

Optimize the Business of Purple Teaming

The Cybersecurity Team's Guide to
Improving Effectiveness with PlexTrac



CONTENTS

Introduction	2	Step 1: Locate Your Preferred Integration	18
Streamlined Workflows for All Aspects of the Security Program	3	Step 2: Configure the Integration	19
Offensive Security Work	3	Step 3: Create a Ticket	20
Defensive Security Work	4	Track and Manage Remediation with PlexTrac Integrations	21
Attestation to Leadership	4	Stakeholder Communication	22
Proactive Purple Teaming	4	One Platform to Produce Analytics for Constituents	22
Red Team Data Aggregation	5	How to View Analytics of Findings in PlexTrac	23
A Centralized Platform for Data Aggregation	6	Step 1: Filter to Find Data	23
How to Import Data from Scanners in PlexTrac	6	Step 2: View the Analytics or Apply More Filters	24
Step 1: Prepare to Add Findings to a Report	6	Step 3: Clear to View More Analytics	25
Step 2: Choose Your Scanner Imports	7	Communicate Your Security Posture Using PlexTrac Analytics	26
Step 3: Modify, Enhance, Analyze the Data	8	Continuous Purple Teaming Assessments	26
Aggregate All the Data from Red Team Operations with PlexTrac	8	A Platform Designed for Collaboration	26
Blue Team Remediation	8	How to Create a Runbook Engagement in PlexTrac	27
An Integrated Platform to Manage Remediation	9	Step 1: Select TTPs	27
How to Use the Jira Integration in PlexTrac	9	Step 2: Input Data	29
Step 1: Locate Your Preferred Integration	9	Step 3: Submit the Engagement to Report	32
Step 2: Configure the Integration	10	Purple Team with PlexTrac Runbooks	32
Step 3: Create a Ticket	16	Adopt PlexTrac as a Cybersecurity Team	33
How to Use the ServiceNow Integration in PlexTrac	18		



Cybersecurity teams exist so their companies can do business without interference. Accomplishing that straightforward sounding purpose is actually an enormous, multifaceted challenge. Teams must balance offensive and defensive security strategies, work and communicate with stakeholders beyond the security team, and contend with differing priorities on processes and budget. They must simultaneously be searching for new threats and risks and remediating the most critical known issues, all while ensuring the business can operate uninterrupted.

What if you could streamline the workflow and communication across the entire security team so that every professional could do their job more efficiently? From powerful data aggregation to simplified reporting and integrated ticketing for remediation to analytics and visualizations for board reporting, PlexTrac improves every aspect of the security management workflow.

In addition, PlexTrac is the mechanism to help cybersecurity teams of all sizes go purple! Purple teaming may seem out of reach for small or less mature teams, but at PlexTrac we embrace a broader definition of the concept that includes any activities involved in proactive security and better collaboration between roles on the security team. With this mindset and the right tools, any team can begin purple teaming or refine their existing purple teaming exercises and start experiencing the benefits.

Cybersecurity teams exist so their companies can do business without interference.

Streamlined Workflows for All Aspects of the Security Program

If your team is ready to improve your workflows, make reporting more efficient, and embrace a purple teaming mindset, the best place to start gaining control of your posture and moving towards proactive activities is by improving workflows and communication for all roles involved with cybersecurity.

PlexTrac is a best-in-class reporting and workflow management platform designed specifically for cybersecurity professionals. Bring all the pieces of the security program together to better manage, visualize, improve, and attest to your security posture.

With features to support offensive and defensive security work, to streamline communication to all stakeholders, and to facilitate purple teaming exercises, PlexTrac will help any cybersecurity team optimize their program and better protect their organization.

Offensive Security Work

Whether you outsource your offensive security or do some or all of it internally, you're dealing with significant data from a variety of sources to gain insight into your security posture. Whether data comes from a pentest report or a variety of automated scanners, cybersecurity teams need to be able to make sense of information about vulnerabilities in order to prioritize remediation efforts.

With PlexTrac, security teams can integrate all their data sources — including automated scanners and manual pentesting activities — of information into one location. PlexTrac aggregates data from red team exercises and tools so it can be analyzed and communicated directly.

Cybersecurity teams need to be able to make sense of information about vulnerabilities in order to prioritize remediation efforts.



Defensive Security Work

Many organizational cybersecurity teams already have workflow tools in place that help their blue teamers or IT analysts assign and manage remediation tasks. The challenge, and time suck, is then needing to manually populate ticketing tools like Jira and ServiceNow. If you have ever faced the pain of combing through hundreds of pages of a penetration test report and copy/pasting narratives into Jira tickets, then you know there has to be a better way.

PlexTrac offers integrations with major workflow and ticketing systems, including Jira and ServiceNow. It's both easy to configure and quick to create tickets out of findings in PlexTrac that will display in the systems you are already using. Or if you are ready to really streamline your processes, you can assign tasks and track remediation progress right in the platform.

Attestation to Leadership

Beyond the concerns of red and blue workflows, security teams must also keep a finger on the pulse of their security posture as a whole. Leaders must be able to not only determine where to prioritize time and resources within the security team but also communicate about priorities to the C-suite, board, and other stakeholders outside the team.

PlexTrac's Analytics module gives cybersecurity teams the tool they need for analyzing the data from all their sources to gain a real-time view of security posture. Slice and dice the data by asset, level of criticality, and more. Granular analytics and visualizations help keep the teams and key decision makers informed.

Proactive Purple Teaming

One of the most promising strategies used by mature cybersecurity programs to improve their security posture is continuous assessment through purple teaming. In fact, [a recent survey by CyberRisk Alliance and PlexTrac](#) found that 89 percent [of survey respondents who had used it] deemed purple teaming

89 percent [of survey respondents who had used it] deemed purple teaming activities “very important” to their security operations.

activities “very important” to their security operations. One IT/IT security director at a high-tech/IT organization described that purple teaming “helps predict the attacks we can expect and maximizes network capabilities through continuous feedback and information sharing.” In short, the research supported that purple teaming provides both strategic and tactical benefits for cybersecurity teams.

While there is plenty of evidence to demonstrate that conducting purple teaming activities in short iterative cycles is highly effective in identifying and remediating vulnerabilities, it can be challenging to know where to start. With the right tools, security teams can begin purple teaming activities regardless of program maturity.

PlexTrac’s Runbooks module is best-in-industry for test plan execution. By using Runbooks for purple teaming activities, your team can script engagements, leverage frameworks like MITRE ATT&CK, and achieve precision and consistency in testing. Runbooks also makes it easy to triage, report, and visualize progress over time.

Let’s take a deep dive into each of the features PlexTrac offers that address the major workflows and pain points for each part of the cybersecurity team.

Red Team Data Aggregation

Cybersecurity teams must have a view of their security posture in order to protect their data. In the typical model, the acquisition of vulnerability data and testing of the parameters has been considered a red team function. Security teams within organizations may have some red team function using automated scanners and in-house red teamers or they may outsource some or all of this work to penetration tester consultants or security service providers.

Regardless of how data is acquired, cybersecurity teams must ingest, dissect, and interpret it in order to flag the correct information and spot the most critical issues. Data handling from multiple sources can become a major headache and a bottleneck to actually becoming more secure. Just having information isn’t very helpful if it is lost in giant reports or siloed in different systems.

Regardless of how data is acquired, cybersecurity teams must ingest, dissect, and interpret it in order to flag the correct information and spot the most critical issues.

With PlexTrac, security teams can aggregate all the data from all the sources and translate it into meaningful and actionable information. PlexTrac allows the blue teamers to use assessment results by assigning and tracking necessary remediation all within the platform. If security service provider partners are also using PlexTrac, they can move beyond the need for a static PDF or Word doc deliverable and instead deliver their results directly to the security team inside of the platform.

A Centralized Platform for Data Aggregation

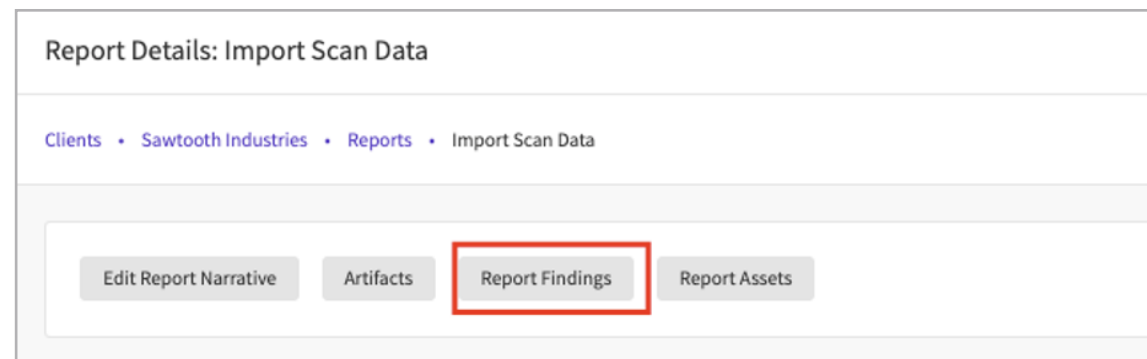
With PlexTrac, you can import all of the data from your network and application scanning tools into one place where it can be triaged into actionable information. Bring all your data together in PlexTrac for better, quicker aggregation and visualization.

