Success Schema:

Enable, Configure and Detect with Panther

Now that you've reviewed the Quick Start guide and have access to your account's Panther Console, it's time to get fully onboarded to start generating alerts and investigating incidents. This checklist will walk you through the steps needed to make the most of Panther's features.

Please note that you will need to make a decision between managing your detections using the Panther Console or outside of the console using the Panther Analysis Tool. We will help you understand your options and make the initial choice that's best for your team.

If you need support, please reach out to your Panther account team.

Table of Contents

Onboarding Data

The first thing you should do is onboard your data sources and start ingesting logs. Please review our Data Sources & Transports documentation↗ for instructions on ingesting logs from common data sources, configuring data mapping for custom log sources, and ensuring you have a healthy data pipeline feeding into Panther.

Required

- □ Onboard logs with Panther-supported schemas
  - □ Supported logs ↗
  - □ Data Transports ↗
- □ Set up data pipeline health alerts
  - □ Set up an alert destination to receive System health notifications ↗
  - □ Monitoring log sources ↗

Recommended

- □ Create custom schemas for custom log types
  - □ Custom log types ↗
  - □ Generate schemas from S3 buckets ↗
- □ Set up cloud scanning
  - □ Cloud security scanning ↗

Detection Management

Now that your data is flowing into Panther, it's time to create your detections. You can create and manage detections in the Panther Console or by using developer workflows with the Panther Analysis Tool (PAT). We have specific checklists for using each option following the descriptions below.

Panther Console

You can leverage the Panther Console to fully customize your security program through out-of-the-box Detection Packs, as well as the option to create and customize detections to leverage the power of detections-as-code from one place.

Panther Developer Workflows

Panther offers different options for leveraging the detections in the panther-analysis GitHub repository as part of your developer workflow, allowing Panther detections to be deployed via Continuous Integration and Continuous Deployment (CI/CD).

Important Note: We strongly advise against using Detection Packs in the Panther Console if you are also using Developer Workflows such as PAT. Managing detections via both methods at the same time will result in unexpected behavior.

Don't forget about Alert Destinations!

Please note that while Panther's detection engine may be running in your account, your Alerts will only be visible within the Panther Console until you configure destinations for them. Review the Destination and Alert

Management section below if you want to activate Alert Destinations before proceeding with more advanced Detection work.

Detection Management in the Panther Console

Required

- □ Review and Activate Detection Packs
    - □ Detection Packs ↗
        - □ Review how to disable and enable individual detections ↗ within Detection Packs to ensure that your detections fit your needs.

Recommended

- □ Configure and Customize Rules
    - □ Create Real-Time Rules ↗
    - □ Create Scheduled Rules ↗
        - □ Scheduled Rules require Scheduled Queries (see Incident Investigations below)
    - □ Create Policies ↗
        - □ Policies require having a Cloud Account configured
- □ Set Up Real-Time Cloud Security Monitoring
    - □ Real-Time Monitoring ↗
- □ Test your Detections
    - □ Testing ↗
    - □ Data Replay ↗

Additional Options

- □ Review and leverage Panther Helper Functions ↗

Detection Management Using PAT for CI/CD Workflows

Use these resources to set up the Panther Analysis Tool (PAT) for developer workflows, including CI/CD.

Required

- ☐ Follow the CI/CD for Panther Content documentation to get started and keep up with Panther-built Detections
  - ☐ Using the Panther detections repo
  - ☐ Deployment workflows using Panther Analysis Tool

Recommended

If you are already managing detections in the Panther Console and wish to migrate to a CI/CD workflow, follow the migration steps.

- ☐ Migrating to a CI/CD Workflow

Additional Resources

- ☐ Video: Writing Custom Python Detections with Panther ↗
- ☐ Video: Writing Custom Python Detections with Panther, Part II ↗
- ☐ Video: Real-Time Alerts With Unified Data Models ↗

Destination and Alert Management

Once you have data in Panther and your detections are enabled, the next step is to set up your Alert Destinations to begin receiving alerts. See this Panther blog post to learn about the value of real-time alerting: Detect Everything, Real-Time Alerts As Needed ↗

Follow the resources below to enhance your detection and response capabilities.

Required

- ☐ Configure your Alert Destination
  - ☐ Destinations ↗
- ☐ Triage Detection Alerts and analyze related events in the Panther Console
  - ☐ Triaging Alerts ↗
  - ☐ Alert Summaries ↗
- ☐ Configure Alert Runbooks
  - ☐ Alert Runbooks ↗

Additional Resources

- ☐ Blog: Triage Alerts Faster with Alert Summaries ↗
- ☐ Blog: Activate Security Automation with Alert Context ↗

Incident Investigation and Data Analysis

Having all of your data readily available for search and investigation is critical for efficient threat hunting and incident triage.

Use Panther's Indicator Search and Data Explorer features to save precious time in your incident response process and conduct a thorough analysis and investigation review.

Required

- □ Search IOCs and standard data fields
  - □ Indicator Search ↗
- □ Execute SQL in the Data Explorer and view results
  - □ Data Explorer ↗
- □ Set Up Scheduled Queries
  - □ Scheduled queries ↗
- □ Triage Policy findings and view resource attributes
  - □ Cloud resource attributes ↗

Additional Resources

- □ Webinar: How to Detect and Investigate Threats with Panther ↗
- □ Blog: Find Patterns Quickly with Indicator Search Drill Down ↗
- □ Blog: Advanced Detections with Scheduled Queries ↗

Enrichment

Alert noise and false positives are often the most significant challenges that security teams face with security information and event management (SIEM).

Leverage Panther's built-in enrichment features to add valuable context to your Alerts and create more robust Detections to keep your team focused on critical alerts (reducing alert fatigue) by ruling out internet background noise in your detection and alerting logic.

Recommended

- ☐ Create Lookup Tables to add context to your detections and alerts
  - ☐ Lookup Tables ↗
- ☐ Configure enrichment data sources to reduce false positive alerts and enhance detections
  - ☐ GreyNoise ↗
  - ☐ IPInfo ↗

Additional Resources

- ☐ Blog: Improve detection fidelity and alert triage with Lookup Tables in Panther ↗
- ☐ Blog: Reduce false positives with GreyNoise threat intelligence in Panther ↗