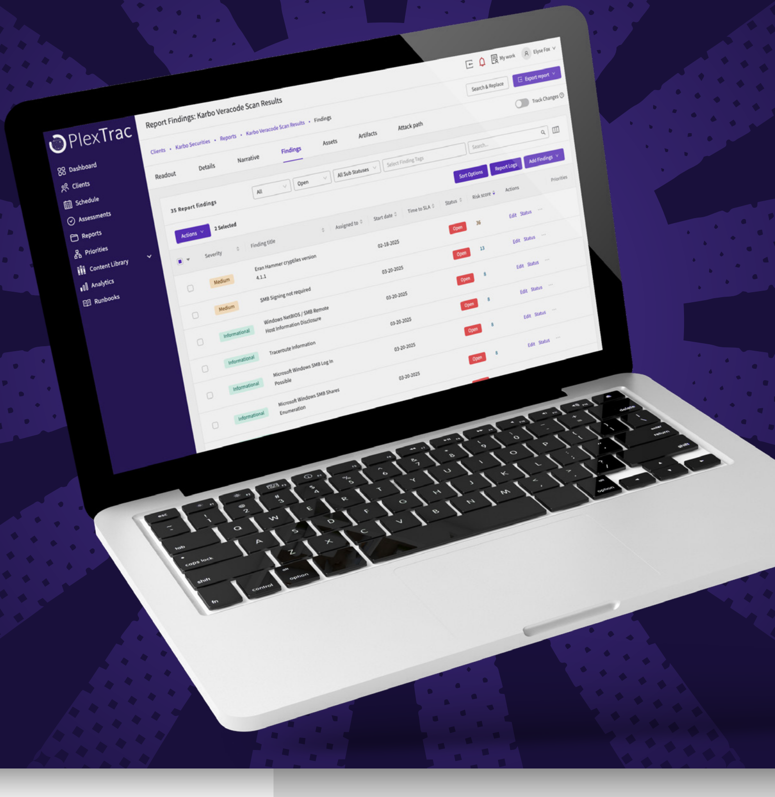
PlexTrac®



The #1 Pentest Reporting and Threat Exposure Management Platform

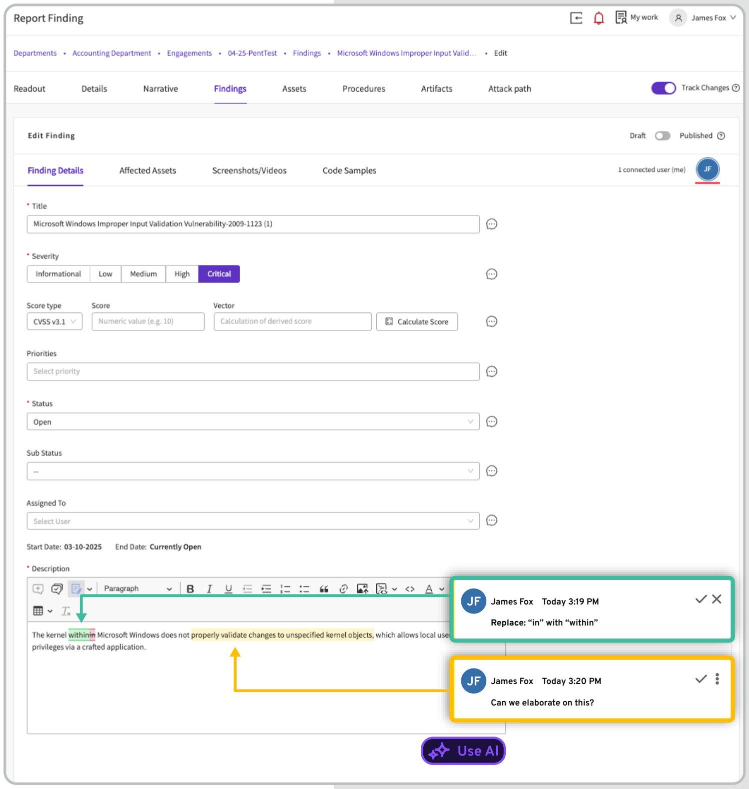
Introducing the PlexTrac platform

Leverage the #1 AI-powered platform for reducing threat exposure by centralizing security data, streamlining pentest reporting, prioritizing risks based on business impact, and automating remediation workflows.