How to Import Data from Scanners in PlexTrac

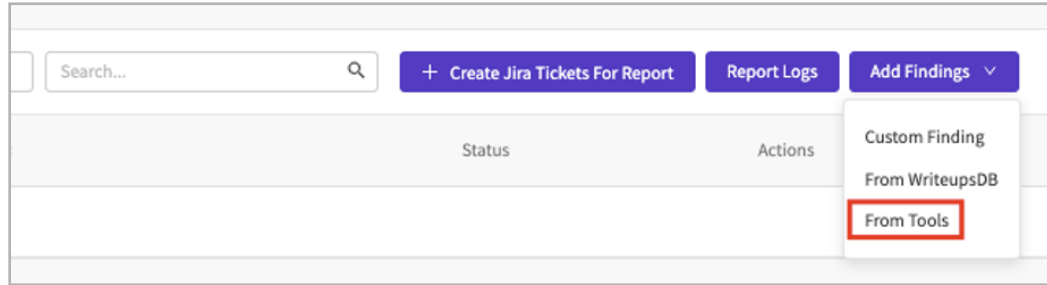
A few simple steps on our user-friendly interface and you'll be saving time while focusing on the real security work.

Step 1: Prepare to Add Findings to a Report

Navigate to the **Report Findings** section.

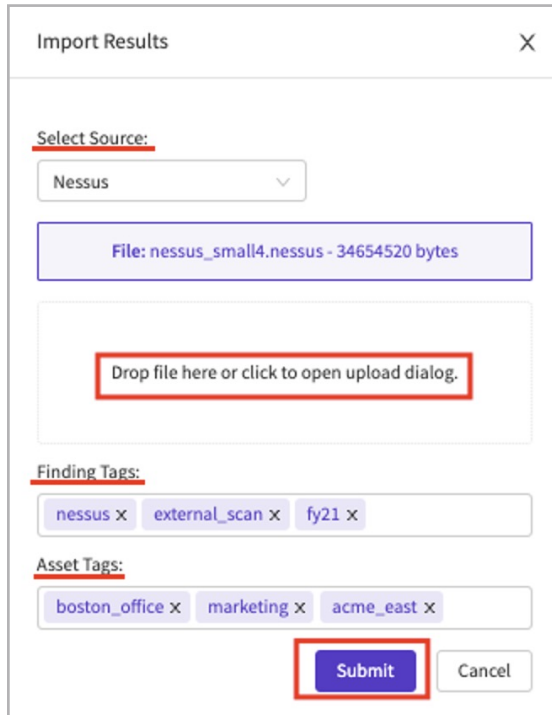


Select the “Add Findings” drop down, and then select the “From Tools” option.



Step 2: Choose Your Scanner Imports

A modal titled “Import Results” will appear. From here, you will use the “Select Source” drop down and choose the tool that the data is coming from (i.e. Nessus, Burp, Qualys). Additionally, you can 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.”

A screenshot of a table titled 'REPORT FINDINGS'. The table has columns for 'Severity', 'Finding Title', 'Assigned To', 'Data Reported', 'Status', and 'Actions'. It contains several rows of data, each representing a finding. The first row is highlighted in yellow. A large grey arrow points from the 'Import Results' modal to this table.

Severity	Finding Title	Assigned To	Data Reported	Status	Actions
Critical	KB422710: Windows 10 Version 1607 and Windows Server 2016 June 2017 Cumulative Update	Not Assigned	8/31/2021	Open	[Icons]
Critical	Windows Server 2012-June 2017 Security Updates	Not Assigned	8/31/2021	Open	[Icons]
Critical	KB4375339: Windows 10 Version 1607 and Windows Server 2016 July 2017 Cumulative Update	Not Assigned	8/31/2021	Open	[Icons]
Critical	FP-110-4 == 2.52 RCE	Not Assigned	8/31/2021	Open	[Icons]
Critical	KB4301110: Security update for Adobe Flash Player (April 2016)	Not Assigned	8/31/2021	Open	[Icons]
Critical	T.0p+ 18.05 Memory Corruption Arbitrary Code Execution	Not Assigned	8/31/2021	Open	[Icons]













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.



Aggregate All the Data from Red Team Operations with PlexTrac

Managing the data doesn't have to be a drag. Easily import the data from all your network and application scanning tools — and data from your service providers — into PlexTrac where it can be triaged and used by ALL team members.

Status	Actions
Open	    Edit
Open	   
Open	   

Blue Team Remediation

Most of the daily cybersecurity work falls under the blue team function — remediating vulnerabilities and maintaining systems. Often those dealing with the results of penetration tests and automated scanners aren't even considered part of the cybersecurity team but rather are IT analysts and other network and system administrators.

Teams need efficient ways to communicate, track, and remediate findings from automated scanners and red team exercises. All that knowledge is useless if nothing ever happens with it. Many organizational cybersecurity teams already have workflow tools in place that help their blue teamers or IT analysts assign and manage remediation tasks. But identifying and moving the pertinent information from reports and scanning tools into a ticketing system is just one more bottle neck, particularly if those receiving the tasks aren't dedicated cybersecurity team members.

With PlexTrac, cybersecurity teams can make better use of the data and improve collaboration with everyone responsible for protecting the parameter. PlexTrac offers tracking and ticketing in the platform and simple integrations with major ticketing systems to make and track remediation progress.

An Integrated Platform to Manage Remediation

With PlexTrac's built in integrations with Jira and ServiceNow, you can coordinate workflows within the team and with the rest of the organization. PlexTrac makes it easy for users to find and use the information they need to get the right work done.

How to Use the Jira Integration in PlexTrac

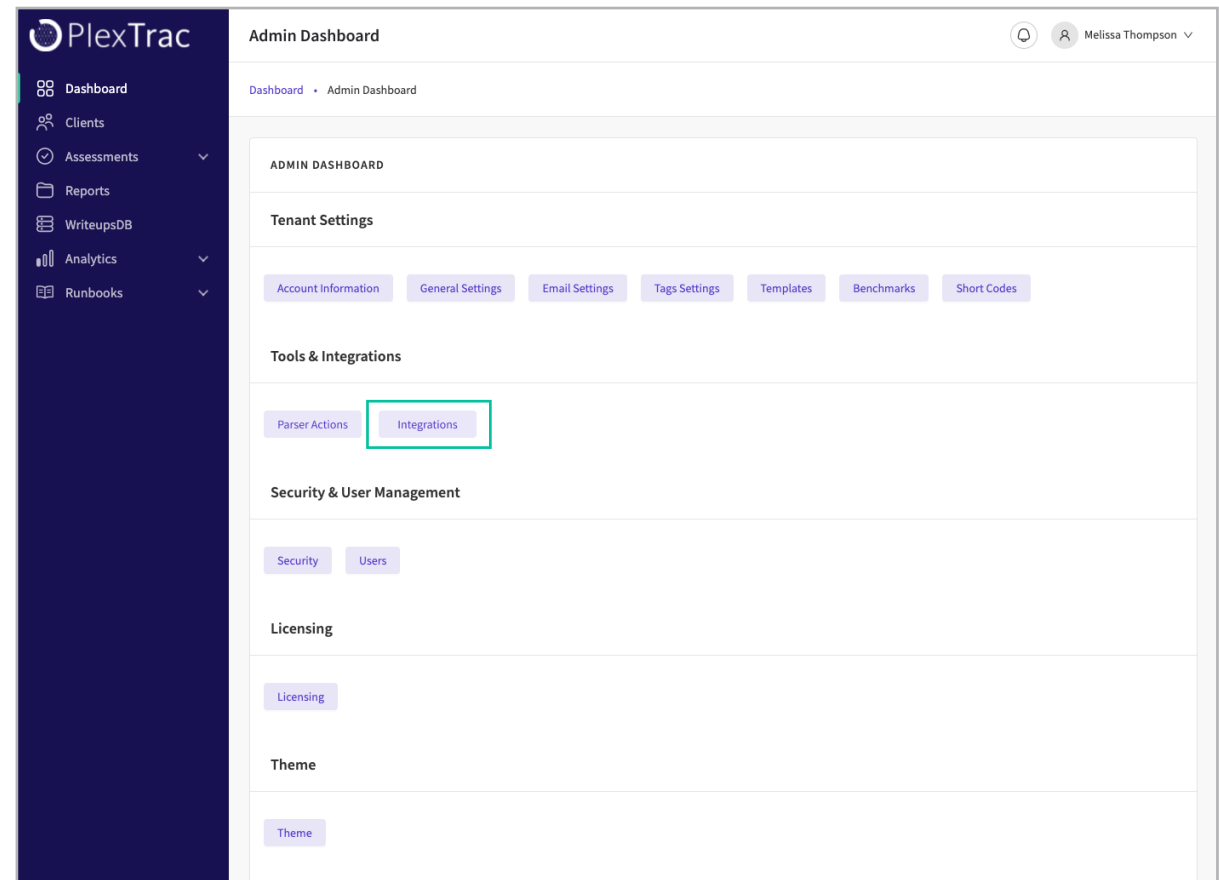
PlexTrac's robust integration with Jira offers extensive customization options.

