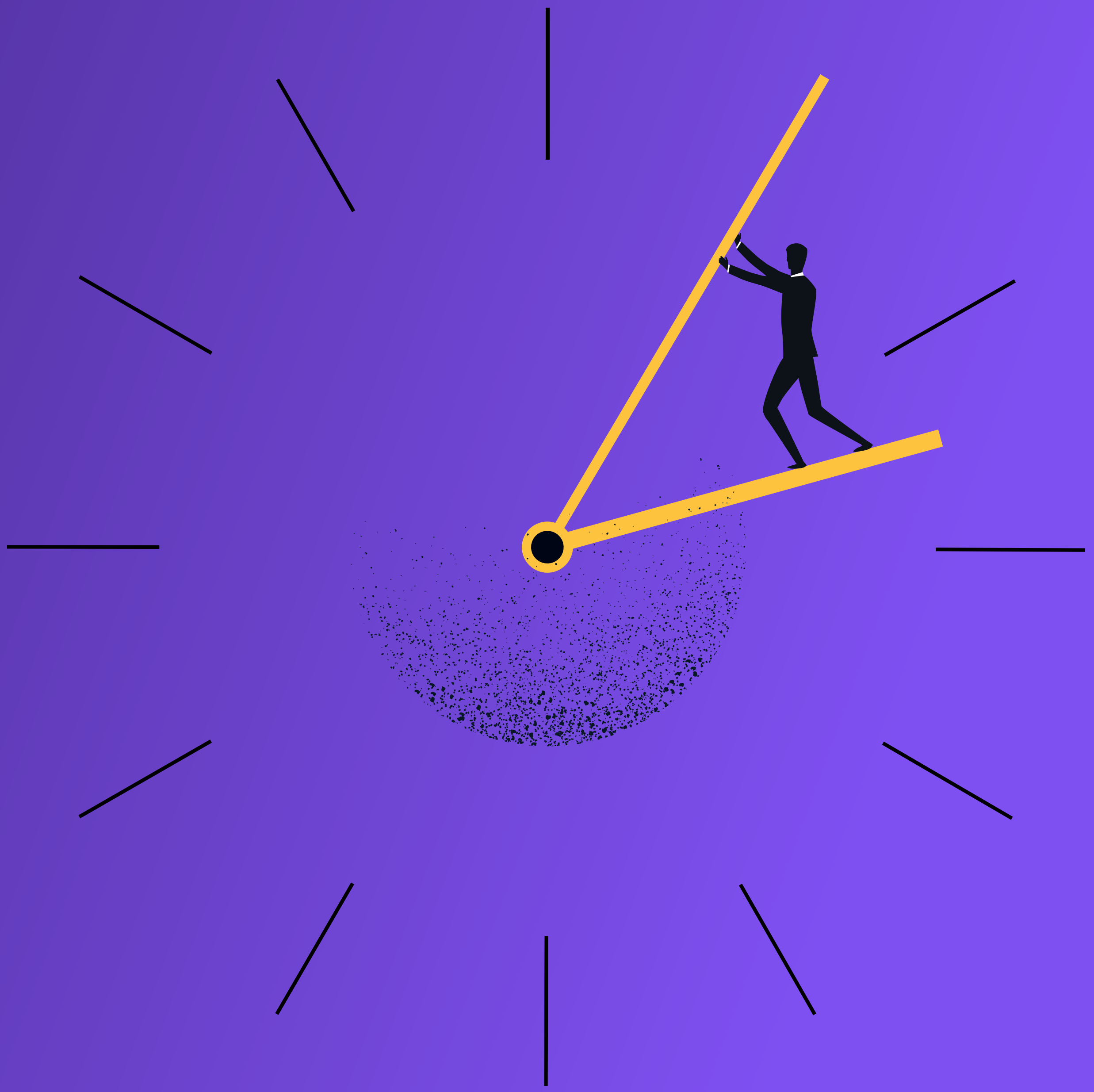
PLEXTRAC EBOOK

# Crushing the Reporting Time Suck

The security service provider's guide to automating pentest planning and delivery with PlexTrac.



PlexTrac®

# CONTENTS

From small pentest consultants to large managed security service providers (MSSPs), cybersecurity service providers stand in a critical gap for organizations of all sizes as their full security team or partner for targeted tasks. In order to serve and protect cyberspace, security service providers need to focus on the right security battles — those that can really move the needle on security posture and risk management for their clients.

Unfortunately, in order to effectively communicate and collaborate with their clients, service providers often spend a lot of time in processes like data aggregation, reporting, templating, and communicating information using tools ill designed for these tasks within the unique cybersecurity environment, particularly in offensive testing workflows.

This lack of efficiency in administrative tasks necessary in offensive security delivery has a significant cost in time and resources, especially in a business where service margins are already slim. What service providers of all sizes need is a product that can automate penetration test planning, reporting, and findings collaboration, enabling service providers to boost margins, scale service delivery, and enhance the value delivered to clients.

**Enter PlexTrac.**

> In order to serve and protect cyberspace, security service providers need to focus on the right security battles — those that can really move the needle on security posture and risk management for their clients.

## Productivity Pain Points for Security Service Providers

PlexTrac addresses all the data integration and management, report writing, white labeling, and assessment administration pain points that security service providers routinely face. These workflow processes are critical to producing final deliverables and communicating effectively with clients, but they typically require way more time and effort than is worthy of a team of skilled security practitioners.

As the premier cybersecurity reporting and collaboration platform, PlexTrac is a force multiplier for service providers, allowing practice managers to improve productivity and the morale of their teams. Higher productivity and morale translates to higher profits, better employee retention, and more satisfied clients. PlexTrac enables service providers to scale service delivery exponentially and differentiate themselves in the marketplace by alleviating four process pain points to improve efficiency and effectiveness.

### Inefficient Data Management

Regardless of the relationship between the consultancy and the client — either long-term management or short-term engagement — efficiently managing data, including collection, analysis, and reporting, is likely to be a continuous area for focus and improvement.

With PlexTrac, you can import all of your network and application scanner data into a single platform, and manipulate and analyze those results to form the basis of findings and writeups and analytics on those findings. Bring all your tools together in PlexTrac for quicker data aggregation and powerful visualization.

> With PlexTrac, you can import all of your network and application scanner data into a single platform, and manipulate and analyze those results to form the basis of findings and writeups and analytics on those findings.

### One-Off Content

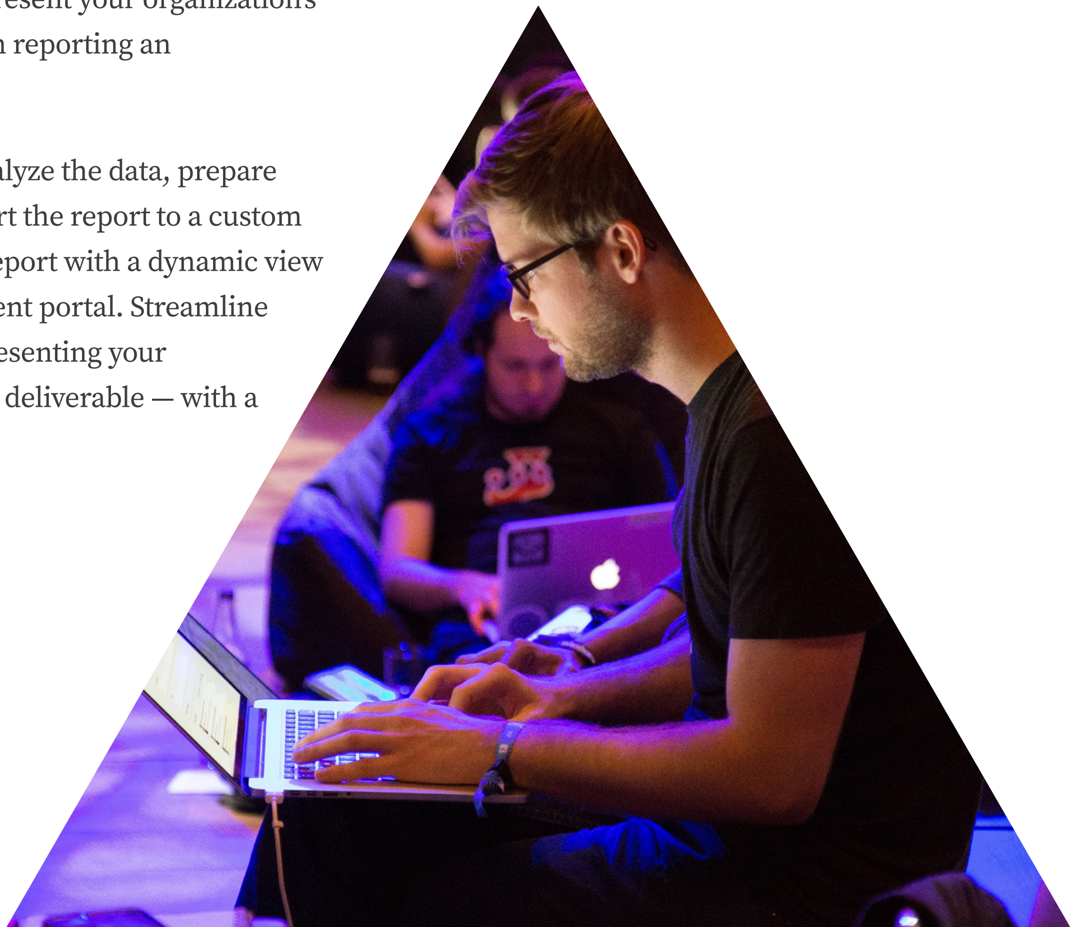
Let’s face it, reporting is a major chore and often the least favorite task of the security professional, yet arguably one of the more important as the report is the key deliverable shared with the client. Efficient reporting starts with modularizing report content, including writeups of common findings, boilerplate, and narratives, so that you aren’t starting from scratch or wasting time searching for baseline notes in products not really designed for your needs.

Your testers need to quit wasting time independently triaging scanner results, searching through Word docs for content used in previous reports, and then copying and pasting everything into a template — which then will still need to be massaged before it's ready to go. PlexTrac provides a customizable database for all your reusable content. Store writeups and narratives in separate repositories accessible to whomever needs them, which can be quickly and easily searched, edited, and added to a report — all inside the platform.

## Messing with Report Templates

Reporting is a time suck at every point in the process, but particularly at the point of delivery when more than just the results of your work matter. You also have to consider each client's preferences for communicating your methodology and how you represent your organization's identity. That's a tall order for any template and makes the last step in reporting an unnecessary lift.

PlexTrac allows you to take all the work your testers have done to analyze the data, prepare the  writeups and narratives, and add evidence, and then easily export the report to a custom .docx or PDF template. Additionally, you can supplement the static report with a dynamic view into your insights and recommendations by providing access to a client portal. Streamline the whole of the reporting process into one platform, while still representing your methodology and retaining your organizational branding in the final deliverable — with a click of a button.



### Bogged Down Assessment Administration

For those service providers that use assessment frameworks, you may have a broader set of needs that go beyond the pentesting workflow alone, but data management and reporting still tend to be areas that lack efficiency. PlexTrac's Assessments Module is an excellent resource for customizing questionnaires, the results of which can be collected, combined with evidence, and placed into customized reports, all in one convenient platform.

