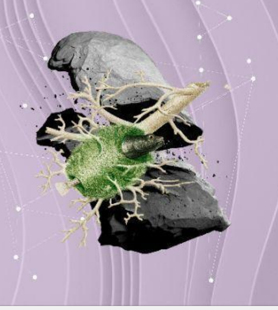
[P] | Prelude



Getting Started with Prelude Detect

Prelude Detect

Prelude Detect is the production-scale continuous security testing platform that helps organizations know with certainty that they are protected against the latest threats. Immediately.

Your Goals

Your goals in using Detect will inform which steps are most important and helpful. First-time users should begin by running Detect on one computer, with a handful of tests. After seeing Detect in action on one computer, run it on a small group of computers, e.g. with varying operating systems.

When testing computers with an enterprise EDR/EPP solution installed, tests may trigger notifications for your Security Operations team. This is good - the tests are being detected! - but your SecOps colleagues will appreciate a heads-up. See below for Alert Suppression methods depending on EDR Vendor.

Whether for one or multiple endpoints, the first steps are to:

- Create an account
- Select and schedule Verified Security Tests

Simple testing on one/several endpoints (development/test computers or your laptop)

- Install a Probe (instructions below) or run one ephemerally (requires use of the Prelude CLI; instructions)
- View results

Advanced testing with multiple endpoints in an Enterprise environment

- Configure your EDR to suppress alerts (*Crowdstrike, SentinelOne, and Microsoft Defender instructions below; contact support@preludesecurity.com for assistance with other EDRs*)
- Connect to your SIEM (*Splunk instructions below; contact support for other SIEMs*)
- Deploy Probes via a Crowdstrike integration (instructions below), Intune (*instructions*), Jamf (*instructions*), or your preferred software deployment tools. Probes can also run in containers.
- View results
- Assess failures and remediate
  - Ensure EDRs are installed and enabled
  - Ensure endpoint policies are applied, active, and effective as intended

Account

Register a Prelude account

Visit https://platform.preludesecurity.com, click “Sign up for a free account” in the top right, and complete the signup steps. Be sure to verify your account via the emailed link (unverified accounts are deleted after 24 hours).

Backup your account credentials

The previous step will create a keychain file which stores the credentials to your new account. Backup the keychain file by selecting your username in the top right and selecting “My Profile” and then clicking “Export Credentials”. Keep a backup of these credentials in a safe place, such as password manager.

Add users and manage permissions

Click the username dropdown in the top right corner of the UI; the “Manage users” item will allow you to add additional users to the account with different permissions.

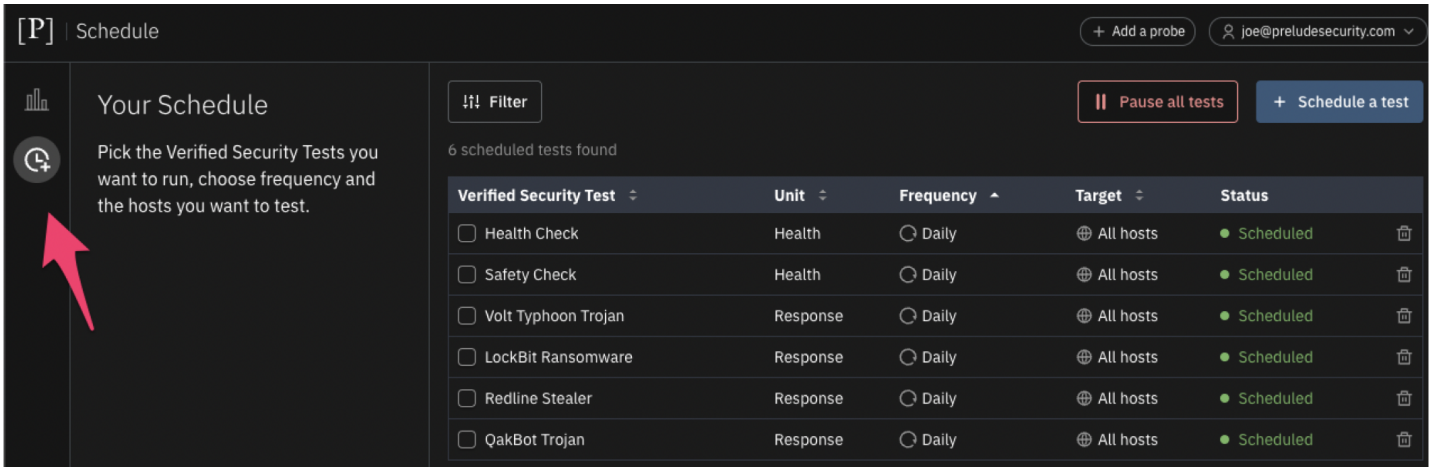
Verified Security Tests (VSTs)

View your VSTs

Every account has access to open-source security tests available through Detect. Notable tests - such as CISA Advisories - are tiled on the homepage. Alternatively, access the test catalog via the scheduling function: click the clock icon in the left sidebar. Click the question mark icon beside each test name for additional information.