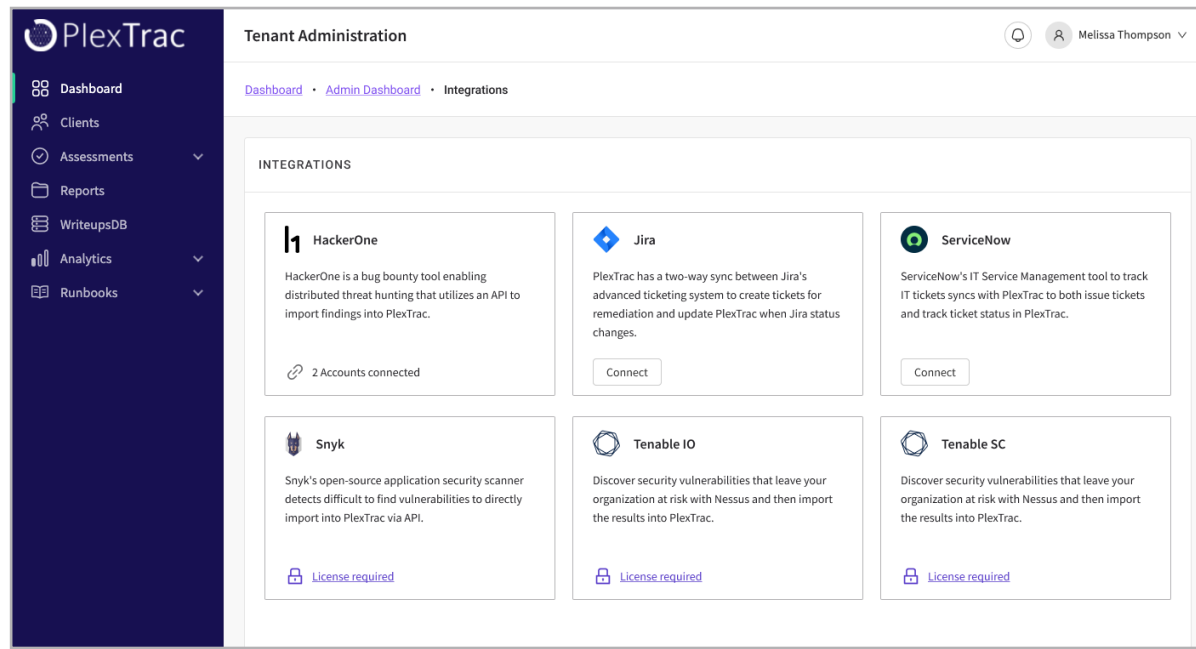
Step 1: Locate Your Preferred Integration

Navigate to the Admin Dashboard. Under Account Admin > Tools & Integrations > Integrations > you'll find the "Jira" integration tile with the "Connect" button. Under Jira, click **"Connect."**



Teams need efficient ways to communicate, track, and remediate findings from automated scanners and red team exercises.

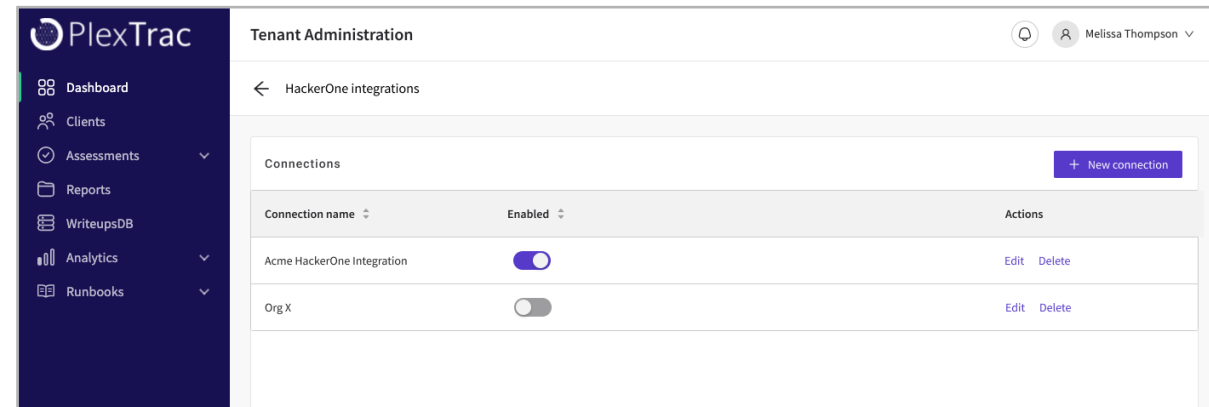




With PlexTrac's built in integrations with Jira and ServiceNow, you can coordinate workflows within the team and with the rest of the organization.

Step 2: Configure the Integration



Click on the “+ **New connection**” button to access the steps to configure and customize the integration.



Select **“Connect to Jira Cloud”** or **“Connect to Jira Server”** and fill out the 3 fields required, then click **“Save & Continue.”**


Create new Jira connection

1 Configure & connect > 2 Select projects > 3 Map fields > 4 Select settings & save

 + 

Create a new PlexTrac and Jira connection

Connect PlexTrac to a Jira instance.

 **Connect to Jira Cloud**

Jira URL


Usually [company name].atlassian.net

Username

Usually your email address

API Key

Generated in Jira

 **Connect to Jira Server**

Jira Cloud API key help

1. Log into Jira Software or Confluence and click your profile image.
2. Open Profile.
3. Click Manage Your Profile.
4. Navigate to Security.
5. Scroll down a little and click Create and manage API tokens.
6. Click Create API token.
7. Enter a Label and click Create.

Complete all fields to continue.

If information is filled out correctly and connection is made, you'll have the options to select which Jira projects to create issues within. You have the option to **“Save as draft”** or make the selections and **“Continue with ‘X’ projects.”**

Create new Jira connection

1 Configure & connect > **2 Select projects** > 3 Map fields > 4 Select settings & save

Select Jira projects to create issues within.

<input type="checkbox"/>	Project name	Key	Type	Lead
<input type="checkbox"/>	Tasty Soft Chicken	TSC	Team-managed software	James Botosh
<input checked="" type="checkbox"/>	Gorgeous Wooden Computer	GWC	Team-managed software	Alena Curtis
<input checked="" type="checkbox"/>	Sleek Rubber Towels	SRT	Team-managed software	Marilyn Gouse
<input type="checkbox"/>	Small Plastic Keyboard	SPK	Team-managed software	Terry Gouse
<input type="checkbox"/>	Licensed Steel Soap	LSS	Team-managed software	Lincoln Septimus
<input checked="" type="checkbox"/>	Fantastic Steel Pants	FSP	Team-managed software	Martin Curtis
<input type="checkbox"/>	Incredible Steel Bacon	ISB	Team-managed software	Lydia Passaquindici Arcand
<input type="checkbox"/>	Practical Granite Mouse	PGM	Team-managed software	Corey Septimus
<input checked="" type="checkbox"/>	Tasty Granite Cheese	TGC	Team-managed software	Allison Passaquindici Arcand
<input type="checkbox"/>	Rustic Wooden Gloves	RWG	Team-managed software	Paityn Workman
<input checked="" type="checkbox"/>	Handmade Cotton Chicken	HCC	Team-managed software	Ryan Calzoni
<input type="checkbox"/>	Rustic Cotton Tuna	RCT	Team-managed software	Ruben Lubin
<input type="checkbox"/>	Awesome Granite Chair	AGC	Team-managed software	Ruben Baptista
<input type="checkbox"/>	Sleek Wooden Cheese	SWC	Team-managed software	Tiana Calzoni

Selecting Jira projects help

Select projects which you will need to push Jira tickets to. Once connected, you will be able to select the project, Jira issue type, and project board (optional) for each finding you connect to a Jira issue.

Cancel Save as draft **Continue with 6 projects**

Next, you can map fields for your epic, story, or task. This example will walk through mapping an epic. As a default, similar fields like severity will be mapped automatically, but you can change these mappings to better fit your workflow.

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

Gorgeous Wooden Computer
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
Workflow Mapping		
Open	→	In Review
In Progress	→	Doing
Closed	→	Done
	→	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.