If you are interested in streamlining your offensive security service administration, evidence collection, and reporting processes AND improving communication for all involved in the process, PlexTrac is the platform for you.

> PlexTrac's Assessments Module is an excellent resource for customizing questionnaires, the results of which can be collected, combined with evidence, and placed into customized reports, all in one convenient platform.

## The PlexTrac Solution

Although PlexTrac is powerful and comprehensive, it is especially valuable for tasks security service providers perform consistently. PlexTrac's scanner integration capabilities, reusable content library, reporting functionality with custom templating, client portal, and assessments feature work together to streamline the whole workflow in one innovative platform.

**Check out how easy going from data to deliverable can be on the PlexTrac platform.**

## Import and Manipulate Results of Network and App Scanning Tools

Automated data collection is critical for security consultancies to maximize their coverage of clients' environments. While automated scanners are necessary, anyone can employ them. The value add is having the expertise to collect, triage, and provide professional analysis of the data to truly support the client's security strategy and the improvement of their security posture.

Providing this expertise is what security service providers do so well. And becoming more effective and efficient with data collection and analysis is one key to scaling service delivery and providing more value to retain clients.

With PlexTrac, you can import all of the data from your network and application scanning and other pentesting tools into one place — in addition to findings from manual testing — and manipulate and analyze those results to form the basis of findings and writeups on those findings. Bring all your data together in PlexTrac for better, quicker aggregation and visualization.

Bring all your data together in PlexTrac for better, quicker aggregation and visualization.

## A Centralized Platform for the Raw Data

PlexTrac supports data imports from all leading vulnerability scanners, including Nessus, Burp Suite, Nexpose, and Veracode. You can also plug and play other scanners or your custom tools with PlexTrac's open API. And we are constantly working on new integrations!

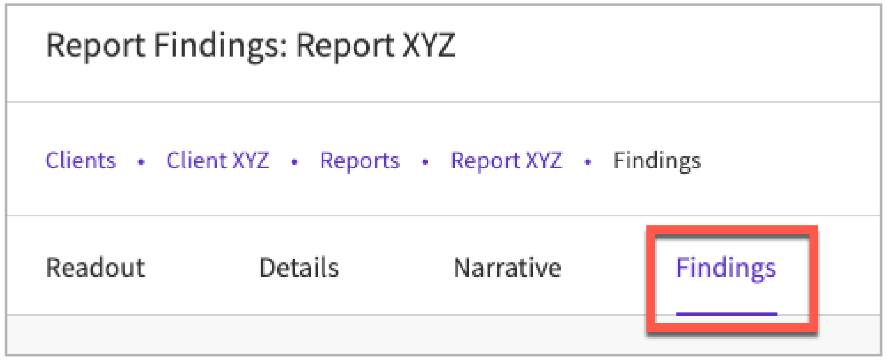
Imagine the convenience and control of being able to deal with all your automated tools in one place where you can import all the data from all the sources, manipulate and enhance it, and add your professional analysis. PlexTrac makes it simple to do just that.

## How to Import Data from Scanners in PlexTrac

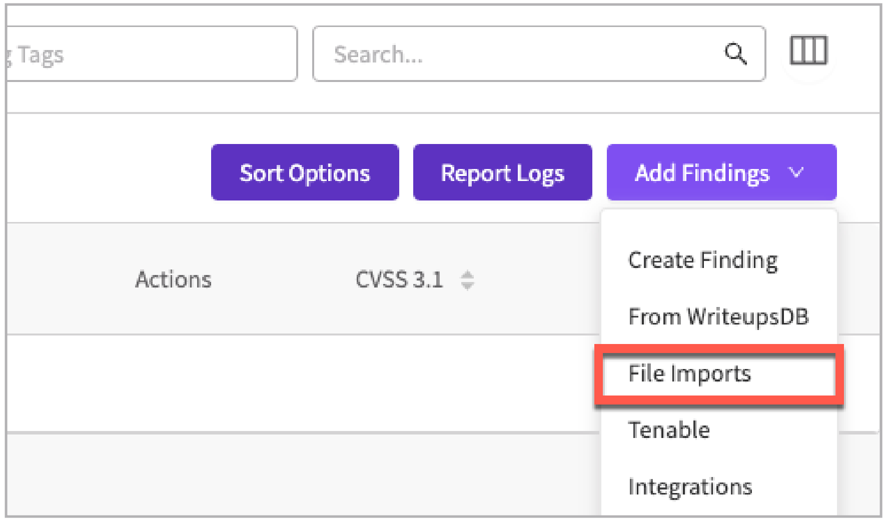
A few easy steps on our user-friendly interface and you'll be saving time while focusing on the real security work.

*Step 1: Prepare to Add Findings to a Report*

Navigate to the **Findings** section.

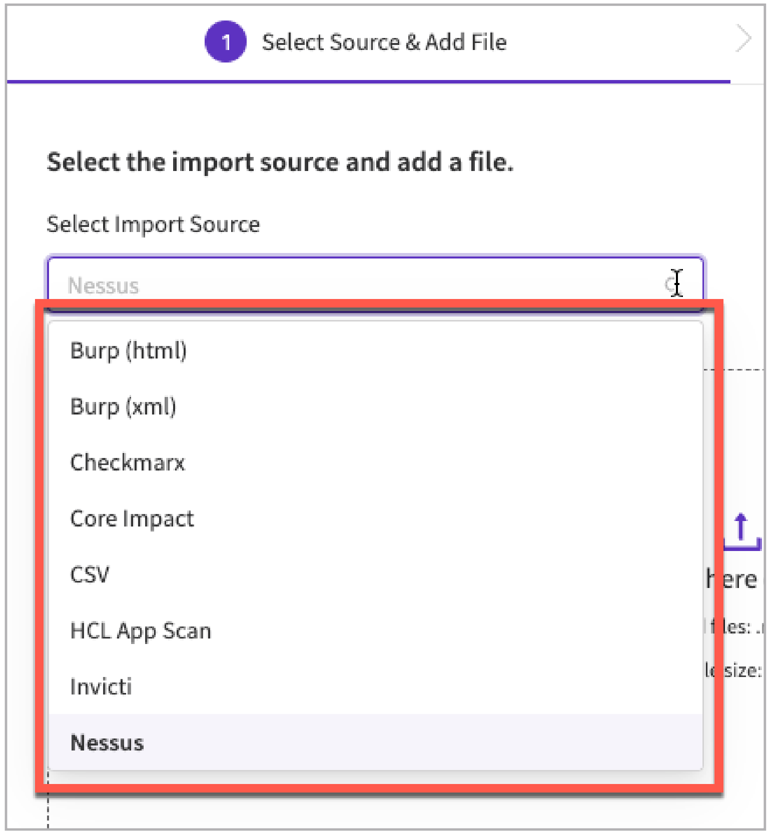

Report Findings: Report XYZ
Clients • Client XYZ • Reports • Report XYZ • Findings
Readout
Details
Narrative
Findings

Select the "**Add Findings Dropdown**," and then select the **"File Imports"** option.



### *Step 2: Choose Your Scanner Imports*

A modal titled **"File Imports"** will appear. From here, you will use the **"Select Import Source"** drop down and choose the tool that the data is coming from (i.e. Nessus, Burp, Qualys). Then upload or drop the file into this section and click continue.



1 Select Source & Add File

**Select the import source and add a file.**

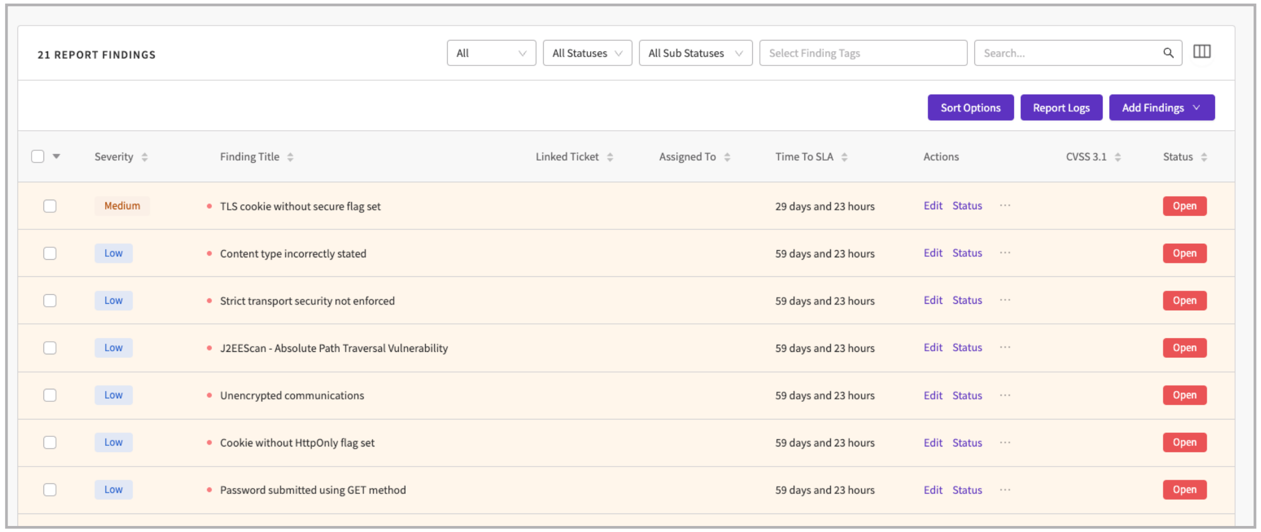
Select Import Source

Nessus

- Burp (html)
- Burp (xml)
- Checkmarx
- Core Impact
- CSV
- HCL App Scan
- Invicti
- **Nessus**

You can also add tags to both the findings and the assets that are being imported.