Key Features

AI-powered pentest reporting

Streamline and automate the end-to-end *pentesting* lifecycle from scope to final delivery. Tool integrations, reusable content, AI, real-time collaborative QA workflows, and automated report generation enable teams to work faster and more efficiently. This helps scale testing operations with existing resources, while delivering more impactful end results.



Report Finding

Edit Finding

* Title: Microsoft Windows Improper Input Validation Vulnerability-2009-1123 (1)

* Severity: Informational | Low | Medium | High | **Critical**

Score type: CVSS v3.1

Score: Numeric value (e.g. 10)

Vector: Calculation of derived score

Priorities: Select priority

* Status: Open

Sub Status: --

Assigned To: Select User

Start Date: **03-10-2025** End Date: **Currently Open**

* Description

The kernel within~~in~~ Microsoft Windows does not properly validate changes to unspecified kernel objects, which allows local use privileges via a crafted application.

JF James Fox Today 3:19 PM

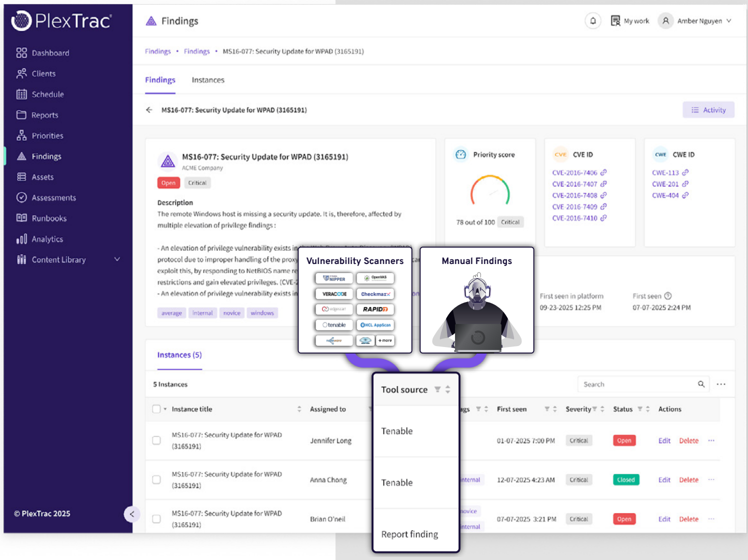
Replace: “in” with “within”

JF James Fox Today 3:20 PM

Can we elaborate on this?

Discover and consolidate issues from all testing

Consolidate security data from manual testing and ***automated discovery tools*** into PlexTrac—your control center hub for identifying issues, managing exposures, and coordinating remediation. This centralized approach improves collaboration, accelerates decision-making, streamlines workflows, and enables teams to more quickly action security issues.



MS16-077: Security Update for WPAD (3165191)

MS16-077: Security Update for WPAD (3165191)
ACME Company
Open · Critical

Description
The remote Windows host is missing a security update. It is, therefore, affected by multiple elevation of privilege findings :

- An elevation of privilege vulnerability exists in
protocol due to improper handling of the proxy
exploit this, by responding to NetBIOS name re
restrictions and gain elevated privileges. (CVE-
- An elevation of privilege vulnerability exists in

average · internal · novice · windows

Priority score: 78 out of 100 · Critical

CVE ID: CVE-2016-7406, CVE-2016-7407, CVE-2016-7408, CVE-2016-7409, CVE-2016-7410

CWE ID: CWE-113, CWE-201, CWE-404

First seen in platform: 09-23-2025 12:25 PM

First seen: 07-07-2025 2:24 PM

Instances (5)

