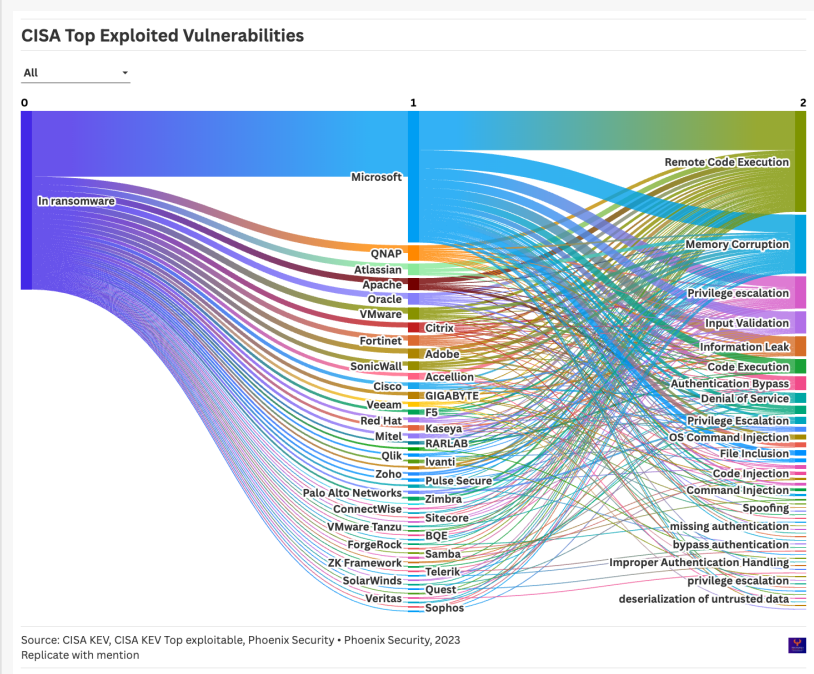
Phoenix Security Unveils Groundbreaking Threat-Centric AI Agent at VulnCon, for a Next-Gen Vulnerability Management

Phoenix Security Unveils Revolutionary Threat-Centric AI Agent at VulnCon predicting which vulnerability will become a ransomware or is likely to be exploited



Phoenix Security Analysis of Ransomware

RALEIGH, NC, UNITED STATES, April 8, 2025 /EINPresswire.com/ -- Phoenix Security is proud to announce the launch of its first AI-powered Threat-Centric Agent at VulnCon, marking a major leap forward in proactive vulnerability management and remediation. This new agent, built on a 3-step threat-centric approach, is designed to work seamlessly alongside Phoenix's Reachability Analysis AI Agent and Blast Radius Analysis Copilot, enabling organizations to focus on the most dangerous vulnerabilities and apply targeted remediation strategies with unmatched precision.

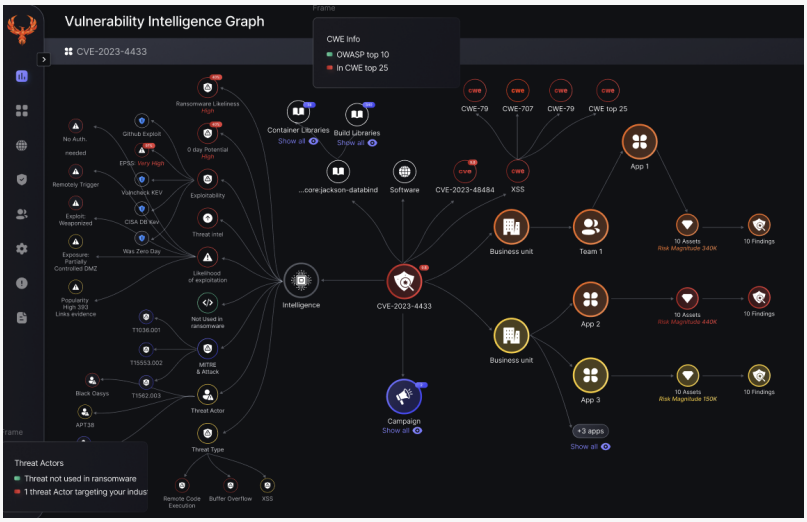
> What we saw in here is beyond ground breaking, nobody has even come remotely close to connecting the threat dots like phoenix security did"
>
> *CTEM Gartner Analyst*

The new Threat-Centric AI Agent is the result of Phoenix Security's continuous innovation in the cybersecurity space. With Reachability Analysis AI already achieving a 71.5% reduction in vulnerabilities for high-profile clients like Clear Bank, and the Blast Radius Analysis Copilot providing invaluable insight into the impact of vulnerabilities within network ecosystems, the integration of this agent promises to provide even greater risk mitigation capabilities. Together, these solutions align to ensure comprehensive, accurate, and efficient vulnerability management across diverse IT environments.

A Groundbreaking New Approach to Vulnerability Risk

At the core of this innovation is the 4D Risk Formula, a sophisticated framework that evaluates threats across four key dimensions:

Phoenix Security ASPM winner of Gartner Peer insight and Get app



1. Business Context (Dimension 1):

This dimension assesses the criticality of the affected software, understanding how disruptions to business operations can amplify the risk of a vulnerability. Whether it's a core application or a high-visibility service, knowing what's mission-critical enables security teams to prioritize threats based on real-world impact.