You will then see all of the scan data brought into PlexTrac in the form of **"Findings."**

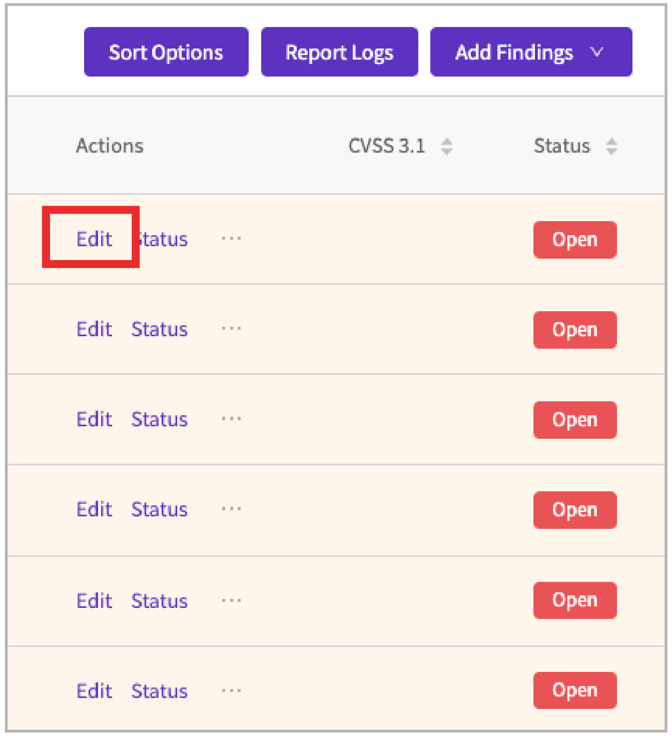


21 REPORT FINDINGS

| □ | Severity | Finding Title | Linked Ticket | Assigned To | Time To SLA | Actions | CVSS 3.1 | Status |
|---|---|---|---|---|---|---|---|---|
| □ | Medium | TLS cookie without secure flag set | | | 29 days and 23 hours | Edit Status ··· | | Open |
| □ | Low | Content type incorrectly stated | | | 59 days and 23 hours | Edit Status ··· | | Open |
| □ | Low | Strict transport security not enforced | | | 59 days and 23 hours | Edit Status ··· | | Open |
| □ | Low | J2EEScan - Absolute Path Traversal Vulnerability | | | 59 days and 23 hours | Edit Status ··· | | Open |
| □ | Low | Unencrypted communications | | | 59 days and 23 hours | Edit Status ··· | | Open |
| □ | Low | Cookie without HttpOnly flag set | | | 59 days and 23 hours | Edit Status ··· | | Open |
| □ | Low | Password submitted using GET method | | | 59 days and 23 hours | Edit Status ··· | | Open |

*Step 3: Modify, Enhance, Analyze the Data*

Once the findings are in PlexTrac, they can then be edited to modify and enhance the existing data from the scanning tool or to add further analysis from your security professionals.



| Actions | CVSS 3.1 | Status |
|---|---|---|
| Edit Status ··· | | Open |
| Edit Status ··· | | Open |
| Edit Status ··· | | Open |
| Edit Status ··· | | Open |
| Edit Status ··· | | Open |
| Edit Status ··· | | Open |

### Conquer Your Automated Scanner Data with PlexTrac

Managing the data doesn't have to be such a drag. Build better reports in half the time by importing the data from all your network and application scanning tools into PlexTrac.

## Customize a Database of Reusable Content

Perhaps the largest drain on the time of a security consultant is creating detailed, client-specific reports. This time suck is compounded by the common use of tools that simply weren't created for the work involved, namely Microsoft Word and Excel. Using a platform for streamlining the reporting process — allowing you to access, customize, and drop into your reports writeups for common findings and reusable narratives — is a game changer in efficiency.

PlexTrac provides a fully customizable content library to store common writeups and narrative language that get used frequently in reports. It includes the capability to organize reusable content into different repositories for easy access control. Imagine being able to run a quick search, customize an existing writeup or narrative, and drop it into your report with a click of a button. You can even collaborate on revision and editing directly in the platform to ensure quality and consistency across different testers' reports. Create, upload, and store all your reusable content  in PlexTrac — a platform designed specifically for the security reporting workflow.

PlexTrac customer Alex Boyle, senior manager of Offensive Security at Early Warning says, “The PlexTrac Content Library has been a huge help in bringing consistency to our findings writeups and report creation. We were able to input 170+ writeups into the WriteupsDB to get to 90 percent writeup content pre-built, making reports fast to write and consistent in content across the organization.”

## A Searchable Repository of All Writeups

PlexTrac’s Content Library includes the WriteupsDB, which allows you to store and reuse the same language for commonly identified findings. Rather than copying and pasting from Word or Excel, you can create, modify, upload, and store all of your frequently used language for reports in the same platform used to aggregate your scanner data and produce the reports themselves.

Modularization is key to streamlining the report writing process. Maintaining an easily searchable database of writeups for common findings will save time and ensure consistency across the security team.

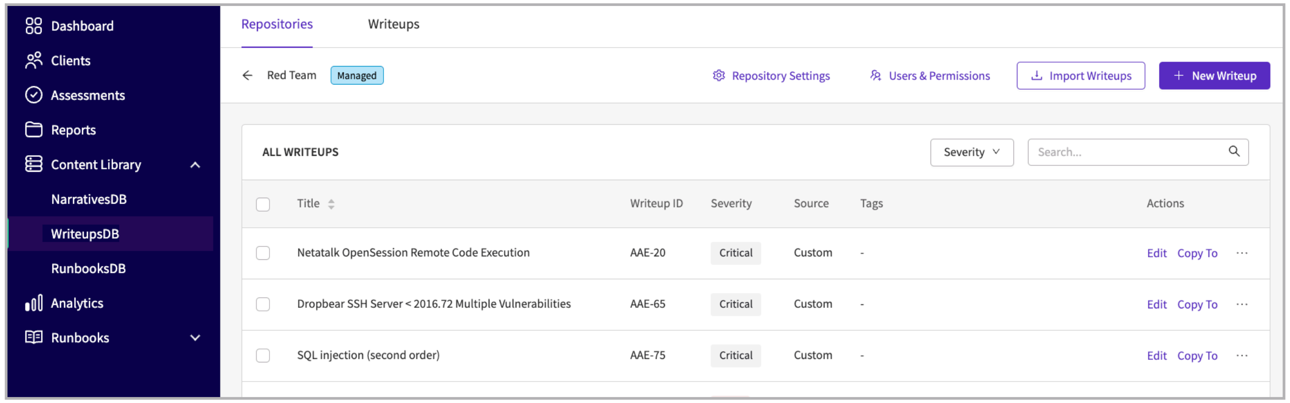
> Create, upload, and store all your reusable content in PlexTrac — a platform designed specifically for the security reporting workflow.

## How to Make the Most of the WriteupsDB in PlexTrac

The best part about the PlexTrac WriteupsDB is how simple it is to navigate and use — immediately streamlining the reporting workflow.

### *Step 1: Create Writeups*

To reduce report writing time and ensure consistency, an organization can leverage the WriteupsDB by codifying any details, references, or recommendations they feel are pertinent to a commonly identified finding.

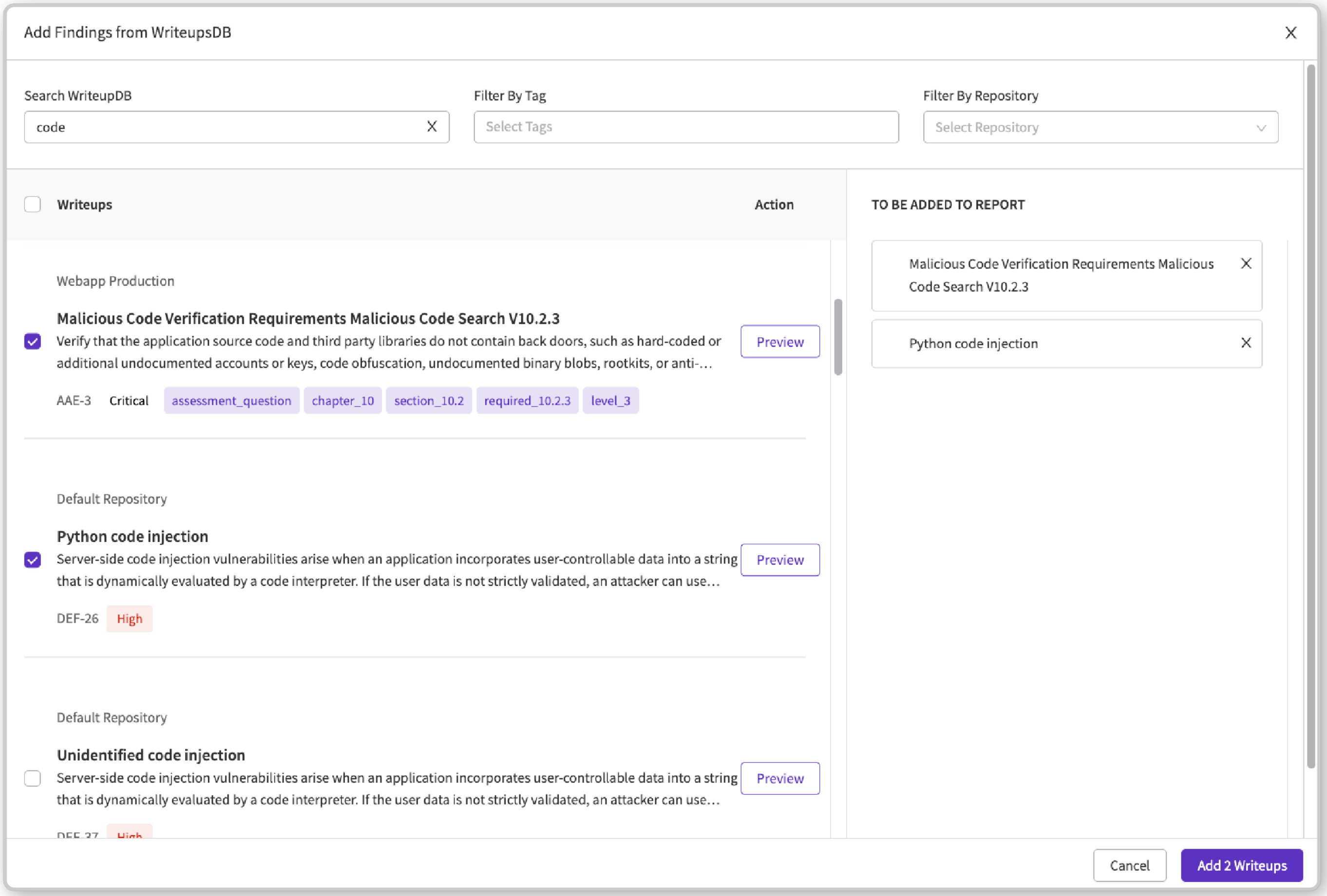


ALL WRITEUPS

| □ | Title | Writeup ID | Severity | Source | Tags | Actions |
|---|---|---|---|---|---|---|
| □ | Netatalk OpenSession Remote Code Execution | AAE-20 | Critical | Custom | - | Edit Copy To ··· |
| □ | Dropbear SSH Server < 2016.72 Multiple Vulnerabilities | AAE-65 | Critical | Custom | - | Edit Copy To ··· |
| □ | SQL injection (second order) | AAE-75 | Critical | Custom | - | Edit Copy To ··· |

### *Step 2: Build a Database of New and Existing Writeups*

While writeups can be created, edited, and viewed within the **WriteupsDB**, it is also important to note that a writeup can be brought into a PlexTrac report at any time. Once added to a report the writeup becomes a **"Finding,"** and any changes made within the report will not affect the writeup.