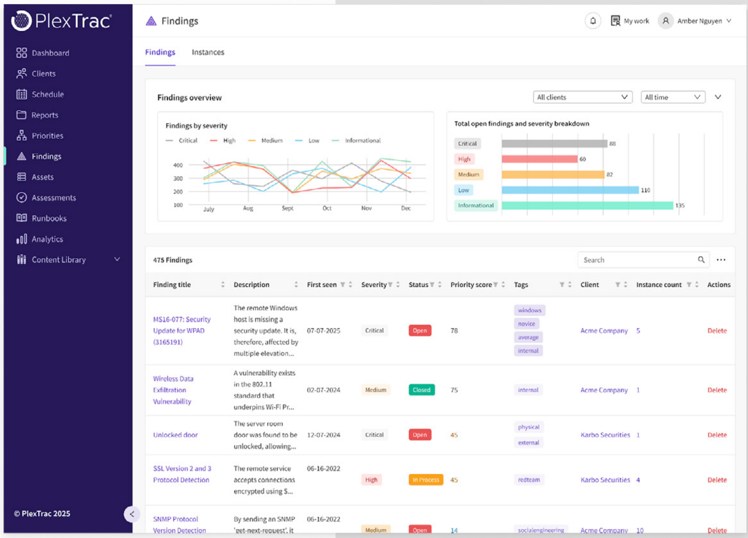
5 Instances

Search

Instance title	Assigned to	Tool source	Tags	First seen	Severity	Status	Actions
MS16-077: Security Update for WPAD (3165191)	Jennifer Long	Tenable		01-07-2025 7:00 PM	Critical	Open	Edit Delete ···
MS16-077: Security Update for WPAD (3165191)	Anna Chong	Tenable	internal	12-07-2025 4:23 AM	Critical	Closed	Edit Delete ···
MS16-077: Security Update for WPAD (3165191)	Brian O'neil	Report finding	novice internal	07-07-2025 3:21 PM	Critical	Open	Edit Delete ···

Manage exposures across your attack surface

By centralizing security data management, you can effectively ***manage threat exposures*** across your entire attack surface by viewing all findings and their associated assets, or all findings and their instances. Continuously assess your consolidated data and better communicate risk across your organization.



Severity	Open findings
Critical	88
High	60
Medium	82
Low	110
Informational	135

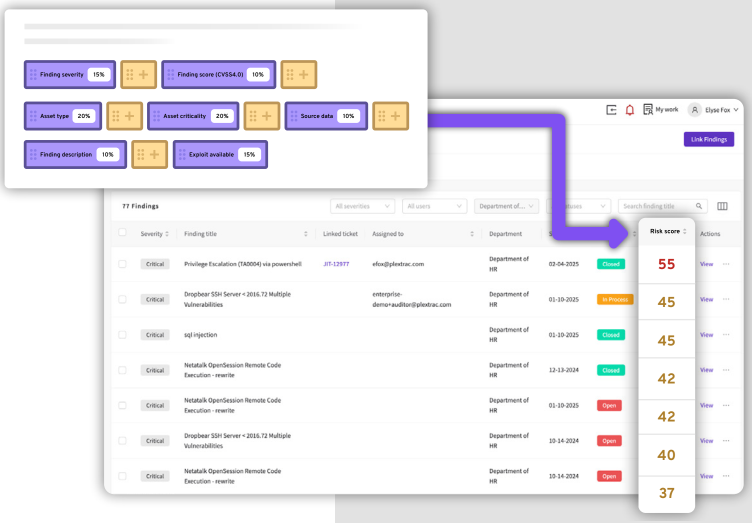
475 Findings

Search

Finding title	Description	First seen	Severity	Status	Priority score	Tags	Client	Instance count	Actions
MS16-077: Security Update for WPAD (3165191)	The remote Windows host is missing a security update. It is, therefore, affected by multiple elevation...	07-07-2025	Critical	Open	78	windows novice average internal	Acme Company	5	Delete
Wireless Data Exfiltration Vulnerability	A vulnerability exists in the 802.11 standard that underpins Wi-Fi Pr...	02-07-2024	Medium	Closed	75	internal	Acme Company	1	Delete
Unlocked door	The server room door was found to be unlocked, allowing...	12-07-2024	Critical	Open	45	physical external	Karbo Securities	1	Delete
SSL Version 2 and 3 Protocol Detection	The remote service accepts connections encrypted using S...	06-16-2022	High	In Process	45	redteam	Karbo Securities	4	Delete
SNMP Protocol Version Detection	By sending an SNMP 'get-next-request', it	06-16-2022	Medium	Open	14	socialengineering	Acme Company	10	Delete

Automatically prioritize risk by business-impact

Build cyber risk scoring equations that leverage your specific business context to automatically ***prioritize remediation*** efforts based on true risk impact across your consolidated security data. Risk scoring may be applied at the individual finding level or across groups of thematic findings.