Schedule VSTs for execution

You can schedule a test by selecting the clock icon on the left side of the Detect interface. From here, click “Schedule a test” and select the tests to be scheduled and their frequency.



Your Schedule

Pick the Verified Security Tests you want to run, choose frequency and the hosts you want to test.

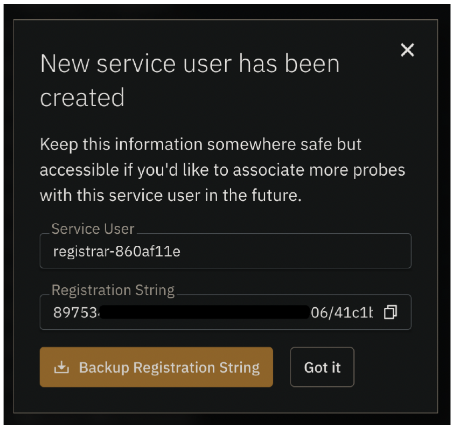
6 scheduled tests found

Verified Security Test	Unit	Frequency	Target	Status
□ Health Check	Health	Daily	All hosts	● Scheduled
□ Safety Check	Health	Daily	All hosts	● Scheduled
□ Volt Typhoon Trojan	Response	Daily	All hosts	● Scheduled
□ LockBit Ransomware	Response	Daily	All hosts	● Scheduled
□ Redline Stealer	Response	Daily	All hosts	● Scheduled
□ QakBot Trojan	Response	Daily	All hosts	● Scheduled

Probes

Generate a Registration String

A registration string is used to identify a probe to a service user within your account. Generate a registration string by clicking “Add a probe” in the top right and then select “Generate a registration string”. Save this string in a safe place if you later wish to deploy more probes on this service account. Your registration string will consist of <account id>/<token>, for example: mt04bs6rvobsi3cy2iio4bl9ysznkc6l/3ptupok7-6wni-lltx-l7sx-yku0k896rgrq



New service user has been created

Keep this information somewhere safe but accessible if you'd like to associate more probes with this service user in the future.

Service User: registrar-860af11e

Registration String: 89753[redacted]06/41c1t

Download a Probe

Click “Add a probe” in the top right and select the operating system for which to download a probe installer.

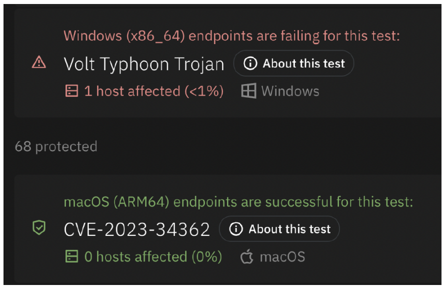
Install a Probe

Execute the probe installer and copy the Registration String into the installer when prompted. Continue clicking through the installer until it completes. The probe is now active and will persist on this host until it is uninstalled.

Results

Protected vs. Unprotected

The default “Decisions” view displays the number of affected hosts that are passing (green) or failing (red) each test. Using these insights you can make personalized security enhancements.



Windows (x86_64) endpoints are failing for this test:

Volt Typhoon Trojan

1 host affected (<1%) Windows

68 protected

macOS (ARM64) endpoints are successful for this test:

CVE-2023-34362

0 hosts affected (0%) macOS

Filter results

Click the “Operating Systems”, “Tags”, test unit (“Health”, “Response”) or test name to filter it from the results view. Use the filter to view results of one or more tests, operating systems, or tags.

Integrations

Configuring EDR Integrations

Prelude Detect integrates with a number of security vendors for enhanced capabilities:

Crowdstrike (setup here)

- IOC Submissions
- Prelude Probe deployment via RTR
- Reporting of Prevention Policies
- Prelude generated Alert Suppression

SentinelOne (setup here)

- Alert Suppression
- IOC Submissions
- Reporting of Prevention Policies

Microsoft Defender (setup here)

- Alert Suppression
- IOC Submissions
- Reporting of Prevention Policies

Configuring SIEM Integrations

Prelude Detect also supports the following reporting SIEM integrations:

Splunk (setup here)

Vectr (setup here)

Alert Management

Through the integrations Prelude Detect can automatically close any detections in the above listed integration partners:

- Crowdstrike Alert Suppression
- Sentinelone Alert Suppression
- Microsoft Defender Alert Suppression

Important Links

- What is Prelude CLI (used to install an ephemeral probe)
- VST result codes
- Persistent Probe Service Controls
  - Windows
  - Linux
  - macOS
  - containers
- Partner Integrations