EINPRESSWIRE

Picus Security Analysis Of 14m Attack Simulations Reveals Organizations Only Prevent 6 Out Of Every 10 Attacks

Blue Report highlights four "impossible trade-offs" security teams make with threat exposure management

SAN FRANCISCO, CA, USA, August 8, 2023 /EINPresswire.com/ -- Picus Security, the pioneer of Breach and Attack Simulation (BAS) technology, has released The Blue Report 2023. Based on an analysis of more than 14 million cyber attacks simulated by The Picus Platform*, the report highlights four “impossible trade-offs” limiting modern security teams’ ability to manage their organization’s threat exposure.

“Like a short blanket that covers either someone’s head or feet, not both, security teams can only dedicate their time, money, and resources to so many problems at once,” said Picus Co-founder and VP of Picus Labs, Dr Suleyman Ozarslan. “They deploy their budgets and resources to cover one exposed spot, but this leaves other areas out in the cold. The Blue Report shines a light on these impossible trade-offs and how they hinder organizations’ readiness to defend themselves against the latest threats.”

According to the report, security teams make four trade-offs in deciding:

Which attacks to prioritize

Picus’ Blue Report data shows that, on average, organizations’ security controls (such as next-gen firewalls and intrusion prevention solutions) only prevent 6 out of every 10 attacks. However, some attack types are prevented far more effectively than others. For instance, organizations can prevent 73% of malware downloads but only 18% of data exfiltration attacks.

Organizations also prevent complex, multi-stage attacks less than half the time. This is particularly concerning given the findings of The Red Report 2023, a previous research study by Picus, which found that over a third of malware samples exhibit 20 or more attacker tactics, techniques and procedures (TTPs).

The Blue Report also reveals wide variations in organizations’ ability to prevent specific threats. For example, over a third of organizations can prevent Black Basta and BianLian ransomware attacks but only 17% can prevent Mount Locker. This is despite Mount Locker’s emergence in

2021 before the other two malware attacks.

Which vulnerabilities to remediate

The Blue Report also reveals the limitations of security teams' approach to managing common vulnerabilities and exposures (CVEs). Analysis of the simulated attacks shows that the list of top 10 CVEs to which they remain most exposed includes mainly critical and high risk vulnerabilities as well as CVEs that have been known for years. Some CVEs discovered in 2019 remain a threat to more than 80% of organizations.

Whether to optimize prevention or detection controls

Generally speaking, the better an organization is at preventing threats, the weaker it is at detecting them, and vice versa. For instance, globally healthcare is the least effective sector at preventing attacks but is twice as successful as the average organization when it comes to detecting them. North American organizations are almost twice as successful at preventing attacks as they are at triggering alerts to detect attacks in progress.

What to log and alert on

Organizations leveraging security event and incident management (SIEM) solutions also face decisions about how much to invest in attack detection. In most cases, organizations routinely prioritize logging over alerting but do neither very well. Simulation data shows that, on average, organizations log 4 out of 10 attacks but only generate alerts for 2 in 10 attacks.

“Since preventing and detecting every threat is practically impossible, security teams will always have to prioritize some aspects of security more than others,” said Dr Ozarslan. “Fortunately, there is an approach that can help them improve their performance. By adopting a more unified approach that incorporates insights from attack simulations combined with attack surface and vulnerability data, security teams can allocate resources efficiently and effectively to address their most critical exposures. As a result, they can simultaneously improve their ability to prevent and detect attacks, rather than making trade-offs between them, and sleep better at night.”

Picus Security will discuss the findings of The Blue Report at Black Hat USA 2023 in Las Vegas on August 9th and 10th. Visit booth #2700 to learn more and discover the benefits of using attack simulations to reduce threat exposure.

Notes

* Picus Labs analyzed over 14 million attack simulations executed by The Picus Complete Security Validation Platform between January and June 2023.

About Picus Security

Picus Security helps security teams of all sizes to continuously validate and enhance organizations’ cyber resilience. Our Complete Security Validation Platform simulates real-world threats to automatically evaluate the effectiveness of security controls, identify high-risk attack paths to critical assets, and optimize threat prevention and detection capabilities.

As the pioneer of Breach and Attack Simulation, we specialize in supplying the actionable insights our customers need to be threat-centric and proactive.

Picus has been named a ‘Cool Vendor’ by Gartner and is recognized by Frost & Sullivan as a leader in the BAS market.

* Frost Radar™:: Breach and Attack Simulation 2022, Frost & Sullivan

Mike Marquiss
Decoded Comms
+61 476267683
Mike@decodedcomms.com

This press release can be viewed online at: https://www.einpresswire.com/article/648850691