PlexTrac

Tracking the signal through noise

How do you track cybersecurity issues?

Internal and External Penetration Tests, Vulnerability Scans, Compliance and Regulatory Assessments, Physical Security Assessments, Bug Bounties, Incident Response, etc. Different formats, reporting templates and delivery methodologies further complicate the process.

How do threat details get to the Blue Team?

The traditional Red and Blue team approach often limits communication and collaboration. Blue teams are left with Word and PDF based documentation and limited details of the threats and vulnerabilities uncovered by the Red Team engagement. Remediation is thus reactive at best.

How do you communicate cybersecurity progress?

More than ever, cybersecurity is a C-Level topic of conversation. But, legacy reporting tools provide limited details on the real activities, analytics and trends taking place and the reporting process is siloed and inconsistent. Up to date, comprehensive detail is hard to cobble together from multiple sources.

PlexTrac

PlexTrac Brings Order

Aggregate

PlexTrac aggregates and consolidates findings from all types of Red Teaming activities into a single, web-based, platform. From one platform, have all the details on each component of your cybersecurity operations, in near real time, with standardized detail, reporting and dashboards.

Remediate

PlexTrac facilitates Red and Blue team communication and collaboration, from finding through remediation. Keep comprehensive finding details, running narratives on redemption progress, and share unparalleled levels of detail about threats and vulnerabilities ensure advancing cybersecurity posture.

Communicate

PlexTrac provides organization wide reporting and graphical dashboards on the comprehensive cybersecurity posture of the organization. Communicate with stakeholders, share reports and analytics, and convey details with one consolidated, web-based platform.