Add Findings from WriteupsDB

Search WriteupDB: code

Filter By Tag: Select Tags

Filter By Repository: Select Repository

□ Writeups — Action

Webapp Production

☑ **Malicious Code Verification Requirements Malicious Code Search V10.2.3**
Verify that the application source code and third party libraries do not contain back doors, such as hard-coded or additional undocumented accounts or keys, code obfuscation, undocumented binary blobs, rootkits, or anti-...
AAE-3 Critical assessment_question chapter_10 section_10.2 required_10.2.3 level_3 — Preview

Default Repository

☑ **Python code injection**
Server-side code injection vulnerabilities arise when an application incorporates user-controllable data into a string that is dynamically evaluated by a code interpreter. If the user data is not strictly validated, an attacker can use...
DEF-26 High — Preview

Default Repository

□ **Unidentified code injection**
Server-side code injection vulnerabilities arise when an application incorporates user-controllable data into a string that is dynamically evaluated by a code interpreter. If the user data is not strictly validated, an attacker can use...
DEF-37 High — Preview

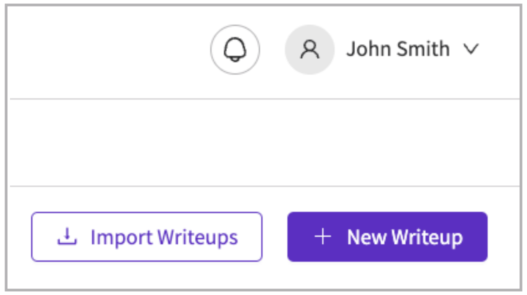
TO BE ADDED TO REPORT

- Malicious Code Verification Requirements Malicious Code Search V10.2.3 ✕
- Python code injection ✕

The best part about the PlexTrac WriteupsDB is how simple it is to navigate and use — immediately streamlining the reporting workflow.

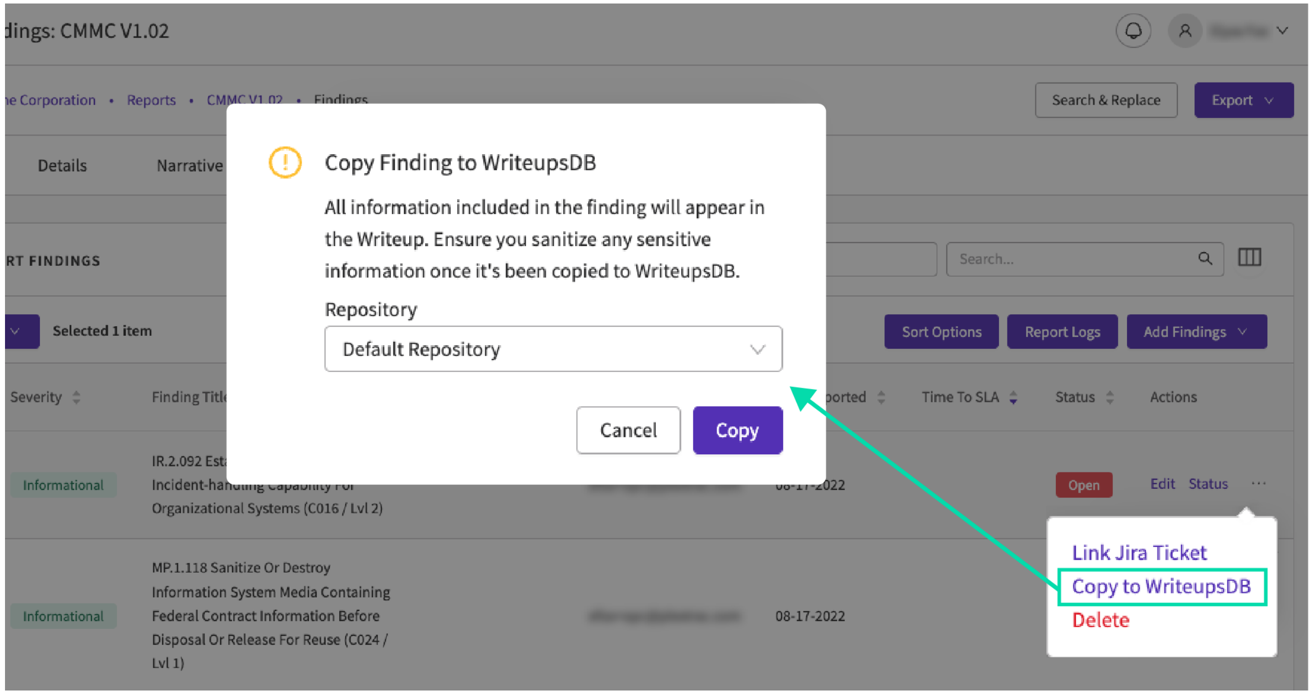
Note that a writeup can be created manually, or an existing database that an organization may already use can be imported into your PlexTrac instance via .csv. This allows organizations with large databases of information to import the information instantly and begin work immediately using their existing data and the PlexTrac library or any writeups already created on the platform.

***Click here** to check out how simple it is to import into the WriteupsDB!*



### *Step 3: Save Report Findings to the WriteupsDB*

Additionally, if at any time you're working in a PlexTrac Report you can copy a finding back to the WriteupsDB. This feature makes it easy for any reusable new work to be moved to and saved in the WriteupsDB.



dings: CMMC V1.02

Copy Finding to WriteupsDB

All information included in the finding will appear in the Writeup. Ensure you sanitize any sensitive information once it's been copied to WriteupsDB.

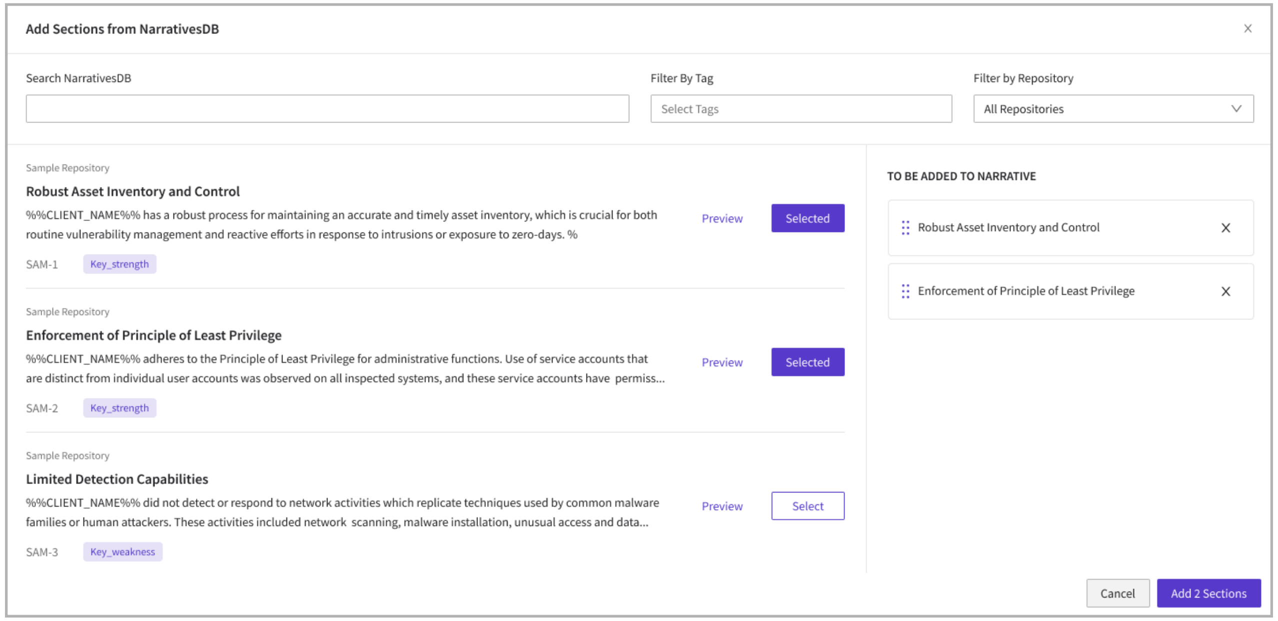
Repository: Default Repository

| Severity | Finding Title | | ported | Time To SLA | Status | Actions |
|---|---|---|---|---|---|---|
| Informational | IR.2.092 Est… Incident-handling Capability For Organizational Systems (C016 / Lvl 2) | [redacted] | 08-17-2022 | | Open | Edit Status ··· |
| Informational | MP.1.118 Sanitize Or Destroy Information System Media Containing Federal Contract Information Before Disposal Or Release For Reuse (C024 / Lvl 1) | [redacted] | 08-17-2022 | | | |

## How to Make the Most of the NarrativesDB in PlexTrac

Similar to WriteupsDB, you may also build out a repository of reusable narrative content, including key strengths, key weaknesses, team member bios, summaries, and more. Organize your narrative snippets into collections for easy and controlled access, ensuring consistency and quality in every report and saving you time in report building.

> Don’t start reports from scratch every time or use tools that weren’t designed for the security reporting process.



Add Sections from NarrativesDB

Search NarrativesDB

Filter By Tag: Select Tags

Filter by Repository: All Repositories

Sample Repository

**Robust Asset Inventory and Control**

%%CLIENT_NAME%% has a robust process for maintaining an accurate and timely asset inventory, which is crucial for both routine vulnerability management and reactive efforts in response to intrusions or exposure to zero-days. %

SAM-1 Key_strength

Sample Repository

**Enforcement of Principle of Least Privilege**

%%CLIENT_NAME%% adheres to the Principle of Least Privilege for administrative functions. Use of service accounts that are distinct from individual user accounts was observed on all inspected systems, and these service accounts have permiss...

SAM-2 Key_strength

Sample Repository

**Limited Detection Capabilities**

%%CLIENT_NAME%% did not detect or respond to network activities which replicate techniques used by common malware families or human attackers. These activities included network scanning, malware installation, unusual access and data...

SAM-3 Key_weakness

TO BE ADDED TO NARRATIVE

- Robust Asset Inventory and Control
- Enforcement of Principle of Least Privilege

## Conquer Your Reports with a Reusable Content Library

Don’t start reports from scratch every time or use tools that weren’t designed for the security reporting process. Instead, use PlexTrac to effectively modularize your common writeups and narratives and put them to work in reports with the click of a button.

## Export to Custom Templates or Share through a Client Portal

Preparing the actual report for clients is often one of the least popular tasks a penetration tester must accomplish, but one the practice manager is deeply concerned about. As the primary deliverable of most engagements, the report must represent and differentiate the organization amongst many competitors. It must account for all the branding demands of the marketing department and meet the standards of organization, quality, and consistency set by the practice to ensure value delivered to the customer. What if your team could manage the data and prepare reports in one platform AND easily export in the look and feel you require?

PlexTrac takes you through the entire security management workflow from data aggregation to deliverable report. How will your report look with PlexTrac? Exactly how it does now. With supported custom templating and PlexTrac's open API, you can match your reporting methodologies and organization's branding guidelines. Export all your report features — findings, narratives, evidence — into your custom .docx template with the click of a button.

And if you're ready to transform reports from static PDFs into dynamic experiences and provide your clients with a richer, premium reporting experience they can consume through a live platform, the PlexTrac Client Portal allows you to give each of your customers read-only access to the UI with role-based access control to customize permissions.

> Export all your report features – findings, narratives, evidence – into your custom .docx template with the click of a button.

## Report Templates Tailored to Your Organization

Within PlexTrac you have the ability to gather and organize all of the potential data points surrounding the security services you provide, including penetration testing, vulnerability scans, or framework-based assessments. This data must be communicated, and a report is typically the key deliverable of an engagement.

PlexTrac streamlines report creation by allowing you to prepare and deliver the report content in the same platform where you have collected and triaged your data and applied existing and customized writeups. Once everything is ready, exporting to a document template designed to your specifications and accessible to your clients is a breeze. You can also share your report PDF securely through the PlexTrac Client Portal so you don't have to encrypt and send via another method.

