same source, what circumstances led to the alert and relate end-user activity to malicious actions.

When applied to security, big data analytics will eliminate the need for manual investigation and provide a more holistic approach in the battle against sophisticated cyber attacks.

Automated Context: Relieving the Burden of Investigation

Advancements in big-data analytics and machine learning can change the current security paradigm. When applied to security, big-data analytics will eliminate the need for manual threat investigation and provide a more holistic approach in the battle against sophisticated cyber attacks. This technology can add context to an attack by monitoring and recording all the endpoint and network activity in an organization.

Machine Learning can then be used to judge individual incidents, similar to how the human brain works. Machine Learning compares isolated actions to historical events, external sources of knowledge and other related communications taking place within an environment. This knowledge aids a security team's decision making, closing the gap between detection and response and enabling them to successfully combat complex hacking operations.

This item was previously featured in Forbes.

cybereason

Cybereason was founded in 2012 by a team of ex-military cybersecurity experts to revolutionize detection and response to cyber attacks. The Cybereason Malop Hunting Engine identifies signature and non-signature based attacks using big data, behavioral analytics, and machine learning. The Incident Response console provides security teams with an at-your-fingertip view of the complete attack story, including the attack's timeline, root cause, adversarial activity and tools, inbound and outbound communication used by the hackers, as well as affected endpoints and users. This eliminates the need for manual investigation and radically reduces response time for security teams. The platform is available as an on premise solution or a cloud-based service. Cybereason is privately held and headquartered in Boston, MA with offices in Tel Aviv, Israel.