[Mapping direction details](#)

Cancel Save as draft **Save & continue**

Clicking on the “**sync direction**” button will open an expanded selector which will allow you to customize and select which sync direction works best: Jira to PlexTrac, Bidirectional, PlexTrac to Jira (Continuous sync) or PlexTrac to Jira (One-time sync). Click “**Save & Continue.**”

Sync Direction Button

Clicking on the direction button pops open an expanded selector



Hovering a button should display a tooltip



Configure the connection settings by selecting a Jira user that will be shown as the updater in PlexTrac and set the frequency that the data is refreshed.

Create new Jira connection ✕

✓ Configure & connect > ✓ Select projects > ✓ Map fields > **4** Select settings & save

Configure the connection settings.

Sync Jira updates as user

RC Ryan Calzoni ▾

Jira user that is shown as the updater in PlexTrac

Refresh frequency

Every 30 minutes ▾

Set the frequency that the data is refreshed

Connection Settings

Sync Jira updates as user

When updates sync from Jira to PlexTrac, this Jira user will be reflected as the finding updater. If you don't want a specific user reflected, you can create a [service account](#) in Jira and select it as the user here.

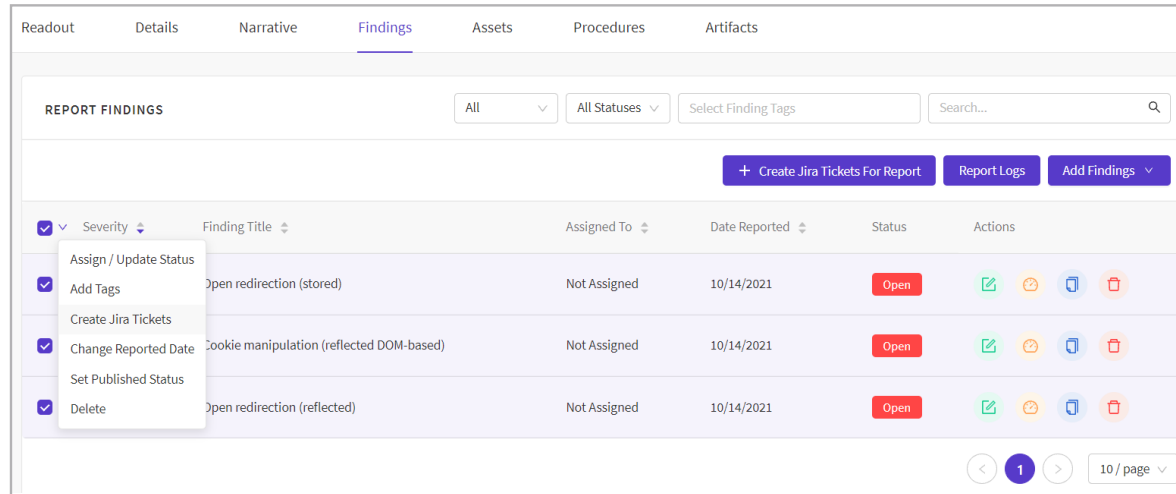
Refresh frequency

Choose how often data will refresh. This frequency is for syncing from PlexTrac to Jira and Jira to PlexTrac.

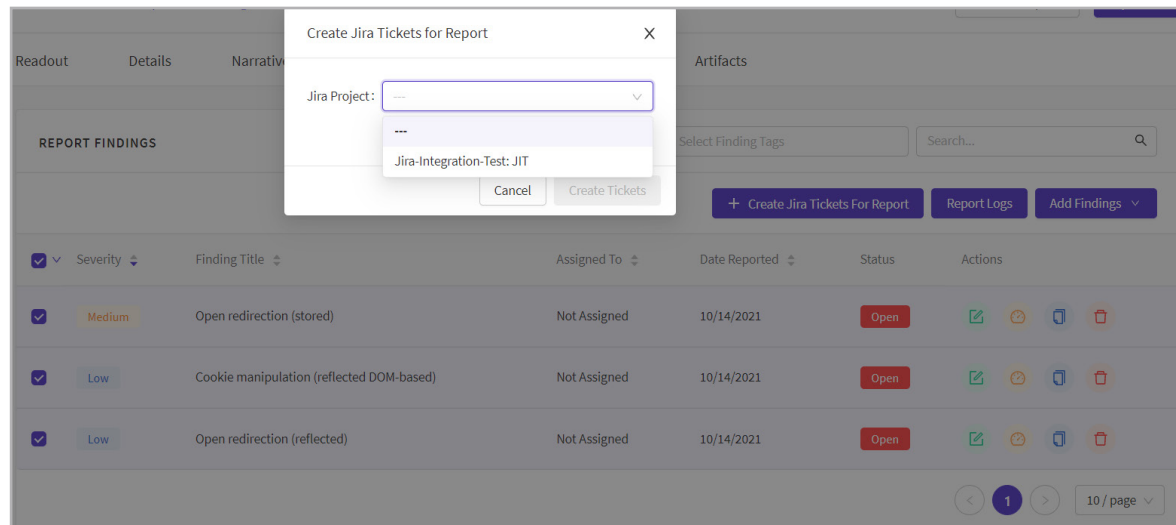
Cancel Save as Draft Save & Enable

Step 3: Create a Ticket

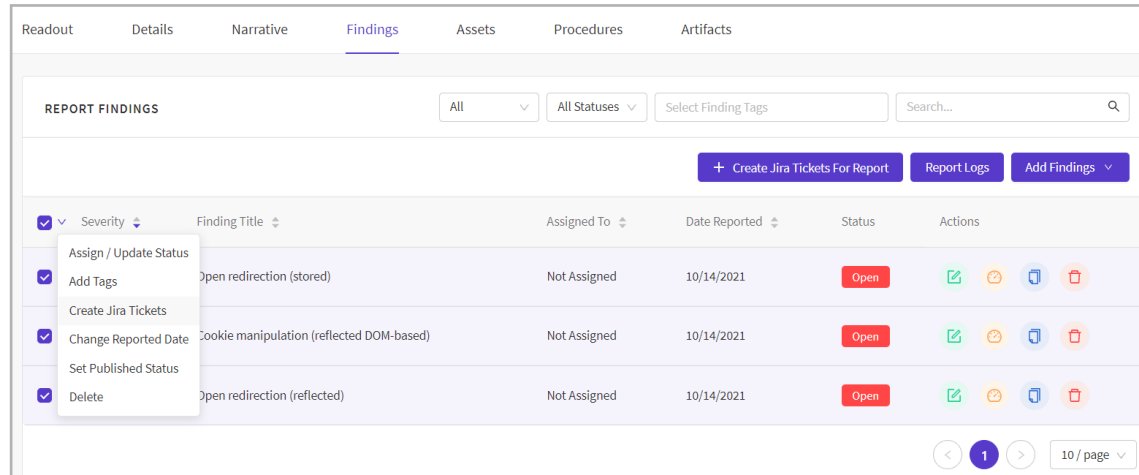
To create a Jira ticket, navigate to a report, and you will see a couple of different areas for creating tickets.



The “+ Create Jira Tickets for Report” button will generate a Jira ticket for whichever Jira project you select.



You can also select multiple tickets and use the bulk selection dropdown to get to the same Jira project selection modal.



Finally, you can click on an individual finding, then click on the **Status button**, and create a ticket for this one finding.



Open redirection (stored)

Report
testing

Description
Open redirection vulnerabilities arise when an application incorporates user-controllable data into the target of a redirection in an unsafe way. An attacker can construct a URL within the application that causes a redirection to an arbitrary external domain. This behavior can be leveraged to facilitate phishing attacks against users of the application. The ability to use an authentic application URL, targeting the correct domain and with a valid SSL certificate (if SSL is used), lends credibility to the phishing attack because many users, even if they verify these features, will not notice the subsequent redirection to a different domain.