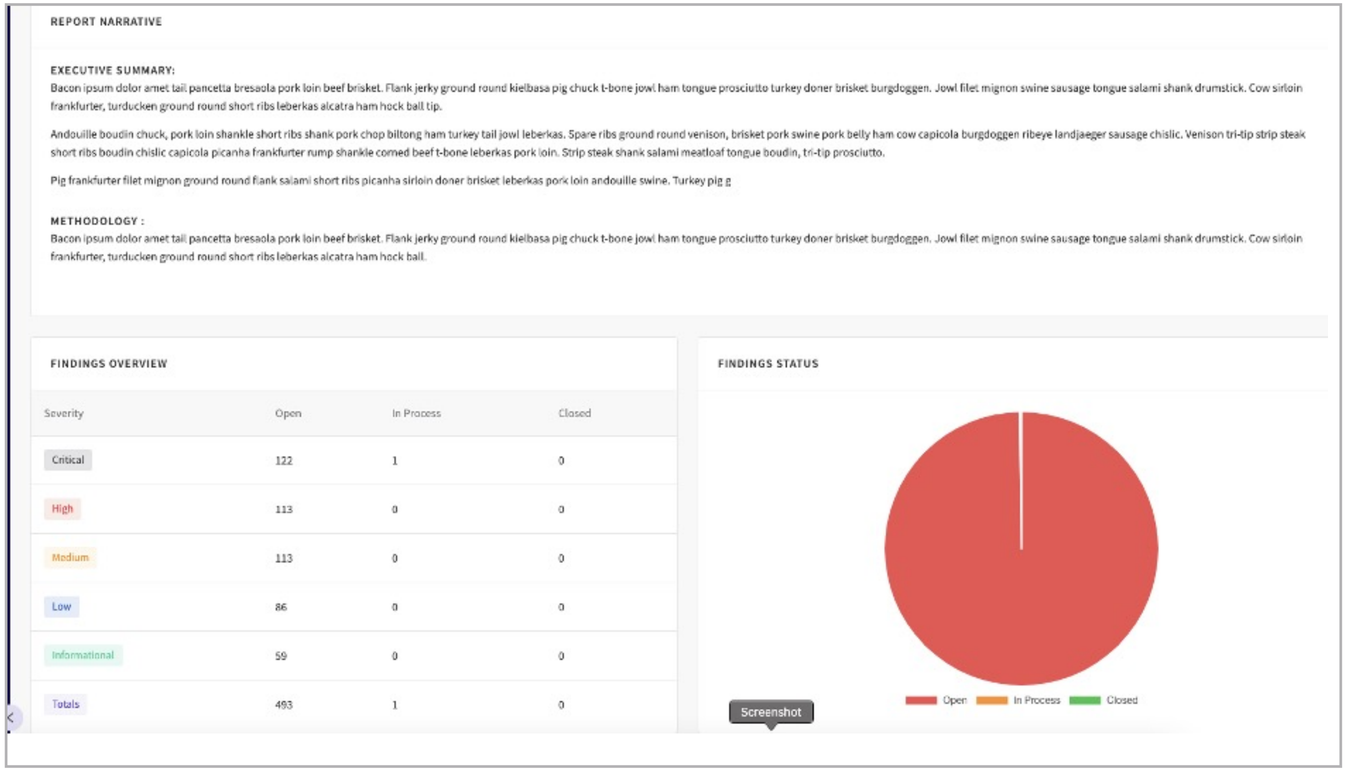
Within PlexTrac you have the ability to gather and organize all of the potential data points surrounding the security services you provide.

## How to Export to Customized Documents in PlexTrac

Moving from data to deliverable is completely streamlined in PlexTrac. Writing quality, consistent, branded, and beautifully formatted reports has never been simpler.

*Step 1: Access All the Report Data*

Prepare your data right in the platform — including narratives, analytics, screenshots, and more.



REPORT NARRATIVE

EXECUTIVE SUMMARY:
Bacon ipsum dolor amet tail pancetta bresaola pork loin beef brisket. Flank jerky ground round kielbasa pig chuck t-bone jowl ham tongue prosciutto turkey doner brisket burgdoggen. Jowl filet mignon swine sausage tongue salami shank drumstick. Cow sirloin frankfurter, turducken ground round short ribs leberkas alcatra ham hock ball tip.

Andouille boudin chuck, pork loin shankle short ribs shank pork chop biltong ham turkey tail jowl leberkas. Spare ribs ground round venison, brisket pork swine pork belly ham cow capicola burgdoggen ribeye landjaeger sausage chislic. Venison tri-tip strip steak short ribs boudin chislic capicola picanha frankfurter rump shankle corned beef t-bone leberkas pork loin. Strip steak shank salami meatloaf tongue boudin, tri-tip prosciutto.

Pig frankfurter filet mignon ground round flank salami short ribs picanha sirloin doner brisket leberkas pork loin andouille swine. Turkey pig g

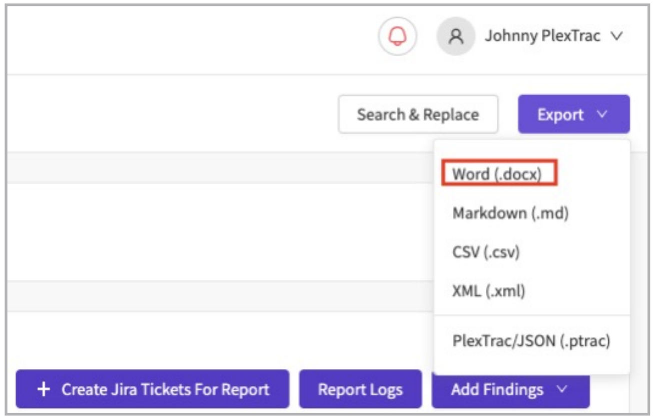
METHODOLOGY :
Bacon ipsum dolor amet tail pancetta bresaola pork loin beef brisket. Flank jerky ground round kielbasa pig chuck t-bone jowl ham tongue prosciutto turkey doner brisket burgdoggen. Jowl filet mignon swine sausage tongue salami shank drumstick. Cow sirloin frankfurter, turducken ground round short ribs leberkas alcatra ham hock ball.

FINDINGS OVERVIEW

| Severity | Open | In Process | Closed |
|---|---|---|---|
| Critical | 122 | 1 | 0 |
| High | 113 | 0 | 0 |
| Medium | 113 | 0 | 0 |
| Low | 86 | 0 | 0 |
| Informational | 59 | 0 | 0 |
| Totals | 493 | 1 | 0 |

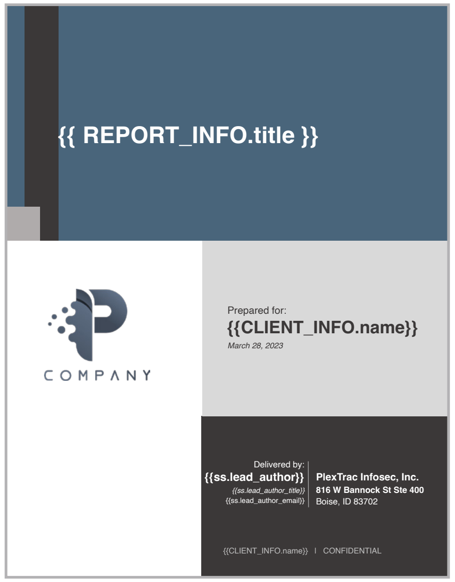
FINDINGS STATUS

While the unique data points that service providers report on may be similar, the format in which different organizations present this data is generally very unique. Using PlexTrac's custom report formatting, you can automate the vast majority of report generation allowing you to build out the data inside of PlexTrac and then simply export to Word.



### *Step 2: Export to a Customized Template*

Once exported, you will see a document that has all the required fonts, formats, and styles to ensure that your reports meet the standards that your organization has defined.



{{ REPORT_INFO.title }}

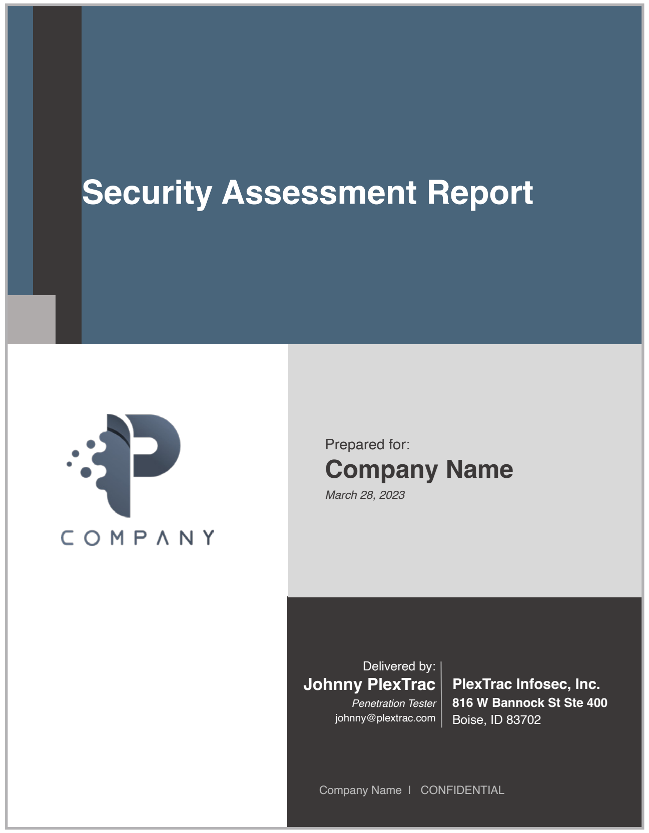
COMPANY

Prepared for:
{{CLIENT_INFO.name}}
March 28, 2023

Delivered by:
{{ss.lead_author}}
{{ss.lead_author_title}}
{{ss.lead_author_email}}

