Cybereason Outperforms Every Company in the MITRE ATT&CK Evaluations

The Cyber Defense Platform’s Automated Threat Detection Delivers the Most Coverage Across the Entire MITRE ATT&CK Framework, the Most Real-Time Alerts and the Most Correlation of Malicious Activity

BOSTON (PRWEB) February 21, 2019 -- Cybereason, creators of the leading Cyber Defense Platform, today announced it has outperformed every competitor as a result of the MITRE ATT&CK Evaluations, released earlier today. The company’s Cyber Defense Platform demonstrates best-in-class automated threat detection, including total coverage across all MITRE ATT&CK phases, the most real-time alerts and correlation of malicious activity.

As a high-level benchmark, the results show that Cybereason covered more of the ATT&CK framework than the eight other vendors evaluated. The company’s Cyber Defense Platform is best at describing in real-time the full story of malicious activity so security analysts can stop attacks before material damage happens.

MITRE ATT&CK serves multiple objectives including defensive gap assessment for organizations or security tools. As a behavior-focused adversary model, it emulates tactics of real threat actors. ATT&CK evaluations reveal how vendors approach the same problem: reducing the time it takes to identify, understand, and respond to malicious actions before material damage occurs. Comparatively, the results also reveal effectiveness under real-world conditions.

Cybereason’s automated threat detection outperformed other tools proving its effectiveness. Cybereason’s evaluation is part of a rolling MITRE ATT&CK process that started in late 2018. To read more about Cybereason’s MITRE ATT&CK evaluation results, visit the company’s blog.

Why Are Cybereason’s MITRE ATT&CK Results Significant to Enterprises?

- Cybereason has the best coverage across all attack phases. Cybereason consistently detected nearly every trace of malicious activity. Fully correlated alerts represent the full attack story, substantially lowering the bar for analysts to take action. If you know everything that happened, cleanup is easy.
- Cybereason alerts, called Malops ™ (malicious operations), tell the complete attack story, detecting initial compromise and providing context for detections that are deliberately connected across all tactics. Too often, analysts are overloaded with multiple, disconnected alerts that become counterproductive, resulting in misses, alert fatigue, or gaps.
- Cybereason is the only vendor to deliver immediate, contextualized, associated alerts automatically and consistently across all tactics without analyst overload or visibility gaps. They did this by delivering more distinctive real-time alerts with no delays and no configuration changes.
- Cybereason’s Cross Machine Correlation Engine powers ‘best in industry’ correlation of malicious activity in an environment by intelligently connecting detections, enrichment, and telemetry across all tactics without requiring additional time and risk of inconsistency due to manual construction of the story.

The Cyber Defense Platform demonstrated best-in-class threat detection coverage across all ATT&CK phases. Using behavioral detection, the evaluation demonstrated Cybereason’s consistent ability to automatically pinpoint attacker methods at each stage of the kill chain. With fully automated alerts or Malops, the solution
delivered in real-time a complete attack story. The console interface visualizes the data and empowers defenders to stop attacks before material damage happens.

“Cybereason is thrilled with the MITRE ATT&CK Evaluation results as they demonstrate that our automated threat detection outperforms all other vendors evaluated. At Cybereason, we define detection not as an alert that says ‘something is wrong,’ but as a signal that empowers the defender to act. Effective alerts are immediately actionable – you shrink to zero the time the attacker can freely roam in your environment,” said Yonatan Striem-Amit, co-founder and CTO, Cybereason.

Cybereason confirmed participation in the MITRE ATT&CK evaluation on July 30, 2018. Its evaluation began on November 27, 2018 and was completed on November 29, 2018. The company wasn’t privy to any results prior to MITRE releasing its first round of evaluation results on November 30, 2018.

To learn more about Mitre ATT&CK evaluations visit their website https://attackevals.mitre.org/

About Cybereason
Cybereason, creators of the leading Cyber Defense Platform, gives the advantage back to the defender through a completely new approach to cybersecurity. Cybereason offers endpoint detection and response (EDR), next-generation antivirus (NGAV), and active monitoring and incident response services, all powered by its Cross-Machine Correlation Engine. The Cyber Defense Platform provides unmatched visibility, increases analyst efficiency and effectiveness, and reduces security risk. Cybereason is privately held, has raised $189 million from top-tier VCs, and is headquartered in Boston, with offices in London, Sydney, Tel Aviv, and Tokyo.

Learn more: https://www.cybereason.com/
Follow us: Blog | Twitter | Facebook

Media Contact:
Bill Keeler
Director, Public Relations
Cybereason
bill.keeler@cybereason.com
(929) 259-3261
Contact Information
Bill Keeler
Cybereason
http://https://www.cybereason.com
929 259-3261

Online Web 2.0 Version
You can read the online version of this press release here.