

Context Is Key

What is contextual risk prioritization and why is it a game changer for your offensive security program?



Context Is Key

What is contextual risk prioritization and why is it a game changer for your offensive security program?

Imagine if you could go beyond pentest management and reporting and vulnerability tracking and into a more programmatic area of risk. With contextual risk-based prioritization of findings, you can close the loop on the continuous validation and start showing quantifiable progress on your security posture, or your client’s security posture, over time.

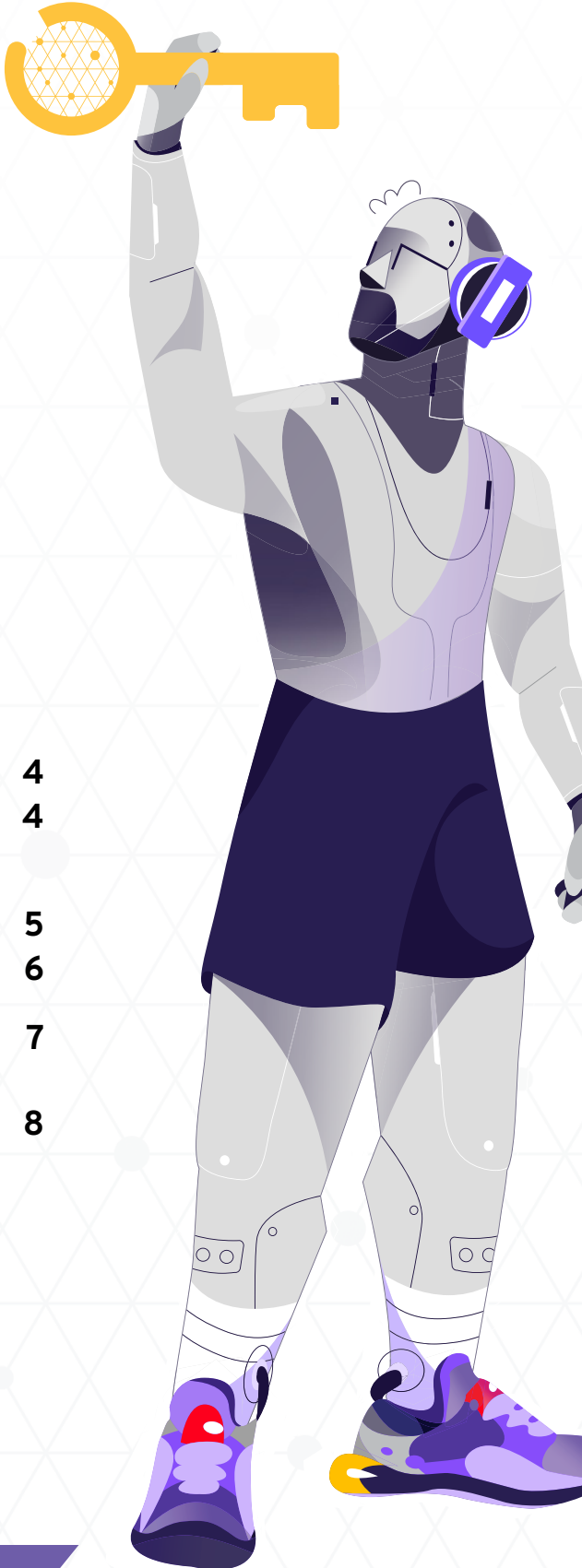



Table of Contents

- The Golden Key: Context-Based Scoring** 4
 - What is the Common Vulnerability Scoring System (CVSS)? 4
- Unlock Your Potential: PlexTrac Priorities** 5
 - How does Priorities work? 6
- Key Players: PlexTrac Priorities Versus Competitor Offerings** 7
 - How does Priorities stack up against traditional risk assessment methods? 8



Remediating vulnerabilities is the key to improving your security posture or your stakeholder's security posture. But with endless vulnerabilities coming in from different sources – vulnerability scans, red team assessments, pentest, risk assessments, etc. – it's hard to know which vulnerabilities to tackle first.

This is where context-based scoring comes in handy.