PlexTrac Infosec, Inc.
816 W Bannock St Ste 400
Boise, ID 83702

{{CLIENT_INFO.name}} I CONFIDENTIAL



Security Assessment Report

COMPANY

Prepared for:
Company Name
March 28, 2023

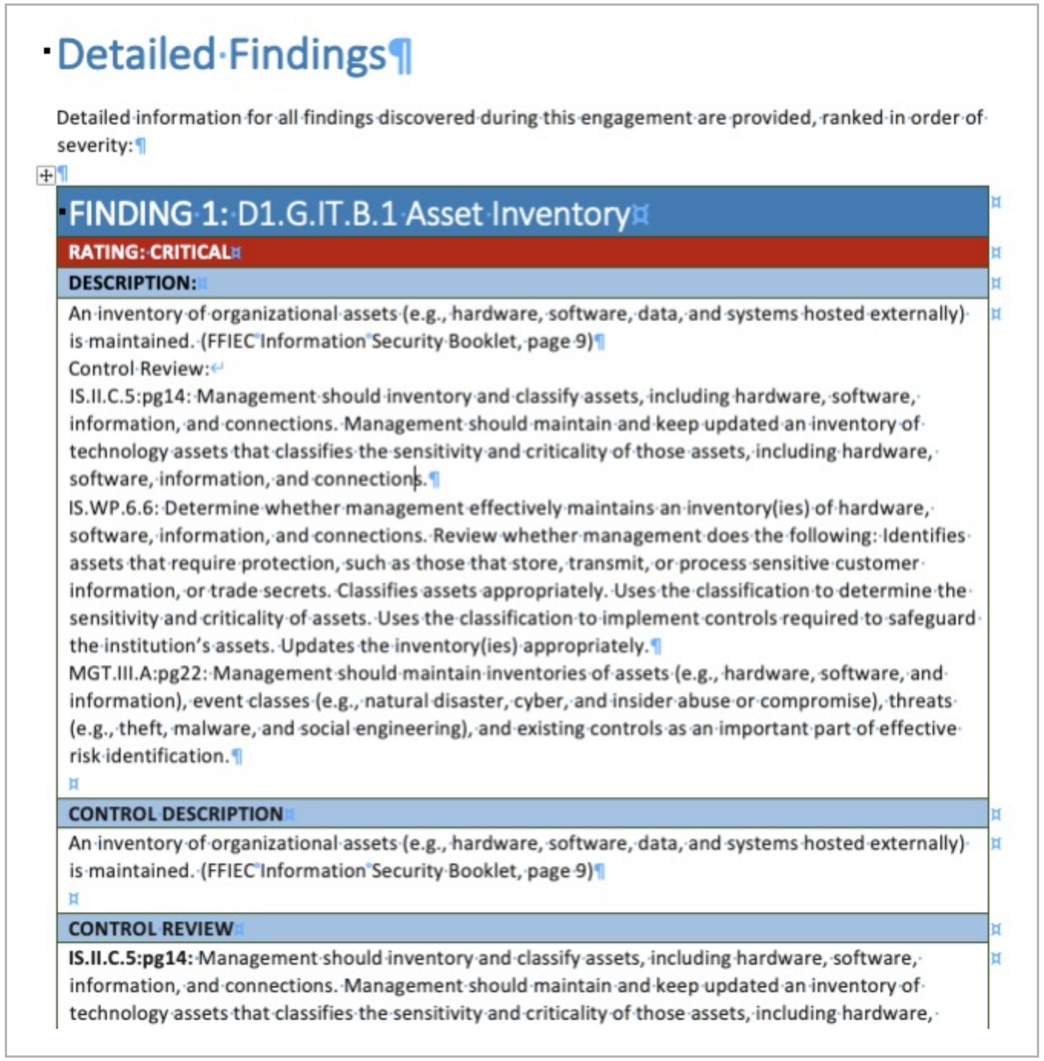
Delivered by:
Johnny PlexTrac
Penetration Tester
johnny@plextrac.com

PlexTrac Infosec, Inc.
816 W Bannock St Ste 400
Boise, ID 83702

Company Name I CONFIDENTIAL

### *Step 3: Display the Data You Want, How You Want*

All of the unique data points within PlexTrac can be presented in the final document. Detailed findings and custom narratives are just two examples of all the potential ways to display this data.



## Detailed Findings

Detailed information for all findings discovered during this engagement are provided, ranked in order of severity:

### FINDING 1: D1.G.IT.B.1 Asset Inventory

**RATING: CRITICAL**

**DESCRIPTION:**

An inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained. (FFIEC Information Security Booklet, page 9)

Control Review:
IS.II.C.5:pg14: Management should inventory and classify assets, including hardware, software, information, and connections. Management should maintain and keep updated an inventory of technology assets that classifies the sensitivity and criticality of those assets, including hardware, software, information, and connections.

IS.WP.6.6: Determine whether management effectively maintains an inventory(ies) of hardware, software, information, and connections. Review whether management does the following: Identifies assets that require protection, such as those that store, transmit, or process sensitive customer information, or trade secrets. Classifies assets appropriately. Uses the classification to determine the sensitivity and criticality of assets. Uses the classification to implement controls required to safeguard the institution's assets. Updates the inventory(ies) appropriately.

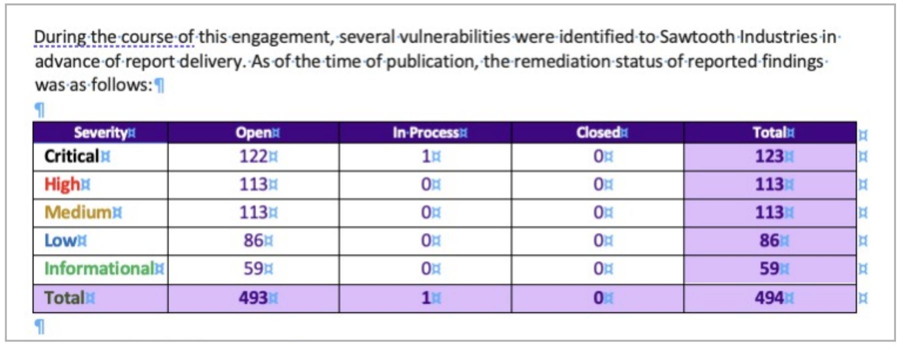
MGT.III.A:pg22: Management should maintain inventories of assets (e.g., hardware, software, and information), event classes (e.g., natural disaster, cyber, and insider abuse or compromise), threats (e.g., theft, malware, and social engineering), and existing controls as an important part of effective risk identification.

**CONTROL DESCRIPTION**

An inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained. (FFIEC Information Security Booklet, page 9)

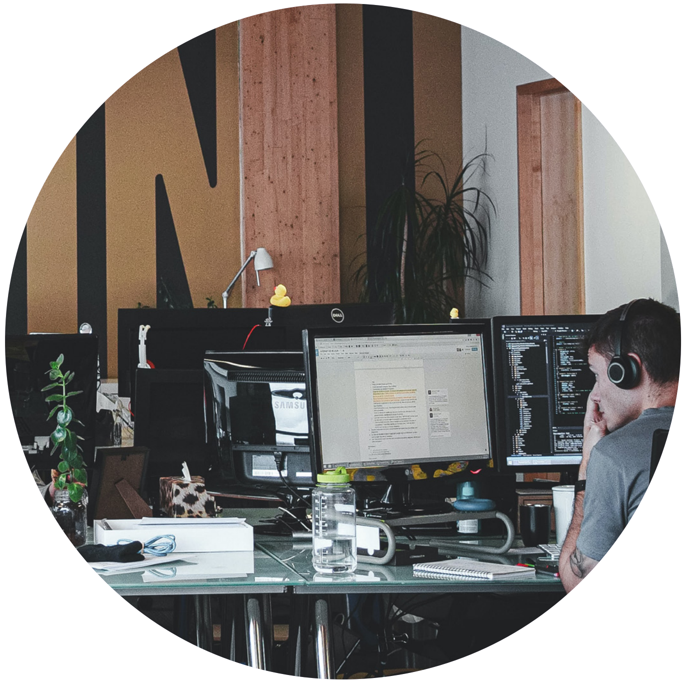
**CONTROL REVIEW**

**IS.II.C.5:pg14:** Management should inventory and classify assets, including hardware, software, information, and connections. Management should maintain and keep updated an inventory of technology assets that classifies the sensitivity and criticality of those assets, including hardware,



During the course of this engagement, several vulnerabilities were identified to Sawtooth Industries in advance of report delivery. As of the time of publication, the remediation status of reported findings was as follows:

| Severity | Open | In Process | Closed | Total |
|---|---|---|---|---|
| Critical | 122 | 1 | 0 | 123 |
| High | 113 | 0 | 0 | 113 |
| Medium | 113 | 0 | 0 | 113 |
| Low | 86 | 0 | 0 | 86 |
| Informational | 59 | 0 | 0 | 59 |
| Total | 493 | 1 | 0 | 494 |



You can also give each client direct access to their data through the Client Portal, which can be white labeled to your organizational branding and access controlled with RBAC.

> *Learn more about PlexTrac's client portal to go beyond a static report document or provide value between reports.*

### Conquer Your Reporting with Easy Exporting, Custom Templating, and a White Labeled Client Portal

Why not write reports in the platform where you manage your data and derive your analytics? Stop wasting time copying and pasting when you can use PlexTrac to instantly export reports to a template personalized for your methodologies and brand identity. Give your clients access to your findings right in the platform, so they can start taking action on your recommendations immediately.

## Streamline Assessments, Evidence Collection, and Reporting

Security service providers who use framework-based assessments offer valuable guidance on risk for the organizations they support. These practices often have an additional set of needs for their processes and reporting.

PlexTrac offers a flexible and comprehensive module for conducting security assessments. Base questionnaires on many of the common assessment frameworks and add and customize unlimited questions in multiple question formats. PlexTrac supports CMMC 2.0, NIST 800-53, NIST CSF, CISv8, ISO 27001, FFIEC, NYDFS compliance assessments among others. With PlexTrac, you can also export content — results, recommendations, references, and more — to your reports directly from the platform and skip the hassle of spreadsheets.

> Base questionnaires on many of the common assessment frameworks and add and customize unlimited questions in multiple question formats.

## Framework-based Assessments with Fully Customized Questionnaires

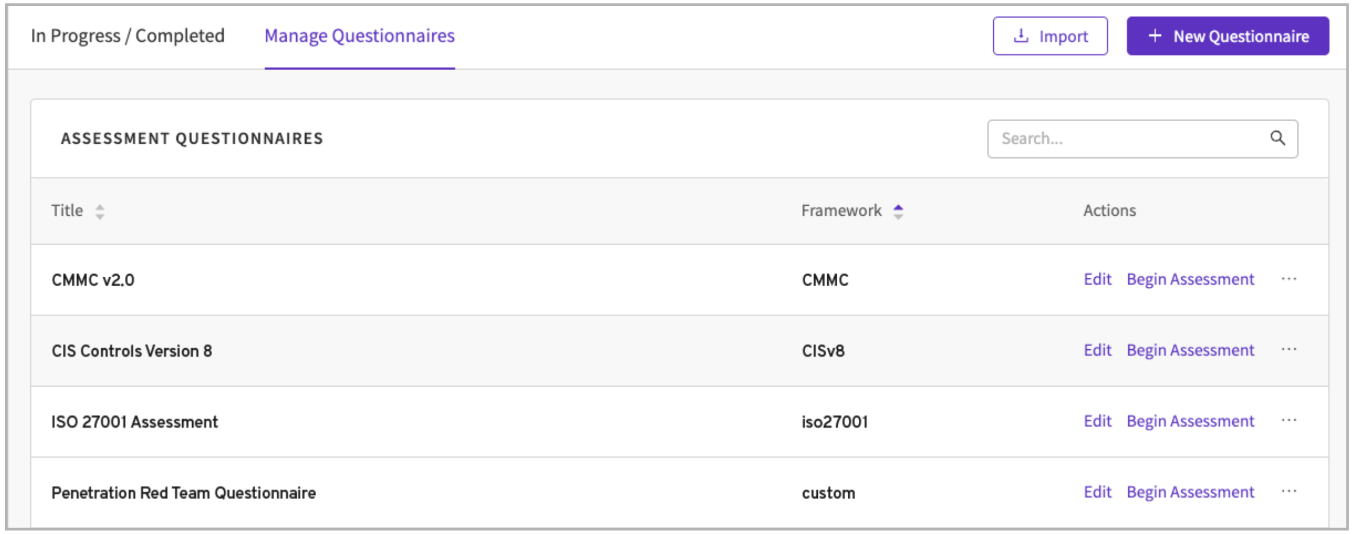
The Assessments Module in PlexTrac allows you to build assessments based on any variety of needs. While framework-based assessments (i.e. NIST, CIS, etc.) are commonplace in the industry, the Assessments Module can also be used to build assessments for scoping, third party attestation, and more. Many PlexTrac clients find Assessments to be a multipurpose module that is useful for providing clients with scoping questionnaires before pentests.