Recommendations

FINDING ID
1926750124

STATUS
Open

SEVERITY
Medium

ASSIGNEE
Not Assigned

DATE REPORTED
10/14/2021

Findings > Stone > Reports > Testing > Findings

Finding Data

Finding Status Tracker: Open redirection (stored)

+ Add Update

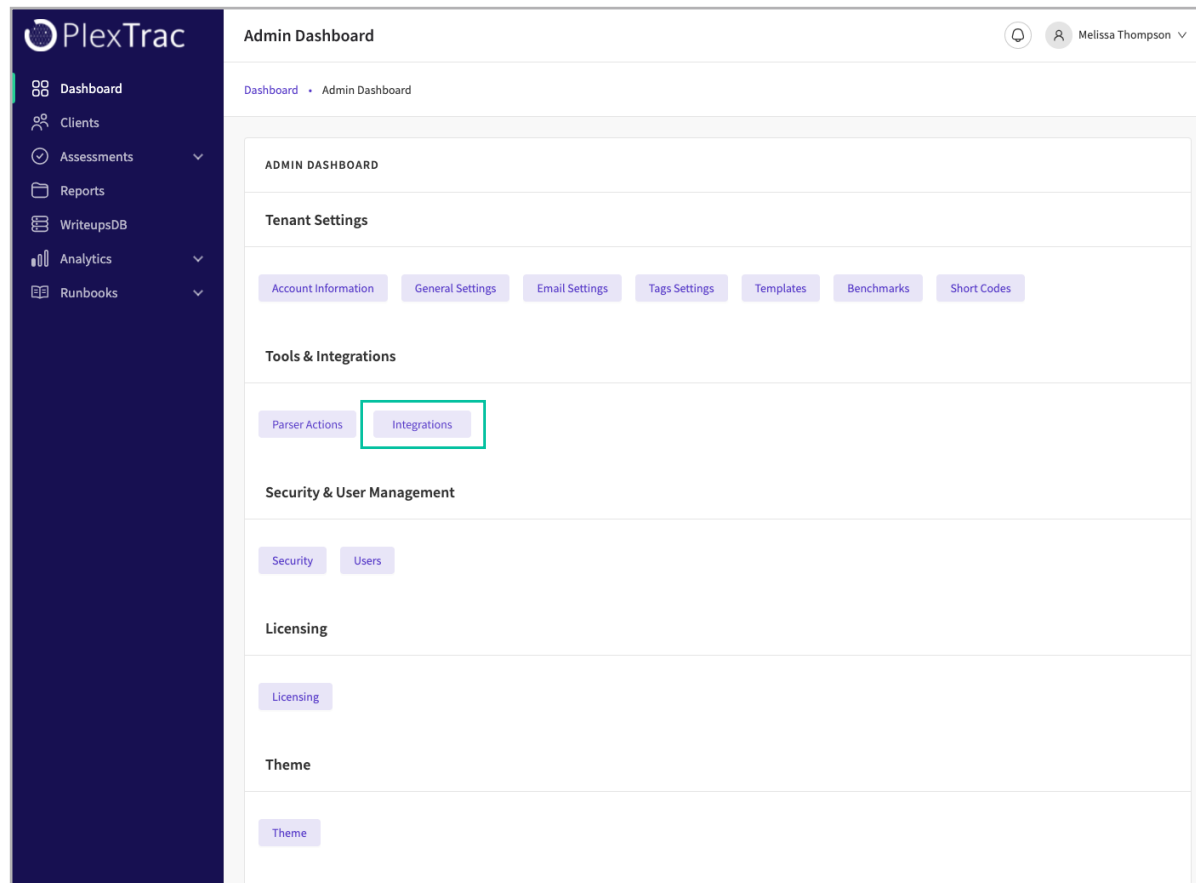
Create Jira Ticket & Link

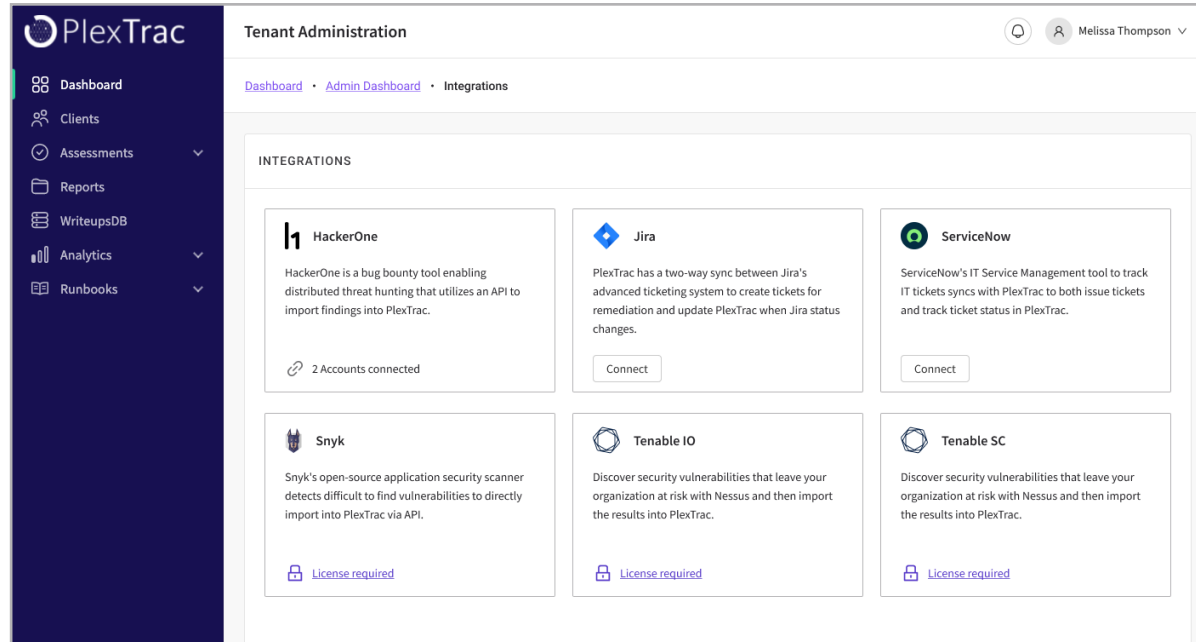
How to Use the ServiceNow Integration in PlexTrac

PlexTrac’s integration with ServiceNow is easy to set up and simple to use.

Step 1: Locate Your Preferred Integration

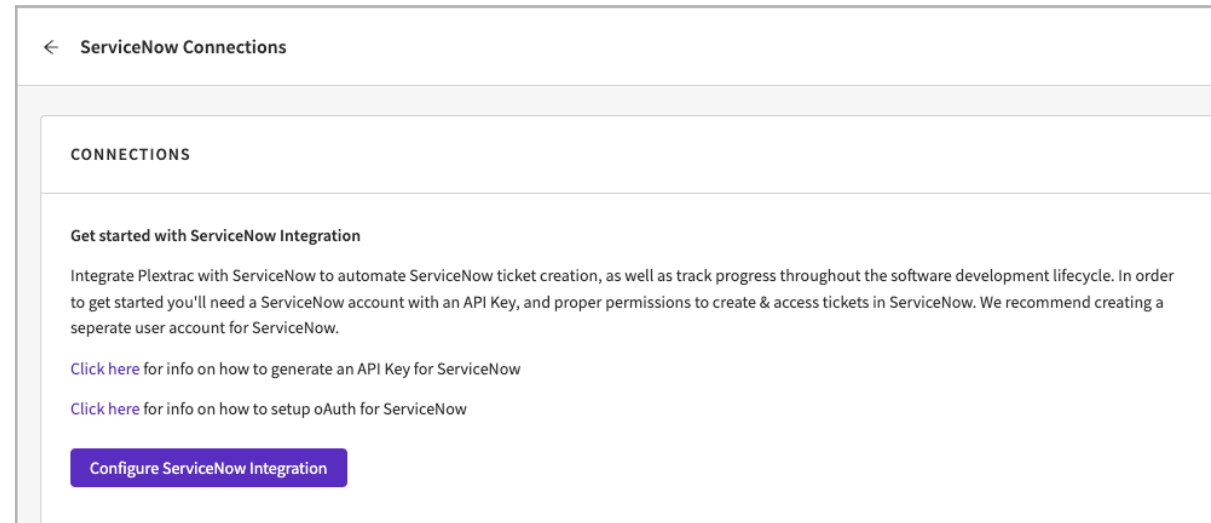
Navigate to the Admin Dashboard. Under Account Admin > Tools & Integrations > Integrations > you’ll find the “**ServiceNow**” integration tile with the “**Connect**” button. Under ServiceNow, Click “**Connect.**”





Step 2: Configure the Integration

When you click on the “**Configure ServiceNow Integration**” button, you will see three fields. Fill them out and click “**Test Connection**” and once successful, click “**Next.**”



Configure Your ServiceNow Integration
×

1 Connecting to ServiceNow
 2 Available Modules

Connect to Service Now

ServiceNow Instance

Your setup ServiceNow instance

Username

Used to log in to Service Now

ServiceNow API Key or Password

ServiceNow account password

Connect oAuth Service Now

Step 3: Create a Ticket

To create a ticket with ServiceNow, navigate to a report, click on a finding to open the modal, and click on **Status**.