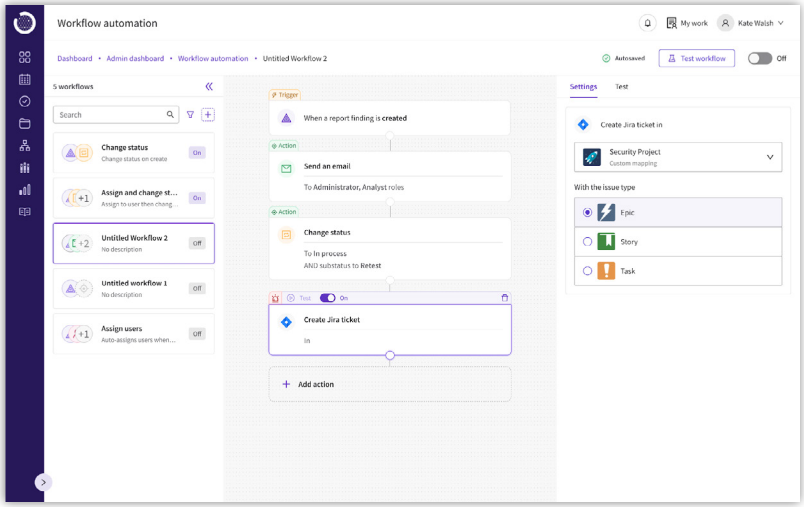


77 Findings

Severity	Finding title	Linked ticket	Assigned to	Department			Risk score	Actions
Critical	Privilege Escalation (TA0004) via powershell	JIT-12977	efox@plextrac.com	Department of HR	02-04-2025	Closed	55	View ···
Critical	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities		enterprise-demo+auditor@plextrac.com	Department of HR	01-10-2025	In Process	45	View ···
Critical	sql injection			Department of HR	01-10-2025	Closed	45	View ···
Critical	Netatalk OpenSession Remote Code Execution - rewrite			Department of HR	12-13-2024	Closed	42	View ···
Critical	Netatalk OpenSession Remote Code Execution - rewrite			Department of HR	01-10-2025	Open	42	View ···
Critical	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities			Department of HR	10-14-2024	Open	40	View ···
Critical	Netatalk OpenSession Remote Code Execution - rewrite			Department of HR	10-14-2024	Open	37	View ···

Automate remediation and validation orchestration

Speed mobilization and eliminate manual tasks by building automated, rule-based workflows triggered by events, such as a new critical finding emerging. Automatically create a Jira ticket, send an email alert, post to a Slack channel, auto-assign the finding, and more.


Workflow automation

Dashboard • Admin dashboard • Workflow automation • Untitled Workflow 2

5 workflows

Workflow	Description	State
Change status	Change status on create	On
Assign and change st…	Assign to user then chang…	On
Untitled Workflow 2	No description	Off
Untitled workflow 1	No description	Off
Assign users	Auto-assigns users when…	Off

Trigger: When a report finding is created

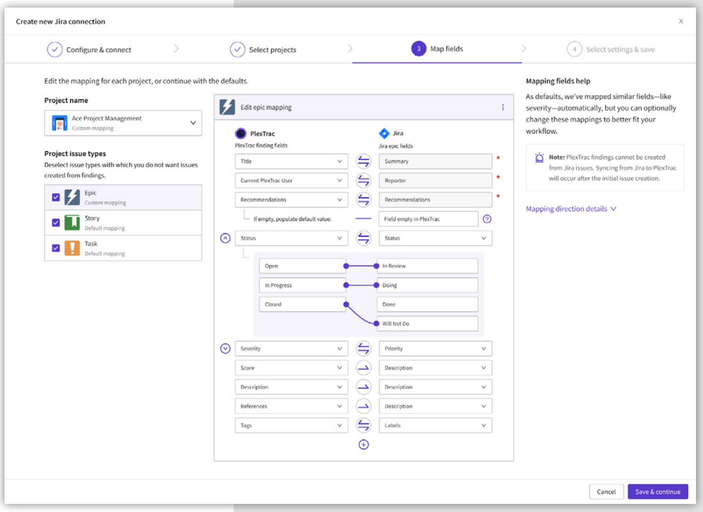
Action: Send an email — To Administrator, Analyst roles

Action: Change status — To In process AND substatus to Retest

Test ● On: Create Jira ticket — In

Settings: Create Jira ticket in Security Project (Custom mapping)

With the issue type:
- ● Epic
- ○ Story
- ○ Task


Create new Jira connection

Configure & connect › Select projects › 3 Map fields › 4 Select settings & save

Edit the mapping for each project, or continue with the defaults.