## How to Maximize Assessments in PlexTrac

Service providers that do assessment work will find the flexibility and efficiency in developing custom questionnaires, conducting assessments, and exporting reports that PlexTrac provides a simple solution for their use case.

### *Step 1: Define Questions per Governing Framework*

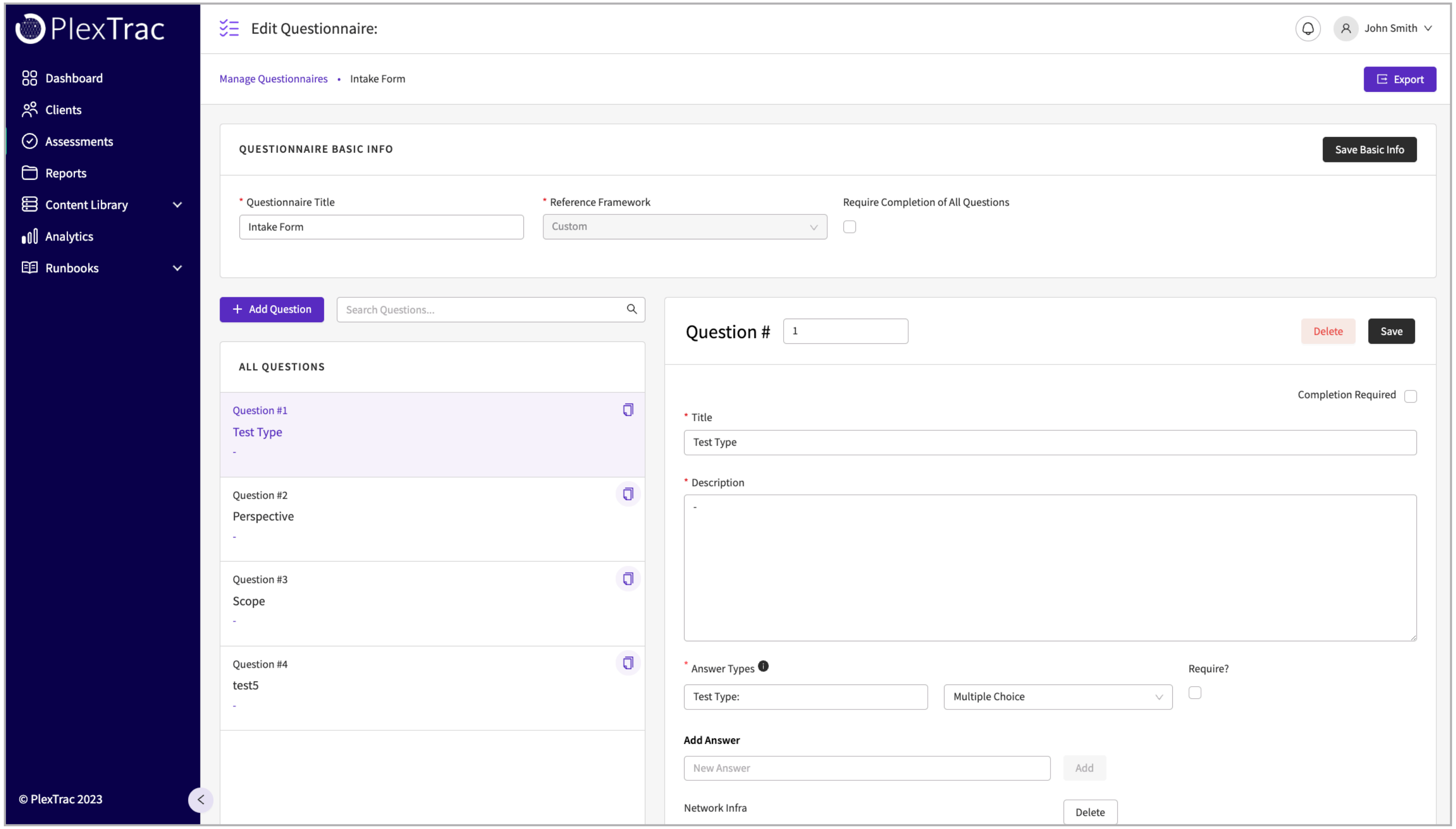
In the Assessments Module, choose the framework you'd like to use or start a new one from scratch.



ASSESSMENT QUESTIONNAIRES

| Title | Framework | Actions |
|---|---|---|
| CMMC v2.0 | CMMC | Edit Begin Assessment ··· |
| CIS Controls Version 8 | CISv8 | Edit Begin Assessment ··· |
| ISO 27001 Assessment | iso27001 | Edit Begin Assessment ··· |
| Penetration Red Team Questionnaire | custom | Edit Begin Assessment ··· |

Within an assessment you have the ability to define each individual question according to the governing document that you've chosen or for general information gathering.



QUESTIONNAIRE BASIC INFO

* Questionnaire Title: Intake Form

* Reference Framework: Custom

Require Completion of All Questions □

ALL QUESTIONS

Question #1
Test Type
-

Question #2
Perspective
-

Question #3
Scope
-

Question #4
test5
-

Question # 1

Completion Required □

* Title: Test Type

* Description: -

* Answer Types: Test Type: Multiple Choice

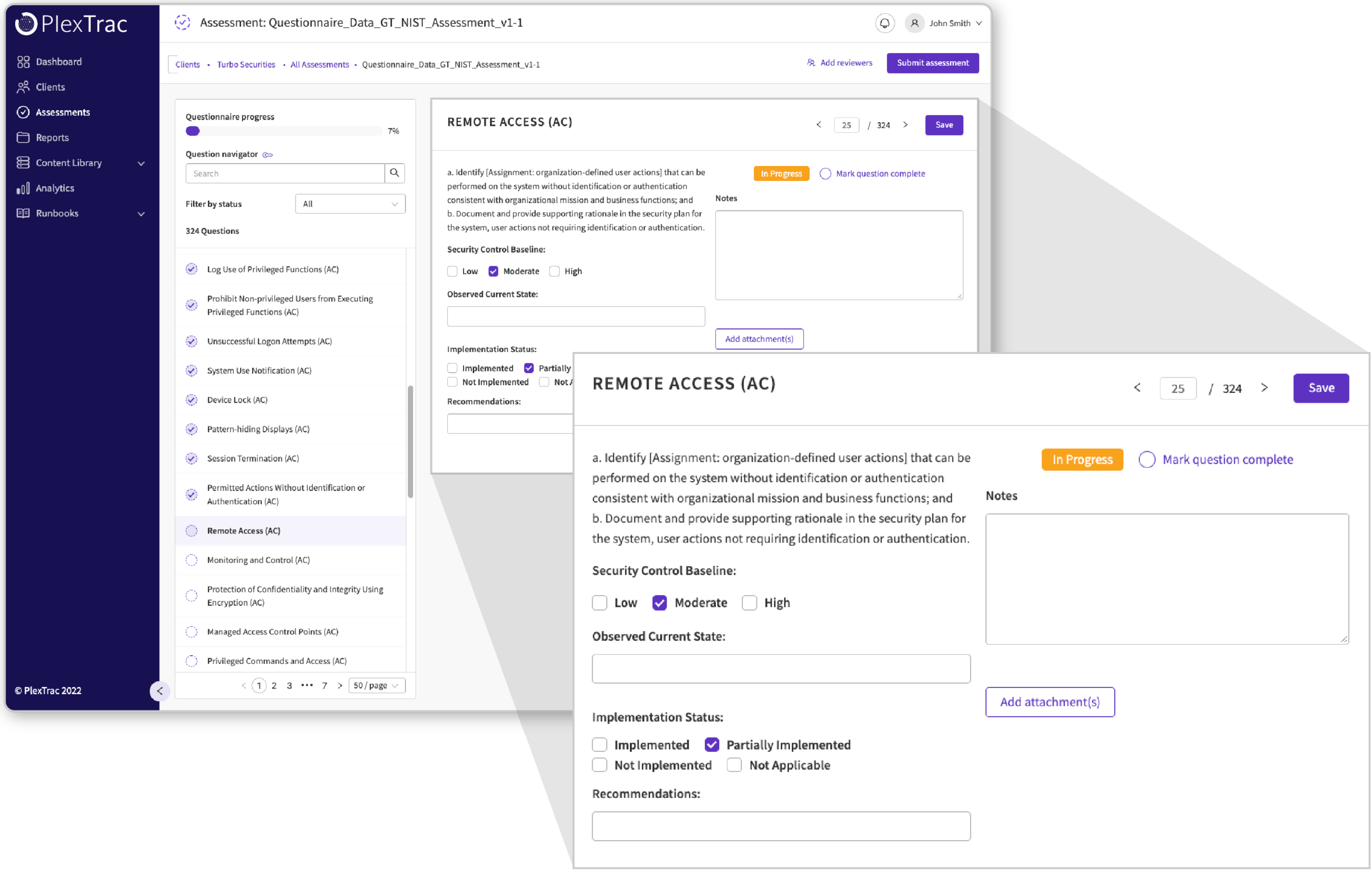
Require? □

Add Answer: New Answer

Network Infra

### *Step 2: Mask and Customize Report Content*

Because each assessment ultimately turns into a PlexTrac report, you can also include data that won't be viewed during the assessment but will be present in the report. This information can include candid recommendations, references, supporting artifacts, and even custom fields for any other information you'd like to attach to this question for report writing.



Assessment: Questionnaire_Data_GT_NIST_Assessment_v1-1

Clients • Turbo Securities • All Assessments • Questionnaire_Data_GT_NIST_Assessment_v1-1

Questionnaire progress 7%

Question navigator

Search

Filter by status: All

324 Questions

- Log Use of Privileged Functions (AC)
- Prohibit Non-privileged Users from Executing Privileged Functions (AC)
- Unsuccessful Logon Attempts (AC)
- System Use Notification (AC)
- Device Lock (AC)
- Pattern-hiding Displays (AC)
- Session Termination (AC)
- Permitted Actions Without Identification or Authentication (AC)
- Remote Access (AC)
- Monitoring and Control (AC)
- Protection of Confidentiality and Integrity Using Encryption (AC)
- Managed Access Control Points (AC)
- Privileged Commands and Access (AC)

< 1 2 3 ••• 7 > 50 / page

REMOTE ACCESS (AC) < 25 / 324 >

In Progress ○ Mark question complete

a. Identify [Assignment: organization-defined user actions] that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and
b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.