Open redirection (stored)

FINDING ID

Report testing
Finding Status Tracker: Open redirection (stored)
×

+ Add Update

🔗 Create Jira Ticket & Link

🔗 Create ServiceNow Ticket & Link

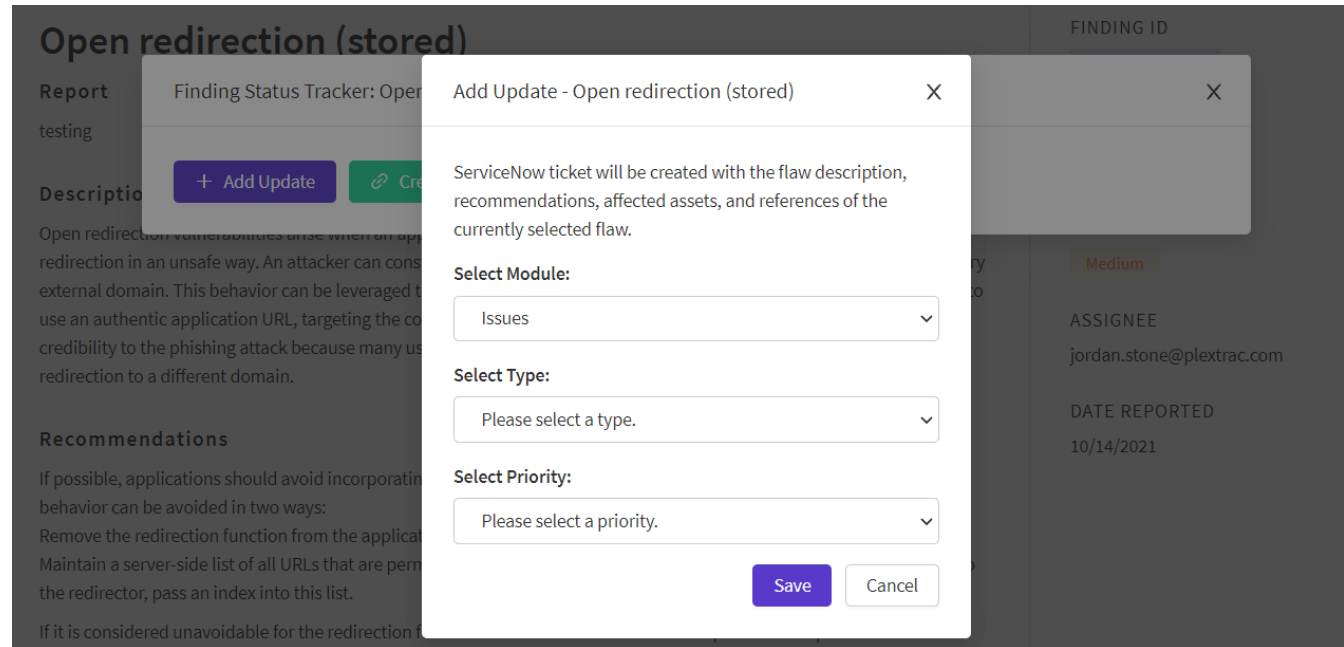
Description

Open redirection vulnerabilities arise when an application incorporates user-controlled data into the target of a redirection in an unsafe way. An attacker can construct a URL within the application that causes a redirection to an arbitrary external domain. This behavior can be leveraged to facilitate phishing attacks against users of the application. The ability to use an authentic application URL, targeting the correct domain and with a valid SSL certificate (if SSL is used), lends credibility to the phishing attack because many users, even if they verify these features, will not notice the subsequent

Medium

ASSIGNEE

Here you can see the available fields for your ServiceNow ticket creation. Click **Save** and your ticket is now created!



Track and Manage Remediation with PlexTrac Integrations

Assuring the work gets done doesn't have to be so hard. Easily integrate the ticketing tools your blue teamers and analysts are already using into PlexTrac for streamlined workflow from finding to fix.



Stakeholder Communication

Cybersecurity teams within organizations are responsible not only for keeping the crown jewels secure but also for planning, communicating, and justifying their strategies to various constituents both internally and externally. It's easy to feel pulled in many directions or to want to take the “just trust us” approach.

Being able to easily view the analytics of your security posture is a much better way to create a security strategy, allocate and lobby for resources, and keep all constituents informed. Whether prioritizing the most critical findings for the blue team analysts or communicating a macro-level view to the C-suite, teams need to track signal through the noise.

With PlexTrac, cybersecurity teams can gain a real-time view of their security posture with robust analytics. PlexTrac's Analytics module lets you slice and dice your data with infinite filtering to tailor the view to the needs of the audience and track progress over time.

One Platform to Produce Analytics for Constituents

The Analytics module enables users to view and visualize vulnerability data at all levels of detail — from a single tag on a finding to a summary of risks and vulnerabilities across the organization.

Whether prioritizing the most critical findings for the blue team analysts or communicating a macro-level view to the C-suite, teams need to track signal through the noise.

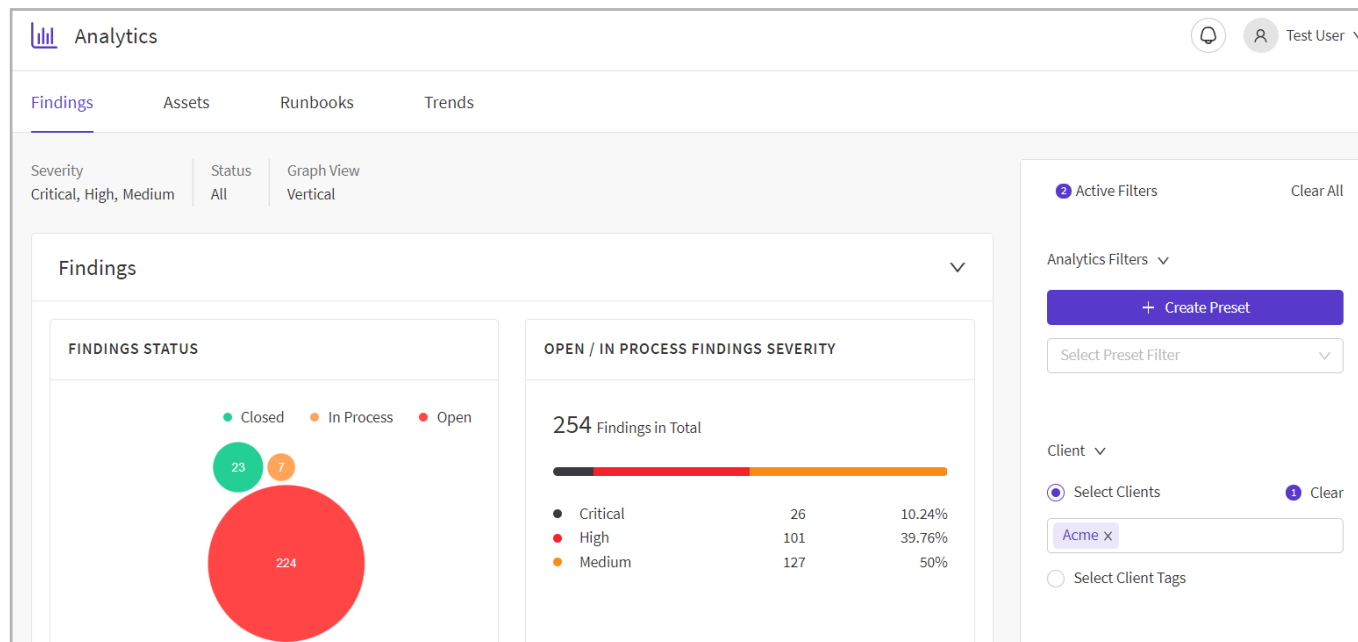
How to View Analytics of Findings in PlexTrac

Creating robust yet understandable analytics and visualizations of your findings in PlexTrac is quick and easy.