The Golden Key: Context-Based Scoring

Simply put, context-based scoring is a configurable scoring equation that measures vulnerabilities against a set of selected criteria – such as asset criticality, finding severity, tags, etc. – where each variable may have a weight applied to influence the contextual score and determine the true impact an issue could potentially have on the business. It goes beyond the industry-standard Common Vulnerability Scoring System (CVSS), considering the unique needs of the given organization.

What is the Common Vulnerability Scoring System (CVSS)

Common Vulnerabilities and Exposures (CVEs) is a glossary that tracks and glossaries common vulnerabilities in consumer hardware and software. Maintained by the MITRE Corporation, vulnerabilities are cataloged using the Security Content Automation Protocol (SCAP) and assigned a unique identifier. Identified vulnerabilities are analyzed by the National Institute of Standards and Technology (NIST), and then listed in NIST's National Vulnerability Database (NVD).

The Common Vulnerability Scoring System (CVSS) is used to rank CVEs on severity. The scale, which goes from 0-10, determines if a vulnerability's severity if exploited is low, medium, high, or critical.

“PlexTrac’s new risk-based prioritization capabilities will help us shift from point-in-time testing to more continual engagements – enabling us to provide deeper value to each client by customizing a contextual risk scoring equation that clearly communicates their highest impact risks on an ongoing basis.”

– *Dahvid Schloss, Director of Offensive Security, Echelon Risk + Cyber*



Unlock Your Potential: PlexTrac Priorities

PlexTrac Priorities is part of our industry-leading automated platform. It's the industry's first configurable contextual scoring engine that empowers security service providers and enterprises to:

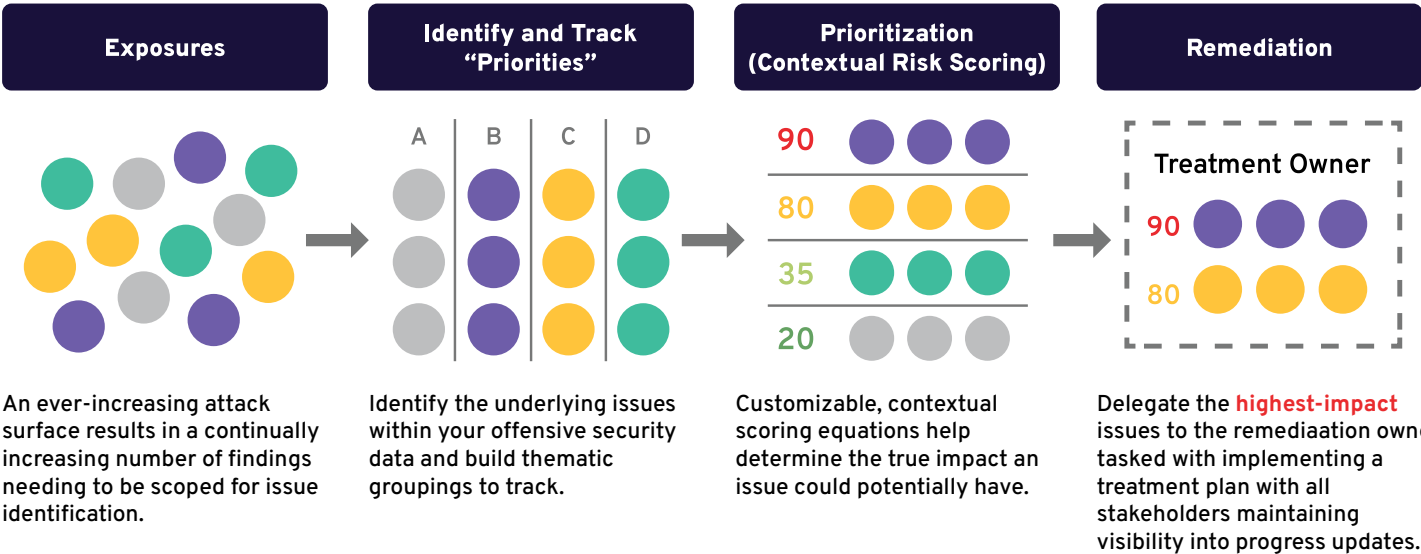
- ✓ ***Prioritize risks based on real impact***
Ditch generic scoring and tailor it to your unique risk tolerance or industry-specific needs.
- ✓ ***Automate workflows***
Streamline processes from assessment to remediation for maximum efficiency.
- ✓ ***Identify underlying issues***
Unearth patterns in your data to prevent future vulnerabilities from recurring.
- ✓ ***Demonstrate value from your continuous validation efforts***
Prove the effectiveness of your security program with continuous risk reduction.