2. Dangerousness of the Vulnerability (Dimension 2):

By leveraging CWE and CVE standards, the agent determines the severity of vulnerabilities, including those not yet publicly disclosed. This dimension ensures that organizations are prepared to respond not just to current threats but also to emerging vulnerabilities that could evolve into critical risks.

3. Probability of Exploitation (Dimension 3):

This dimension predicts the likelihood of a vulnerability being exploited by attackers, factoring in the presence of weaponized exploits, zero-day threats, and real-time threat intelligence feeds. By considering historical exploitation trends and current attack vectors, the Threat-Centric Agent offers organizations a highly predictive view of their exposure.

4. Deployment Context (Dimension 4):

Understanding the context of vulnerability deployment—whether in production systems or isolated test environments—is crucial for prioritization. This dimension uses contextual canary tokens to measure exposure levels, ensuring that remediation efforts are applied first to the most exposed assets.

The Threat-Centric Approach: A Revolution in Remediation

By adopting a threat-centric approach, Phoenix Security's new agent shifts the focus from traditional, CVSS-based scoring to a more comprehensive model that incorporates real-time, attack-driven intelligence. This method ensures that remediation efforts are aligned with actual threats rather than theoretical vulnerabilities. With its ability to correlate threat data across

attack vectors and exploit trends, the Threat-Centric Agent helps security teams make faster, more informed decisions on where to allocate resources and which vulnerabilities pose the greatest risk to their organization.

The integration of Phoenix's Application Security Posture Management (ASPM) strategy further enhances the effectiveness of this new agent. By providing a continuous feedback loop between vulnerability identification, exploitation probability, business impact, and asset exposure, security teams can gain a clearer view of immediate threats, accelerating the path to remediation and reducing response time.

Real-World Impact: A Focus on Ransomware and Exploitability

Ransomware, a prominent and growing cybersecurity threat, is at the center of Phoenix Security's Threat-Centric AI Agent. This agent analyzes vulnerabilities based on their exploitation potential by ransomware actors, offering immediate, actionable insights. With the rise of ransomware as a significant global threat, the agent's ability to identify which vulnerabilities are likely to be leveraged in future ransomware attacks is crucial for businesses to protect their critical assets.

Phoenix Security's Threat-Centric AI Agent tracks the most common ransomware tactics used by threat actors, including Remote Code Execution (RCE), Privilege Escalation (PrivEsc), and Authentication Bypass. By incorporating threat actor data from multiple sources, the agent not only detects but also anticipates which vulnerabilities ransomware groups will target next, helping organizations stay one step ahead of potential attacks.

Zero-Day Exploits: Identifying and Mitigating Emerging Threats

In addition to ransomware, the agent is designed to detect and assess zero-day exploits, which are especially challenging to defend against due to their stealthy nature. A zero-day exploit occurs when an attacker leverages a previously unknown vulnerability, one that vendors have not had the opportunity to patch. Phoenix Security's Threat-Centric AI Agent works to identify these vulnerabilities early in their lifecycle, reducing the likelihood of successful exploitation.

Empowering Organizations to Take Action

What sets this new solution apart is its real-time adaptability and ability to integrate seamlessly with existing security infrastructure. The Threat-Centric Agent continuously monitors and adapts to the evolving threat landscape, ensuring that vulnerabilities are prioritized and addressed based on their real-time risk factor. By analyzing vulnerabilities in the context of real-world exploit data and business-critical assets, Phoenix's solution provides security leaders with the visibility they need to act quickly and decisively.

Continuous Threat Exposure Management (CTEM)

Phoenix Security's Threat-Centric Agent integrates with Continuous Threat Exposure Management (CTEM), a framework that ensures organizations can detect, assess, and respond to threats as they evolve. This integration allows for continuous vulnerability monitoring, ensuring

that as new vulnerabilities are discovered or exploits become active, organizations can adjust their remediation efforts without missing a beat.

A Powerful Suite of Tools for Comprehensive Coverage
The Threat-Centric Agent works in tandem with Phoenix's Reachability Analysis AI Agent and Blast Radius Analysis Copilot to provide a 360-degree approach to vulnerability management. This integration ensures that vulnerabilities are not only detected but also understood in the context of their impact across the entire network. By combining these tools, Phoenix Security offers businesses a unified solution that helps them respond proactively to emerging threats, ensuring rapid identification and remediation before exploits can cause significant harm.

Looking to the Future of Cybersecurity
Phoenix Security's Threat-Centric AI Agent is the next evolution in vulnerability management. By combining powerful AI with the proven 4D Risk Formula, this solution empowers security teams to identify and prioritize vulnerabilities with unparalleled accuracy. Early testing and more information are available at https://ai-threat.phoenix.security

Phil Moroni
Phoenix Security
+1 919-594-8888
email us here
Visit us on social media:
Facebook
X
LinkedIn
Instagram
YouTube