Step 1: Filter to Find Data

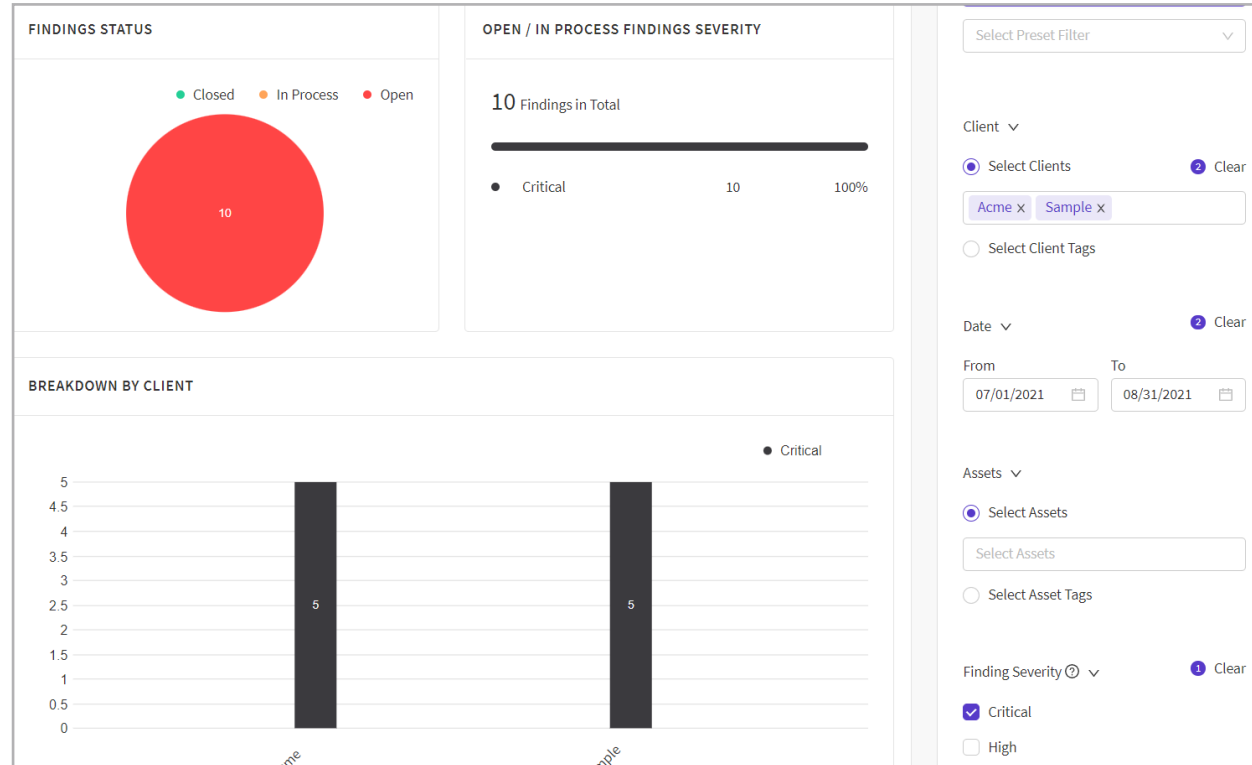
In the Analytics module, you'll see four tabs: **Findings**, **Assets**, **Runbooks**, **Trends**.

Open the **Findings** tab and select one or more filters on the right hand panel to get the data you're looking for.

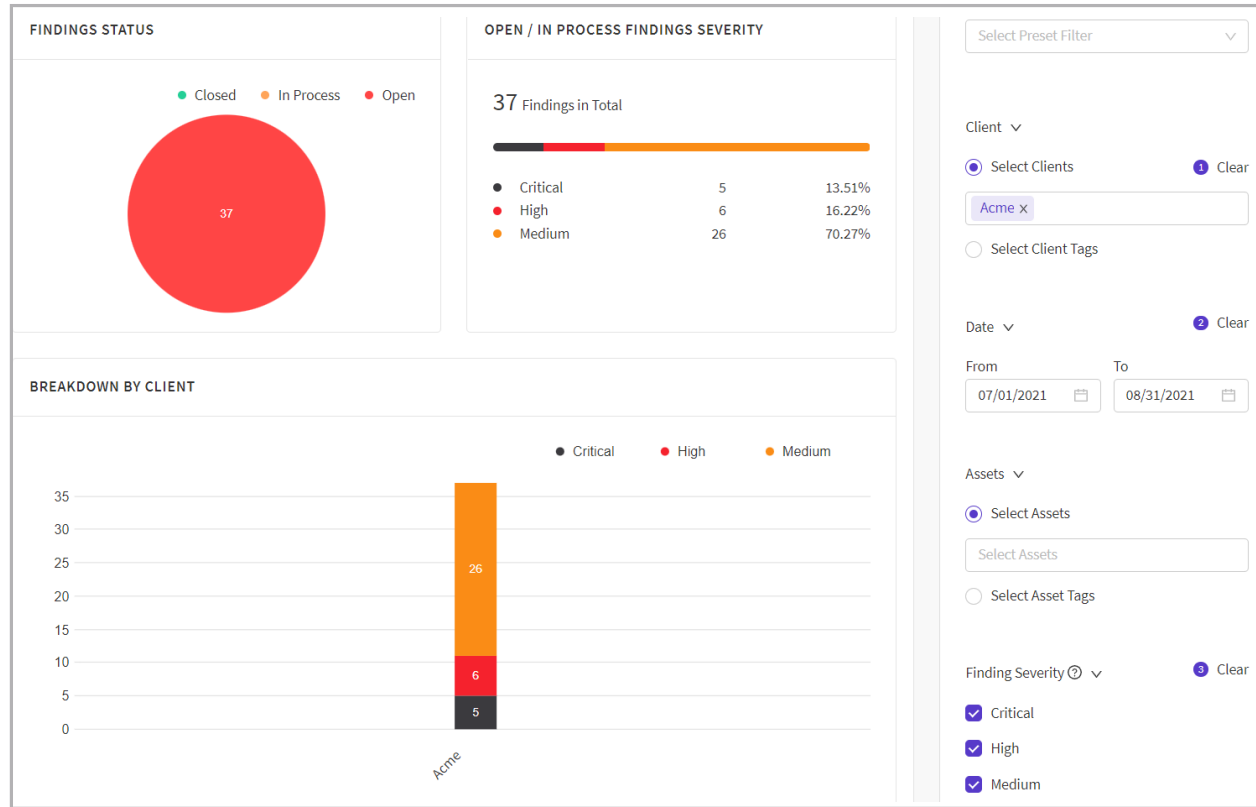


Step 2: View the Analytics or Apply More Filters

Parse your finding however necessary to get the information and view needed. The example below shows findings filtered by two different clients and a severity of “**Critical**.”



Adding back in “High” and “Medium” severity findings and removing the sample client provides a different view.



The 'Active Filters' panel shows the current filters applied: Client (Acme), Date (07/01/2021 to 08/31/2021), and Finding Severity (Critical, High, Medium). A red arrow points to the 'Clear All' button in the top right corner of the panel.

Step 3: Clear to View More Analytics

Select “Clear All” on the top right to reset to the broadest view of findings data. Add new filters to instantly see new breakdowns and visualizations of information.



Communicate Your Security Posture Using PlexTrac Analytics

Whether strategizing and allocating resources or attesting to your security posture and program, cybersecurity teams need to harness their data in a meaningful way. PlexTrac Analytics is the answer to understanding your most critical issues at a glance.

Continuous Purple Teaming Assessments

A [recent survey of industry professionals](#) revealed that 88 percent of purple teaming users — compared to only 52 percent of red/blue team users — say their exercises are “very effective” in defending their organization against ransomware and advanced attacks.

Cybersecurity teams of every size and maturity need to start reaping the benefits of being purple. Adopting a continuous assessment mindset that prioritizes short iterative cycles of adversary emulation activities can improve the security posture of any organization. But where to start can be daunting!

PlexTrac is the Purple Teaming Platform. It exists to improve collaboration and communication between offensive and defensive teams and to make continuous purple teaming assessments accessible for every security team. PlexTrac’s Runbooks module is the best-in-industry solution for test plan execution.

A Platform Designed for Collaboration

Runbooks is a purple team module that allows you to get the best of both worlds (red and blue teams) in a pentesting engagement.

Adopting a continuous assessment mindset that prioritizes short iterative cycles of adversary emulation activities can improve the security posture of any organization.

How to Create a Runbook Engagement in PlexTrac

Planning, executing, and reporting a purple team engagement in Runbooks couldn't be simpler.

Step 1: Select TTPs

Go to the Runbooks tab under Runbooks and click **“Create.”** From here, you can select your TTPs.

Runbook Title

Runbook Example

Add content to your Runbook

Select one or multiple Tactics, Techniques and/or Procedures

Tactics Techniques Procedures Review

Select All Clear All

+	TA0001	Initial Access	✓
+	TA0002	Execution	
+	TA0003	Persistence	✓
+	TA0004	Privilege Escalation	✓