How does Priorities work?

With our Priorities feature, you can create a set of business priorities to address – like Simple Network Management Protocol (SNMP) weaknesses – and link findings and assets to a designated priority. Our contextual scoring engine then calculates a risk score based on the corporate risk equation that your organization, or client’s organization, sets. If different departments, or different clients, need a separate risk equation, you can easily update the criteria.

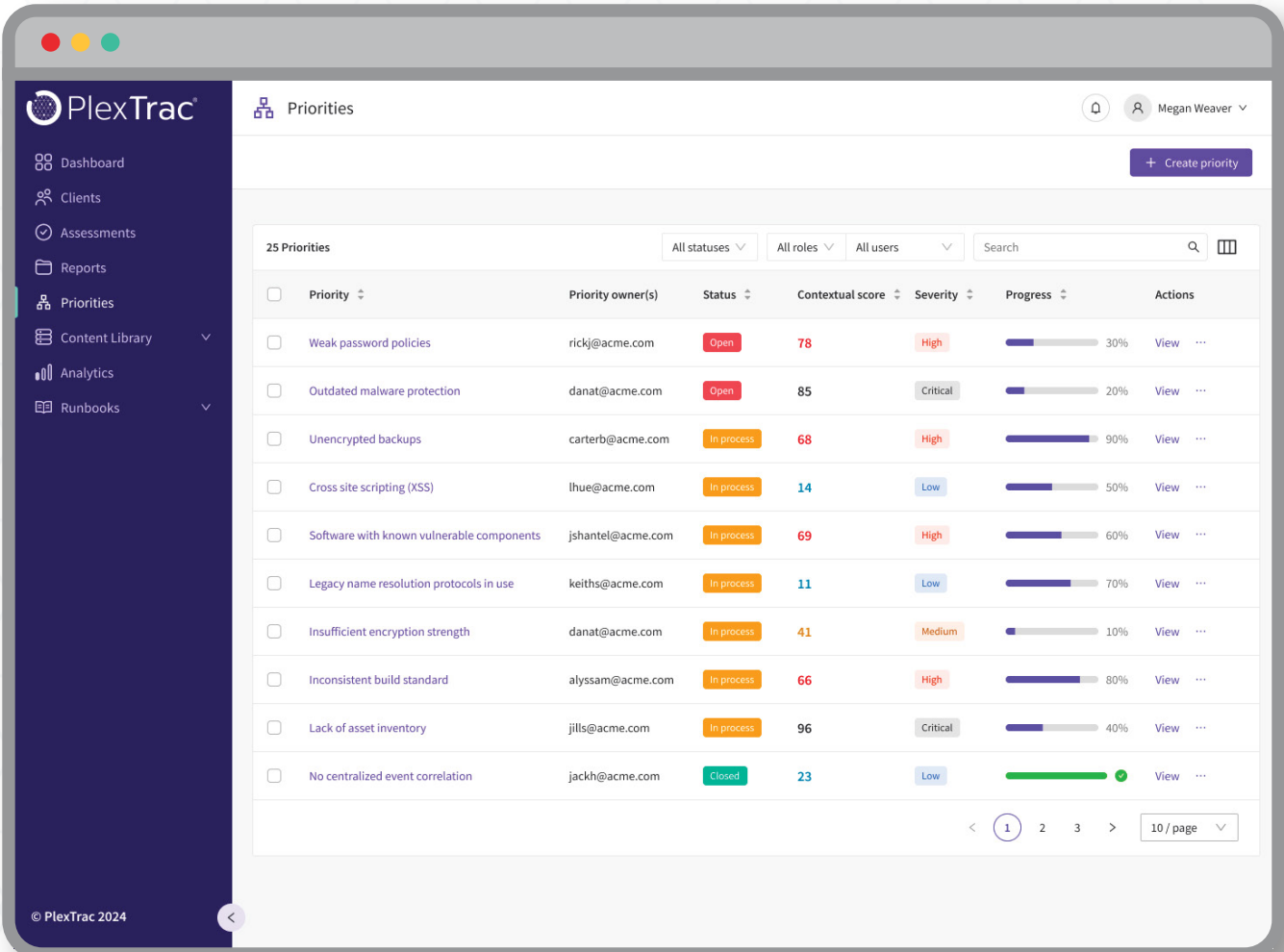
PlexTrac Priorities enables you to pinpoint the fixes that will make the greatest impact on your security posture, or your client’s security posture, without the need for additional resources. Best of all, you can set a treatment plan, assign owners to remediate the findings, set due dates, and track progress.