Project name: Ace Project Management (Custom mapping)

Project issue types
Deselect issue types with which you do not want issues created from findings.

- ☑ Epic — Custom mapping
- ☑ Story — Default mapping
- ☑ Task — Default mapping

Edit epic mapping

PlexTrac finding fields		Jira epic fields
Title	⇆	Summary *
Current PlexTrac User	⇆	Reporter *
Recommendations	⇆	Recommendations *
If empty, populate default value:	—	Field empty in PlexTrac
Status	⇆	Status
Open	—	In Review
In Progress	—	Doing
		Done
Closed	—	Will Not Do
Severity	⇆	Priority
Score	→	Description
Description	→	Description
References	→	Description
Tags	⇆	Labels

Mapping fields help

As defaults, we've mapped similar fields—like severity—automatically, but you can optionally change these mappings to better fit your workflow.

Note: PlexTrac findings cannot be created from Jira issues. Syncing from Jira to PlexTrac will occur after the initial issue creation.

To help organizations stay ahead of the evolving threat landscape, PlexTrac delivers a comprehensive solution that enables both enterprises and Managed Security Service Providers (MSSPs) to streamline security operations, unify cross-functional teams within a centralized platform, strengthen threat exposure management, and demonstrate measurable improvements in their overall security posture.

Benefits

Use PlexTrac as a data control center

Use PlexTrac as the control center and point-of-truth to streamline and automate security workflows across your entire cybersecurity program.

Achieve continuous validation with contextual risk prioritization

Ensure high risk findings discovered during ongoing testing are automatically prioritized based on business impact and quickly actioned to prevent risk recurrence.

Speed pentesting and offensive engagements by up to 75%

Complete more engagements in less time by streamlining and automating the end-to-end pentesting lifecycle while delivering more impactful end results.

Reduce Risk

Centralize security data, contextually prioritize risk, and automate remediation workflows for ongoing, more effective threat management to measurably reduce risk.

Detailed Capabilities

Discover issues through manual testing and automated tools

Execute manual pentesting, adversary emulation, and other offensive assessments within PlexTrac. Consolidate your manual test data along with ingested data from all your security tools and scanners via a wide range of platform integrations.

AI-powered pentest reporting

- Schedule new engagements and manage inbound requests with a calendar overview of each team member's capacity.
- Ensure consistent coverage by creating your own or using 500+ pre-built procedures mapped to MITRE ATT&CK for executing repeatable, step-by-step test plans.
- Visualize tactics, techniques and procedures coverage to identify gaps and areas of focus.
- Create visual attack path representations of the tactics, techniques, and procedures (TTPs) used.
- Report-as-you-go in a platform built for your workflow, documenting screenshots, code samples, videos, and more throughout your testing.
- Use AI to auto-generate descriptions and remediation steps and analyze report data to summarize key themes for your narratives.
- Speed reporting by saving narratives and writeups for reuse or pull from a pre-built repository of over 25,000 CWEs, CVEs, and KEVs.
- Use Google-doc like quality assurance (QA) workflows for real-time collaboration with editing, commenting, and change tracking.
- Customize reports at scale with no-code style guides and configurable layouts.
- Present your security findings in the method – and with the branding and formatting – that your organization requires with little to no code.
- Streamline the findings handoff with automated workflows and bi-directional Jira and ServiceNow integrations.