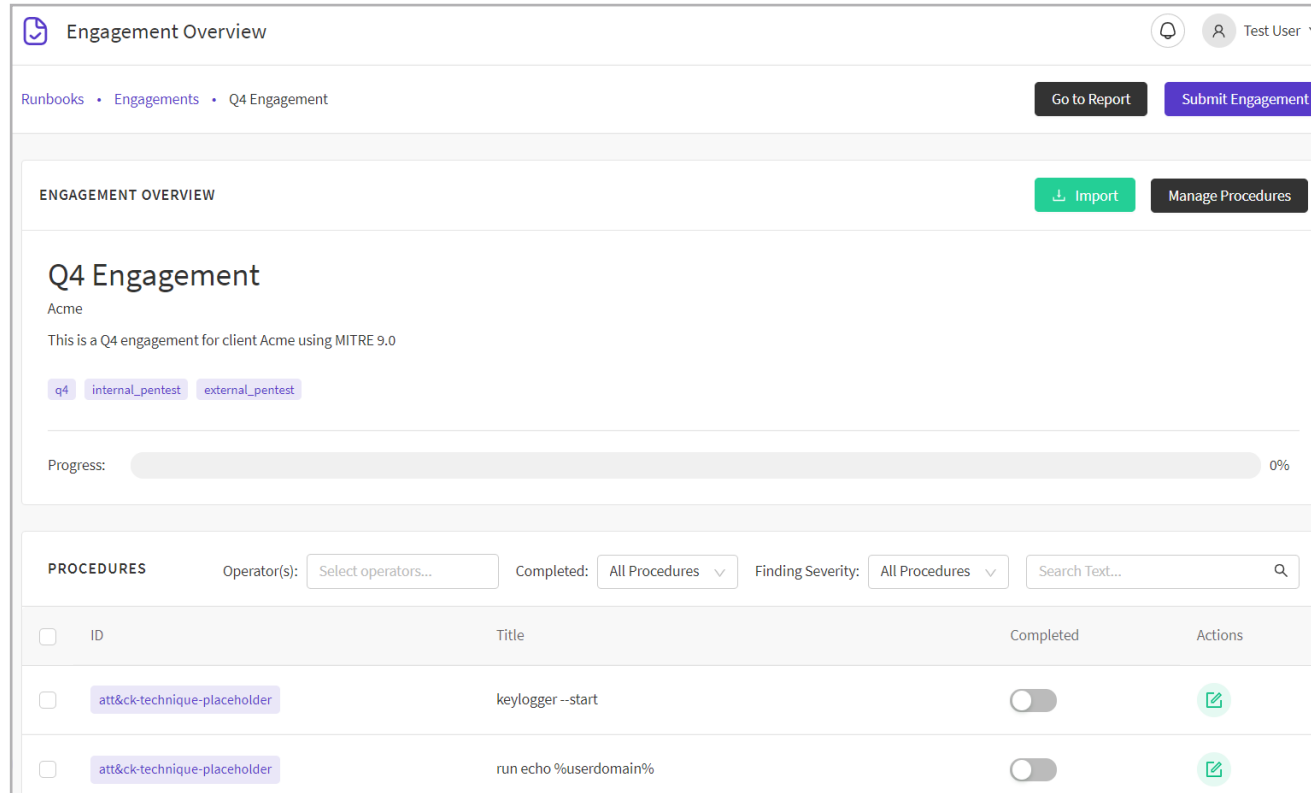
The Review tab will show you which procedures you selected and will be included in your runbook each time you start an engagement.

The screenshot shows the 'Create Runbook' interface. At the top, there is a breadcrumb trail: 'Runbooks > Runbook Example > Create'. To the right of the breadcrumb are two buttons: 'Save and Close' and 'Save and Continue'. Below the breadcrumb is a section titled 'RUNBOOK INFO' with a 'Runbook Title' field containing 'Runbook Example'. Underneath is a section titled 'Add content to your Runbook' with the instruction 'Select one or multiple Tactics, Techniques and/or Procedures'. There are four tabs: 'Tactics', 'Techniques', 'Procedures', and 'Review' (which is selected and underlined). To the right of the tabs is a search box labeled 'Search Text...'. Below the tabs is a list of three items, each with a placeholder 'att&ck-technique-placeholder' on the left and a command on the right: 'keylogger --start', 'run echo %userdomain%', and 'run net user APT41 Passw0rd! /add'.

Tactics	Techniques	Procedures	Review
att&ck-technique-placeholder	keylogger --start		
att&ck-technique-placeholder	run echo %userdomain%		
att&ck-technique-placeholder	run net user APT41 Passw0rd! /add		

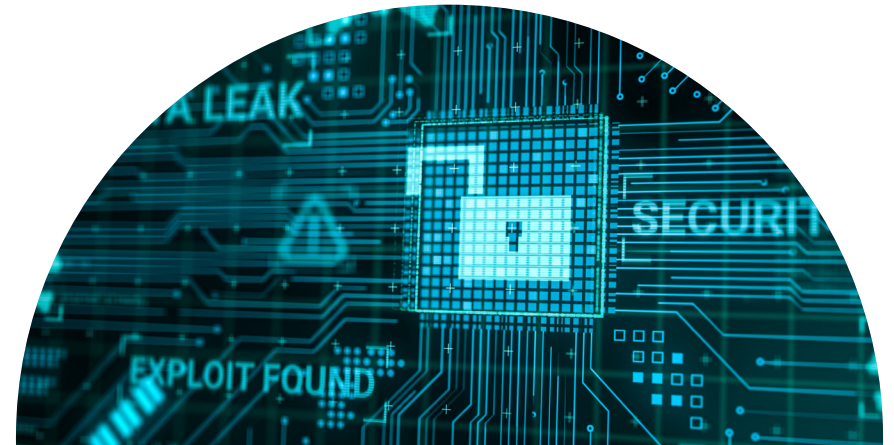
Step 2: Input Data

After your engagement is started, you can now click into each procedure to input all your data.



The screenshot displays the 'Engagement Overview' page for a 'Q4 Engagement' for client 'Acme'. The page includes navigation links for 'Runbooks', 'Engagements', and 'Q4 Engagement', along with buttons for 'Go to Report' and 'Submit Engagement'. The 'ENGAGEMENT OVERVIEW' section features an 'Import' button and a 'Manage Procedures' button. Below this, the engagement details are shown, including a progress bar at 0%. The 'PROCEDURES' section contains a table with columns for ID, Title, Completed, and Actions. The table lists two procedures, both with 'att&ck-technique-placeholder' as the ID and 'run echo %userdomain%' as the title. The 'Completed' column shows toggle switches, and the 'Actions' column shows edit icons.

ID	Title	Completed	Actions
att&ck-technique-placeholder	keylogger --start	<input type="checkbox"/>	
att&ck-technique-placeholder	run echo %userdomain%	<input type="checkbox"/>	



Blue team

Red Team Blue Team

ATTACK OUTCOME
Partially Successful

EXECUTION STEPS 1 Step in Total

keylogger --start	
-------------------	--

DETECTION OUTCOME
 Detected/Blocked Detected/Alerted Forensically Logged No Evidence

ATTACHMENTS [Attach](#)

Title	Actions
sergei-akulich--heLWtuAN3c-unsplash.jpg	<input checked="" type="checkbox"/>
luca-bravo-ESkw2ayO2As-unsplash.jpg	<input checked="" type="checkbox"/>

[Expand View](#)

TARGETED ASSETS [Add Asset](#)

Asset	Actions
10.10.11.10	<input checked="" type="checkbox"/>
Defensive Outcome: <input type="radio"/> Detected/Blocked <input type="radio"/> Detected/Alerted <input checked="" type="radio"/> Forensically Logged <input type="radio"/> No Evidence	
10.10.11.11	<input type="checkbox"/>
Defensive Outcome: <input checked="" type="radio"/> Detected/Blocked <input type="radio"/> Detected/Alerted <input type="radio"/> Forensically Logged <input type="radio"/> No Evidence	

Step 3: Submit the Engagement to Report

Once all your procedures have been completed, submit your engagement, which then turns it into a report under the client you selected!

The screenshot shows a web interface for a report titled "Report Readout: Q4 Engagement". The breadcrumb trail is "Clients > Acme > Reports > Q4 Engagement". Navigation buttons include "Go to Engagement", "Search & Replace", and "Export". The main content area has tabs for "Readout", "Details", "Narrative", "Findings", "Assets", "Procedures", "Artifacts", and "Attack Path". The "Readout" tab is active, displaying a "REPORT NARRATIVE" section with an "Edit/Comment" button. Below this is a "FINDINGS OVERVIEW" table and a "FINDINGS STATUS" pie chart. The "REPORT READOUT" section on the right lists findings with their severity levels and associated commands.

Severity	Open	In Process	Closed
Critical	1	0	0
High	1	0	0
Medium	1	0	0
Low	1	0	0
Informational	0	0	0

FINDINGS STATUS

Legend: Open (Red), In Process (Orange), Closed (Green)

REPORT READOUT

- Report Narrative
- Medium: `run echo %userdomain%`
- Low: `run net user APT41 Passw0rd! /add`
- Critical: Test Ability to Forge Requests


Purple Team with PlexTrac Runbooks

Leveraging continuous assessment and collaboration between teams is possible for every internal security team regardless of size or program maturity. With PlexTrac Runbooks, any team can start testing their defenses with proven adversary emulation plans on a platform designed to pull all the pieces together.



Adopt PlexTrac as a Cybersecurity Team

Cybersecurity teams within organizations have to do it all. Why not help everyone on the security team work more effectively and efficiently and begin taking advantage of a purple teaming strategy? With PlexTrac, your cybersecurity team can gain control over its security posture and break down silos between stakeholders.

 *Schedule a live demonstration of PlexTrac today at plextrac.com/demo and level up the capabilities of your cybersecurity team.*



PlexTrac is a proactive cybersecurity reporting platform built to streamline the report writing of a variety of security assessments, provide a richer remediation and collaboration experience and make it easier to ensure teams are focusing on the right security work. For more information, please visit www.plextrac.com