Key Players: PlexTrac Priorities Versus Competitor Offerings

As of today, PlexTrac Priorities is the only true configurable context-based scoring engine on the market. Other solutions in the space offer limited configurability and don't provide the same level of visibility into risk factors. In other words, they don't provide the level of detail needed to confidently prioritize remediation efforts.

Competitive offerings also lack the real-time visibility offered with Priorities. With Priorities, key stakeholders can follow the progress of risks in a continuous fashion and see a measurable reduction over time.



How does Priorities stack up against traditional risk assessment methods?

Use Case	Without Priorities	With Priorities
Prioritizing risk based on business needs	Leverage CVSS scores, but they don't take unique business needs into account. This can lead to ineffective prioritization and wasted effort on high-criticality issues with low business impact.	Group vulnerabilities/assets and apply contextualization into the scoring equation to determine the true impact an issue could potentially have on the business. Leveraging data-backed prioritization ensures efforts are spent on the issues that pose the largest organizational risk.
Maximizing the impact of remediation efforts with limited resources	There's not enough time to patch and implement threat-prevention measures for every vulnerability, especially with limited resources. And without a way to prioritize risks that will have the highest impact on a given business, you could waste time – or worse – impactful vulnerabilities could be exploited.	Tracking thematic groupings of vulnerabilities and scoring risk with additional context – such as asset criticality, finding criticality, tags, etc.– enables the identification of true risk, allowing a team of limited resources to prioritize remediation of the highest impact issues. This evidence-based approach to prioritization can significantly reduce the possibility of a breach.
Tracking the remediation of critical flaws	Without a platform to house all of your data from vulnerability scans, red team assessments, pentest, risk assessments, etc., you either need to work out of multiple tools or manually aggregate data on spreadsheets that quickly become outdated. This makes it challenging to effectively prioritize risks and track remediation	With one central, web-based location to aggregate all offensive security data, like PlexTrac, you can seamlessly tag and group findings, assign fixes, and track remediation with all stakeholders maintaining visibility into progress.
Showing a measurable risk reduction	You might be able to show a point-in-time analysis of your risk posture, but competitor offerings do not offer real-time visibility. And without the ability to prioritize risks based on business impact, the risk reduction will likely be less significant compared to PlexTrac Priorities users.	PlexTrac Priorities enables you to show progress in real time. Your key stakeholders can see the priorities you've set, progress being made to impactful findings, and risk reduction over time.

Your Key to Success Is Waiting to Be Claimed

If you're ready to improve your security posture, or your client's security posture, request a demo of PlexTrac Priorities.

Claim Your Key to Success >>



PlexTrac, the market leader in pentest reporting and management, allows MSSP and Enterprise customers to extend beyond pentesting by streamlining critical offensive security workflows as part of a continuous validation strategy. With PlexTrac, security teams can aggregate offensive security data from multiple sources, prioritize risk with the industry's first fully configurable contextual scoring engine, and close the loop on continuous validation with measurable risk reduction.

www.plextrac.com



© 2024 PlexTrac, Inc., all rights reserved.