Recognize Immediate Value

75%
Shorter Reporting Cycle

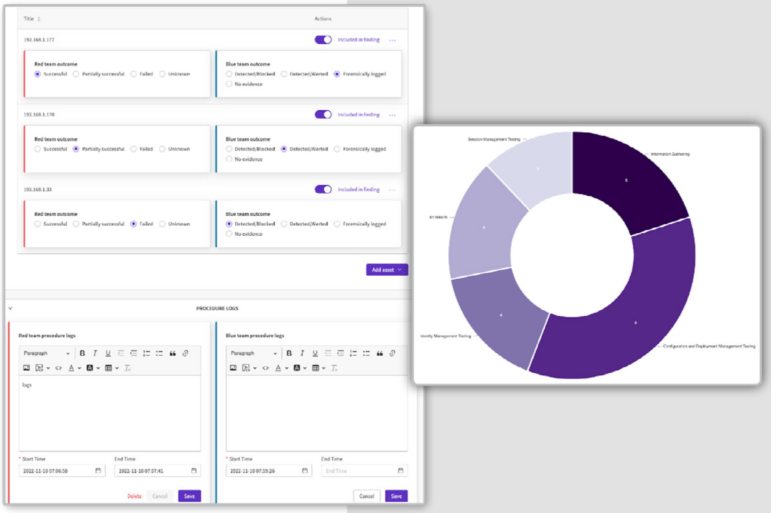
5X
ROI in Year One

30%
Increase in Efficiency

25K
CVE, CWE, and KEV Findings Writeups

Adversary emulation and tabletop exercises

- Execute side-by-side test plans to ensure consistent testing, support junior testers, and demonstrate progress over time with iterative testing.
- Create your own custom procedures or leverage 500+ pre-built procedures mapped to MITRE ATT&CK to align test coverage to your framework of choice.



Title | Actions

192.168.1.177 — Included in finding

Red team outcome: ● Successful ○ Partially successful ○ Failed ○ Unknown

Blue team outcome: ○ Detected/Blocked ○ Detected/Alerted ● Forensically logged ○ No evidence

192.168.1.170 — Included in finding

Red team outcome: ○ Successful ● Partially successful ○ Failed ○ Unknown

Blue team outcome: ○ Detected/Blocked ● Detected/Alerted ○ Forensically logged ○ No evidence

192.168.1.33 — Included in finding

Red team outcome: ○ Successful ○ Partially successful ● Failed ○ Unknown

Blue team outcome: ● Detected/Blocked ○ Detected/Alerted ○ Forensically logged ○ No evidence

PROCEDURE LOGS

Red team procedure logs

logs

* Start Time: 2022-11-10 07:06:58 — End Time: 2022-11-10 07:07:41

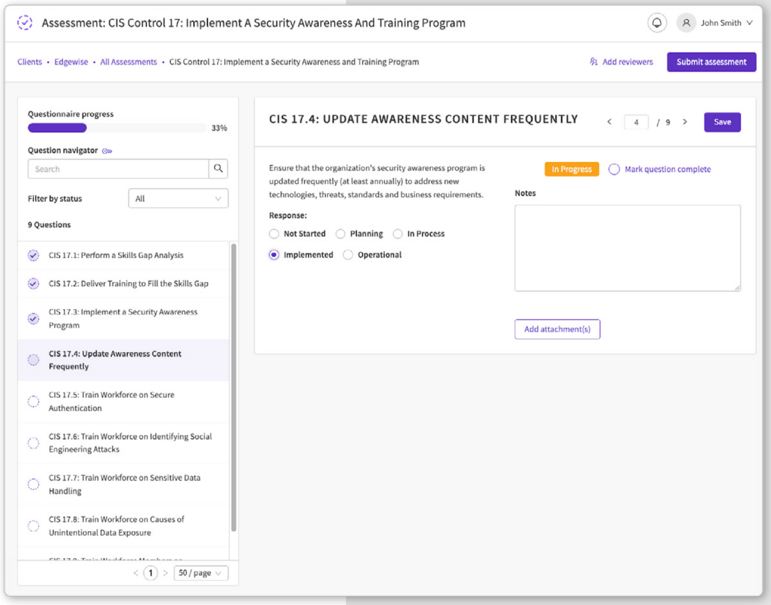
Blue team procedure logs

* Start Time: 2022-11-10 07:59:26 — End Time: End Time

Add asset
Paragraph
Delete
Cancel
Save
Session Management Testing
3
Information Gathering
5
A1788678
4
Identity Management Testing
4
Configuration and Deployment Management Testing
9

Framework-based assessments and questionnaires

- Create questionnaires based on common frameworks, such as CMMC 2.0, or build custom assessments to identify risks unique to your organization using customizable radio buttons, multiple choice and free response questions.
- Perform assessments in an easy-to-navigate environment built for your workflow.
- Pre-populate information to streamline assessment completion.



Assessment: CIS Control 17: Implement A Security Awareness And Training Program

Clients • Edgewise • All Assessments • CIS Control 17: Implement a Security Awareness and Training Program

Questionnaire progress 33%

Question navigator

Filter by status: All

9 Questions

- ✓ CIS 17.1: Perform a Skills Gap Analysis
- ✓ CIS 17.2: Deliver Training to Fill the Skills Gap
- ✓ CIS 17.3: Implement a Security Awareness Program
- ○ **CIS 17.4: Update Awareness Content Frequently**
- ○ CIS 17.5: Train Workforce on Secure Authentication
- ○ CIS 17.6: Train Workforce on Identifying Social Engineering Attacks
- ○ CIS 17.7: Train Workforce on Sensitive Data Handling
- ○ CIS 17.8: Train Workforce on Causes of Unintentional Data Exposure

CIS 17.4: UPDATE AWARENESS CONTENT FREQUENTLY — 4 / 9

Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards and business requirements.