Security Control Baseline:

□ Low ☑ Moderate □ High

Observed Current State:

Notes

Implementation Status:

□ Implemented ☑ Partially Implemented
□ Not Implemented □ Not Applicable

Recommendations:

REMOTE ACCESS (AC) < 25 / 324 > Save

In Progress ○ Mark question complete

a. Identify [Assignment: organization-defined user actions] that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and
b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.

Notes

Security Control Baseline:

□ Low ☑ Moderate □ High

Observed Current State:

Add attachment(s)

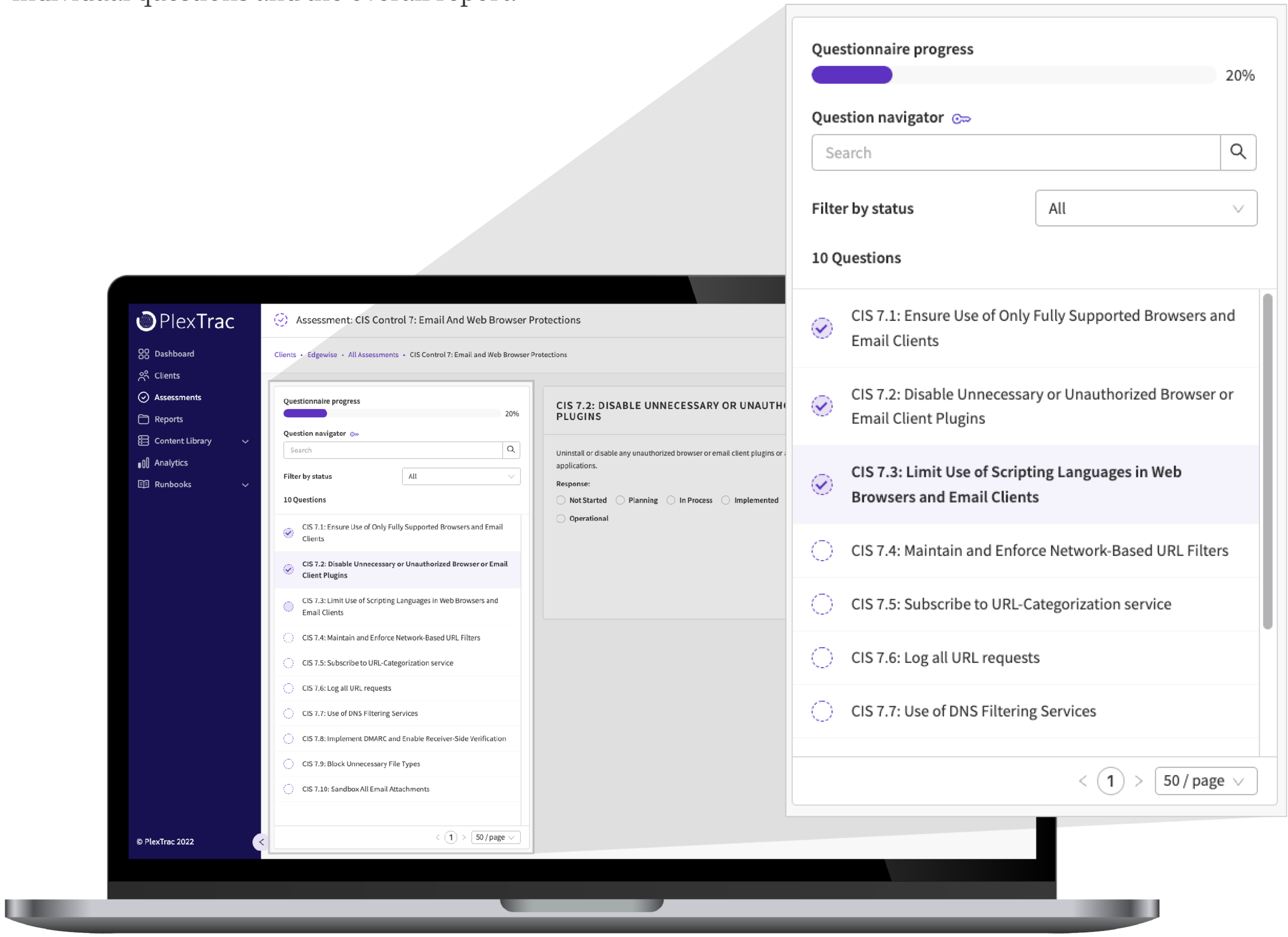
Implementation Status:

□ Implemented ☑ Partially Implemented
□ Not Implemented □ Not Applicable

Recommendations:

### *Step 3: Track Status and Attach Evidence*

Once an assessment has begun, you can track the status of both individual questions and the overall report.



Assessment: CIS Control 7: Email And Web Browser Protections

Clients • Edgewise • All Assessments • CIS Control 7: Email and Web Browser Protections

Questionnaire progress 20%

Question navigator

Search

Filter by status: All

10 Questions

- CIS 7.1: Ensure Use of Only Fully Supported Browsers and Email Clients
- CIS 7.2: Disable Unnecessary or Unauthorized Browser or Email Client Plugins
- CIS 7.3: Limit Use of Scripting Languages in Web Browsers and Email Clients
- CIS 7.4: Maintain and Enforce Network-Based URL Filters
- CIS 7.5: Subscribe to URL-Categorization service
- CIS 7.6: Log all URL requests
- CIS 7.7: Use of DNS Filtering Services
- CIS 7.8: Implement DMARC and Enable Receiver-Side Verification
- CIS 7.9: Block Unnecessary File Types
- CIS 7.10: Sandbox All Email Attachments

< 1 > 50 / page

CIS 7.2: DISABLE UNNECESSARY OR UNAUTH PLUGINS

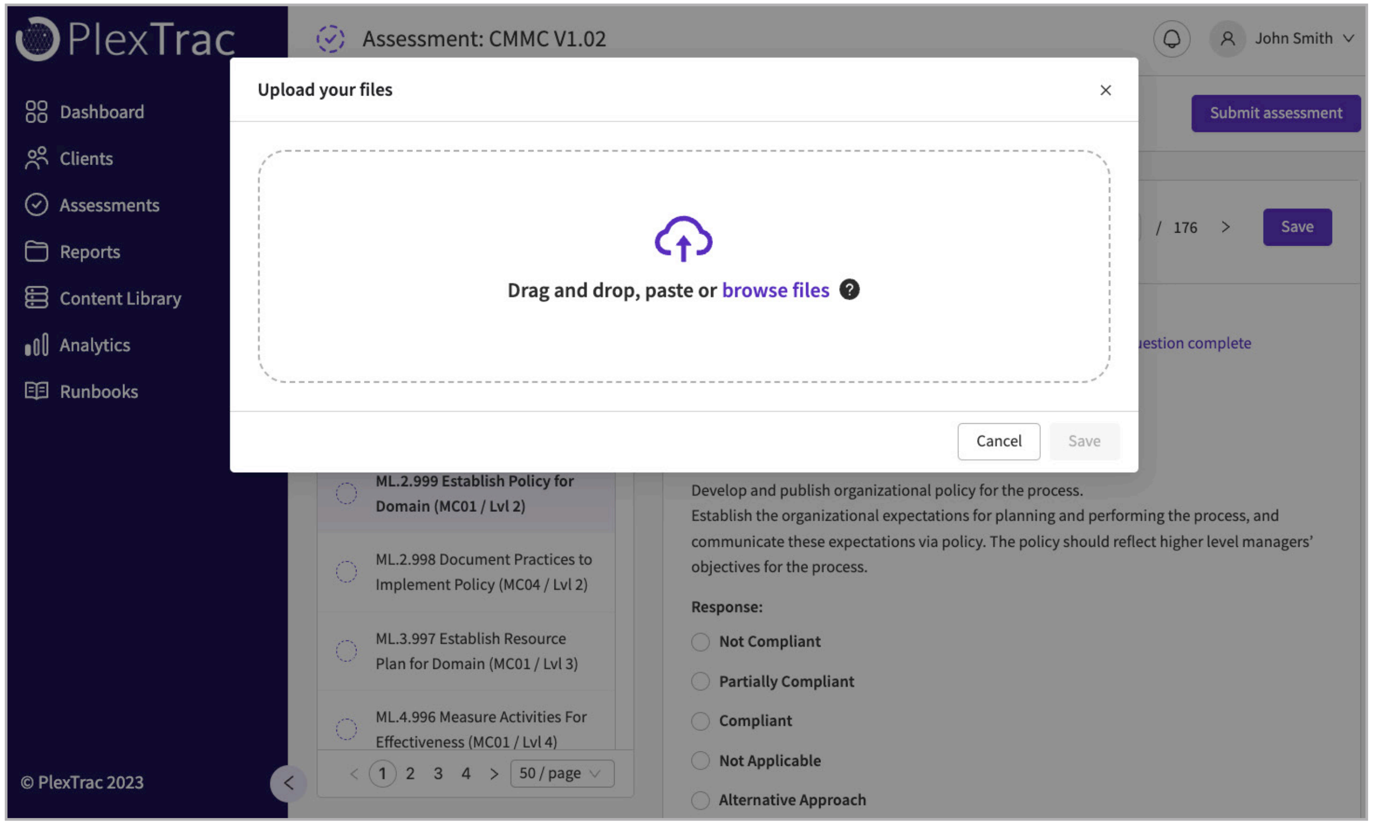
Uninstall or disable any unauthorized browser or email client plugins or applications.

Response:

○ Not Started ○ Planning ○ In Process ○ Implemented ○ Operational

While taking the assessment, you will see all of the answer types, input fields, and general details around the question that you've defined.

For each question in the assessment, you also have the ability to attach any relevant files to the specific question, including actual copies of written policy and screen shots of collected evidence. All of this information is passed on to the final report for further analysis, record keeping, and attestation.



ML.2.999 Establish Policy for Domain (MC01 / Lvl 2)

ML.2.998 Document Practices to Implement Policy (MC04 / Lvl 2)

ML.3.997 Establish Resource Plan for Domain (MC01 / Lvl 3)

ML.4.996 Measure Activities For Effectiveness (MC01 / Lvl 4)

Develop and publish organizational policy for the process.
Establish the organizational expectations for planning and performing the process, and communicate these expectations via policy. The policy should reflect higher level managers' objectives for the process.

Response:

○ Not Compliant
○ Partially Compliant
○ Compliant
○ Not Applicable
○ Alternative Approach

## Conquer Your Assessments with PlexTrac

Why not use one platform to support all the services your security consultancy offers? With modules designed to streamline data collection, reusable content, reporting, AND assessments, PlexTrac offers one solution for all the needs of security service providers.

## Deploy PlexTrac as a Security Service Provider

Whether you are evaluating the PlexTrac platform for the first time or you are a current PlexTrac customer seeking to maximize or expand your use case, take the next step by seeing the platform in action for your needs.

> ***Schedule a live demonstration** of PlexTrac today at plextrac.com/demo to begin driving higher profits and delivering more value.*

Fueled by a $70M Series B investment from Insight Partners, PlexTrac is a cybersecurity ScaleUp company on a mission to empower security service providers and teams to become more efficient and effective in their pentesting activities. The Plextrac platform automates pentest planning, reporting, and findings collaboration, allowing service providers to enhance margins and client outcomes, and enterprises to demonstrate the value of internal pentesting efforts and improved security posture.

PlexTrac®