Help Net Security newsletters Daily and weekly news, cybersecurity jobs, open source projects, breaking news – **subscribe here!**

Bitdefender. Introducing GravityZone PHASR LEARN MORE

Dan DeCloss, CTO, PlexTrac SPONSORED
June 26, 2025

How exposure-enriched SOC data can cut cyberattacks in half by 2028

Gartner projects that by 2028, organizations enriching their Security Operations Center (SOC) data with exposure insights will reduce the frequency and impact of cyberattacks by 50%. This bold forecast underscores a crucial shift: proactive exposure management is quickly becoming foundational to modern cyber defense.

Why organizations struggle to prioritize what matters

Security teams are responsible for defending an organization against looming cyber threats. Needless to say, they're inundated with data from constantly expanding attack surfaces. But what are teams supposed to do with all? Addressing thousands of vulnerabilities is far from realistic.

Enter the looming spiral of trying to pick the most critical vulnerabilities. Without real context, it's a struggle to identify the real threats, prioritize what matters most, and do so with speed and precision. Most teams lack sufficient environmental awareness and a clear understanding of asset to business mapping, threat intel, and additional business context to effectively prioritize in a timely manner, if at all.

More tools or manual testing just add noise. Teams may waste valuable resources chasing low-impact issues while critical threats go unaddressed. Time is inefficiently spent mapping ownership or assessing business impact while critical threats remain exploitable.

Bottom line: Detection alone isn't enough.

Detecting issues is only the beginning. Once identified, a strong proactive exposure management framework must be established to develop an understanding of where your weaknesses lie, which assets are business critical, what mitigating controls are in place, and how adversaries can exploit them.

Bridging the gap between reactive discovery and proactive exposure management through enriched security data is key to getting ahead of threats.

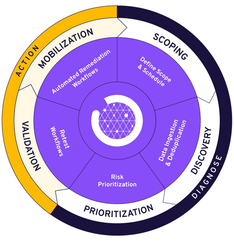
Exposure data: The context that powers risk-based decisions

Exposure data includes information from vulnerability scans, threat intelligence, attack paths, asset criticality, ownership, security control effectiveness, business goals and priorities, and more. Embedding this context into detection and response workflows is essential to enable risk-informed action.

Without this level of contextualization for decision-making, organizations have no way to effectively manage risk.

PlexTrac: Enriching security data with context for risk-based prioritization

PlexTrac can help organizations realize the vision of proactive exposure management, even if they are just starting out on their journey to aligning to the CTEM framework.



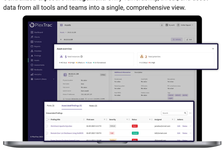
The PlexTrac platform bridges the gap between exposure management and operational response by enabling teams to consolidate all their security data in one platform. Built to support manual test data, PlexTrac acts as the security data hub so teams can identify, prioritize, and orchestrate remediation on the exposures that have the highest business impact.

With PlexTrac's risk-based prioritization engine, security teams can contextualize vulnerabilities with asset metadata, business criticality, exploitability, and threat intelligence. The result: a smarter, faster way to assign and remediate the most impactful issues.

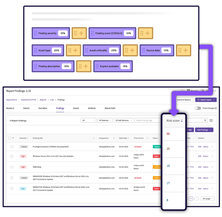
No more spreadsheet workflows. No more guessing. No more delays.

Key PlexTrac capabilities include:

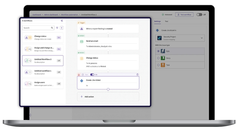
- **Centralized exposure management:** Unify vulnerability, threat, and asset data from all tools and teams into a single, comprehensive view.



- **Risk scoring and prioritization:** Automatically calculate risk to prioritize the most business-critical issues by leveraging fully-configurable risk scoring equations that factor in business context to support effective prioritization.



- **Automated remediation orchestration:** With the most critical issues prioritized, quickly track, assign and validate remediation efforts across your organization, automating orchestration to delay mean-time-to-remediation (MTTR).



An example of a contextualized workflow

Imagine a low-severity vulnerability is discovered during a Tenable scan that is ingested into PlexTrac. On its own, the issue might not raise alarms, but it has an active exploit and impacts a business-critical asset.

PlexTrac's risk scoring engine factors in the exploitability and business impact, automatically assigning a high custom risk score. This automatically triggers a workflow that:

- Escalates the finding
- Generates a Jira or ServiceNow ticket
- Alerts the asset owner or business unit for immediate triage

The ticket includes the exploit descriptions, patching details, asset details, risk score, and service level agreement.

Validation and remediation tracking is automated as well to ensure the issue has been effectively closed.

Value delivered by PlexTrac

Capability	Impact
Risk-based prioritization	Elevates threats based on exploitability, asset value, and threat intelligence.
Workflow automation	Instantly triggers and tracks remediation workflows.
Real-time collaboration	Provides a centralized, shared view across all teams.
End-to-end trackability	Logs and communicates every step from detection to resolution in a reportable format.

Schedule a personalized demo to see PlexTrac in action.

Measurably reduce risk over time

By proactively managing exposures with a contextual, risk-based approach, PlexTrac helps teams show measurable impact over time. Deliver clear metrics and evidence of how risk is decreasing to validate the impact of your security program.

A realistic roadmap to a 50% reduction in cyberattacks

Gartner's 2028 prediction isn't just aspirational. It's achievable for organizations that treat exposure enrichment as a strategic priority.

Many teams are just starting on their journey to realize this vision. With tools like PlexTrac, teams can enrich security data with asset ownership, risk scores, threat intel, known attack paths, and additional business context. This ensures critical issues are immediately addressed by surfacing them from the rest of the noise.

More about

cyberattacks | data | PlexTrac | risk | SOC

Featured news

NTLM relay attacks are back from the dead

Africa's cybersecurity crisis and the push to mobilizing communities to safeguard a digital future

You can't trust AI chatbots not to serve you phishing pages, malicious downloads, or bad code

Product showcase: Smarter pentest reporting and exposure management with PlexTrac

Resources

Download: Edgescan 2025 Vulnerability Statistics Report

Enzoic AD Life Password Audit Report

Report: Fortune 500 employee-linked account exposure

Don't miss

NTLM relay attacks are back from the dead

Africa's cybersecurity crisis and the push to mobilizing communities to safeguard a digital future

Google open-sources privacy tech for age verification

You can't trust AI chatbots not to serve you phishing pages, malicious downloads, or bad code

Cisco fixes maximum-severity flaw in enterprise unified comms platform (CVE-2025-20309)

CYBERSECURITY NEWS

HNS Daily
Daily newsletter sent Monday-Friday

HNS Newsletter
Weekly newsletter sent on Mondays

InSecure Newsletter
Editor's choice newsletter sent twice a month

Breaking news
Periodical newsletter released when there is breaking news

Cybersecurity jobs
Weekly newsletter listing new cybersecurity job positions

Open source
Monthly newsletter focusing on open source cybersecurity tools

Please enter your e-mail address Subscribe

I have read and agree to the terms & conditions

© Copyright 1998-2025 by Help Net Security