In Progress ○ Mark question complete

Response:

○ Not Started ○ Planning ○ In Process

● Implemented ○ Operational

Notes

Ingest data from automated security tools

- Ingest security data from a wide range of API integrations, file import integrations, or CSV import.
- Keep your data clean by automatically deduplicating findings from tool integrations.
- Create rule-based actions to map findings ingested from security tools to be replaced with your own custom writeup verbiage, adjust the severity, or choose to ignore.
- Customize your custom solutions by leveraging PlexTrac's open API to efficiently access and modify data within the platform.

Manage exposures across your attack surface

Continuously assess your attack surface by managing all consolidated data within PlexTrac. Better communicate risk with the ability to see all unique issues in your organization and group thematic issues into focus areas that may be delegated and tracked.

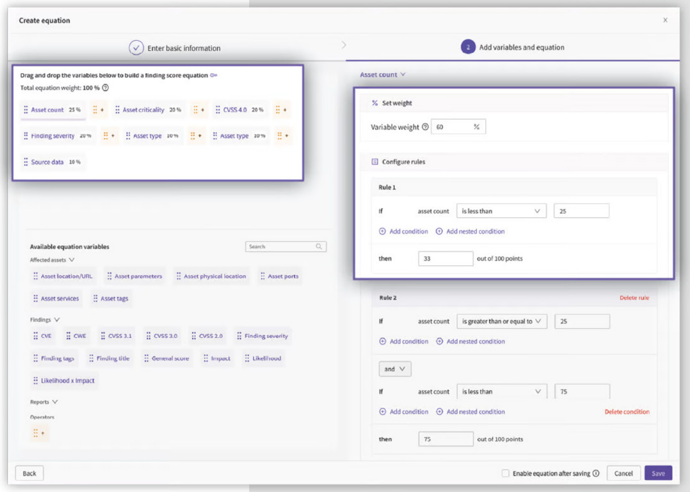
- Continuously assess your attack surface by managing exposures across your consolidated data with either a finding-first lens or an asset-first lens
- Enable asset owners to effectively manage their assigned assets with a view of all assets and their associated findings.
- Enable continuous validation with the ability to view and manage all findings and their instances across your assets.
- Identify and track the underlying issues introducing vulnerabilities into your environment by creating thematic groupings of vulnerabilities.
- Delegate and assign focus areas or thematic groupings to responsible owners and keep stakeholders informed with automated notifications and progress tracking.

> "As our primary tool, everything we deliver comes out of PlexTrac and we are excited to leverage their risk-based prioritization features to further expand our existing offerings into more strategic services. PlexTrac's contextual risk scoring engine streamlines and adds logic into our workflow to drive additional value for our clients by readily communicating their highest impact risks so they can focus in on these areas."
>
> **Qasim Ijaz**
> ***Offensive Security Director***
> ***Ideal Integrations***

Automatically prioritize risk by business impact

Automatically prioritize remediation across your consolidated security data with configurable risk scoring equations that leverage business context – enabling you to cut through the noise and quickly identify your most impactful risks.

- Automatically prioritize risk by building fully-configurable risk scoring equations that leverage business context such as asset criticality or asset type.
- Apply your contextual risk scoring equations across all individual findings or groups of findings to auto-generate a risk score based on business impact.



Create equation

Enter basic information | 2 Add variables and equation

Drag and drop the variables below to build a finding score equation

Total equation weight: 100 %

Asset count 25 % + Asset criticality 20 % + CVSS 4.0 20 % + Finding severity 20 % + Asset type 10 % + Asset type 10 % + Source data 10 %

Asset count

Set weight

Variable weight: 60 %

Configure rules

Rule 1

If asset count is less than 25

then 33 out of 100 points

Rule 2

If asset count is greater than or equal to 25

and

If asset count is less than 75

then 75 out of 100 points

Automate remediation & validation orchestration with rule-based workflows

Replace manual triage processes with automated, repeatable workflows to speed mobilization and accountability, and reduce mean time to remediation (MTTR).

- Build rule-based workflows to trigger automated actions—such as creating tickets in Jira or ServiceNow,send email alerts, auto-assign findings, update finding status—when critical findings are detected.
- Seamlessly track remediation and validation with bi-directional integrations with Jira and ServiceNow
- Use webhooks to enable custom workflows for various in-platform event triggers.

Dynamic analytics and web-based results delivery

Access real-time insights to make data-driven decisions and communicate risk effectively with powerful visuals to compare trends and demonstrate ROI from continuous validation efforts. Customize dynamic dashboards for any audience.

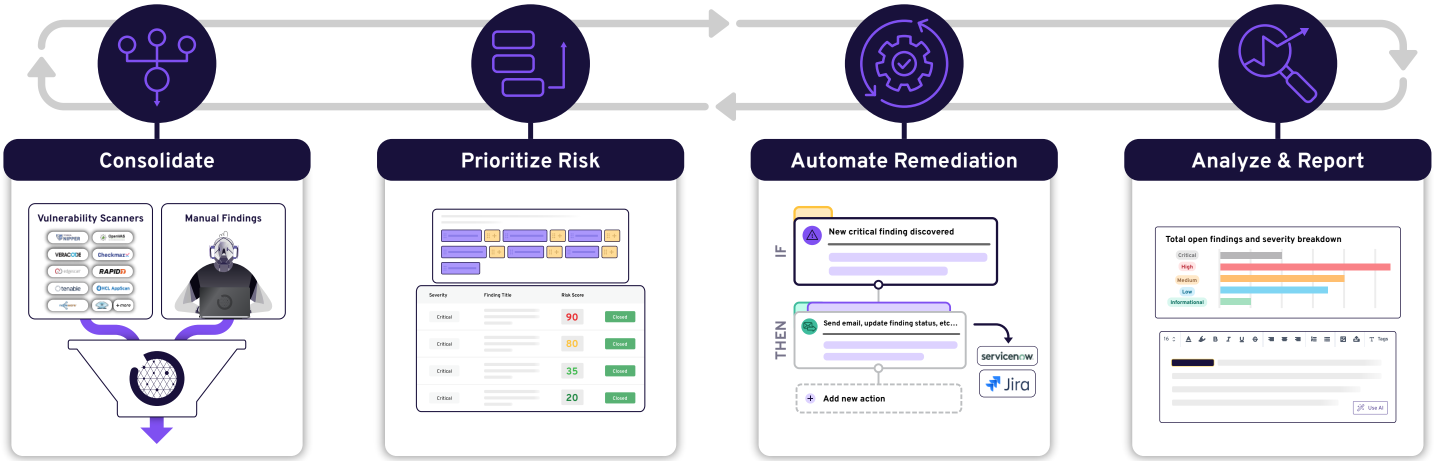
- Deliver role-based access to a web-based portal to keep all cross-functional stakeholders informed on progress updates and status.
- Drill into dynamic, interactive dashboard analytics with click-through functionality so you can make fast, informed decisions.
- Simplify reporting for stakeholders with easy-to-understand visuals to help communicate the status of risk and progress.
- Create preset views to communicate aspects of your security posture by department, client, date, specific assets, severity, CVE, status, assignee and more.

Deployment

PlexTrac offers multiple deployment options, including multitenant cloud, private instances, or on-premises using Docker containers.

- PlexTrac's multitenant cloud SaaS platform enables your team to get started right away without provisioning a new server.
- For enhanced security protection, PlexTrac offers private instances to ensure your data is segregated from other tenants and enables you to host the application under your own subdomain.
- For those that want maximum control of their data, PlexTrac offers the ability to deploy on-premises using Docker containers. Client hosting enables you to deploy in your selected environment, whether in a physical data center or through a cloud solution.

Adopt a dynamic and continuous approach to security with PlexTrac



Ready to see PlexTrac for CTEM in action?
Request a demo: plextrac.com/demo

PlexTrac is the market leader in pentest reporting and management, empowering MSSPs and enterprises to automate and streamline their Continuous Threat Exposure Management (CTEM) lifecycle. Our platform enhances the entire risk management workflow — from identifying and prioritizing risks in a business context to tracking remediation progress and measuring security posture trends with real-time analytics.

Discover how PlexTrac can revolutionize your security operations at:
www.plextrac.com

PlexTrac®