An Introduction to Continuous Security Testing

HackSpaceCon - April 14, 2023

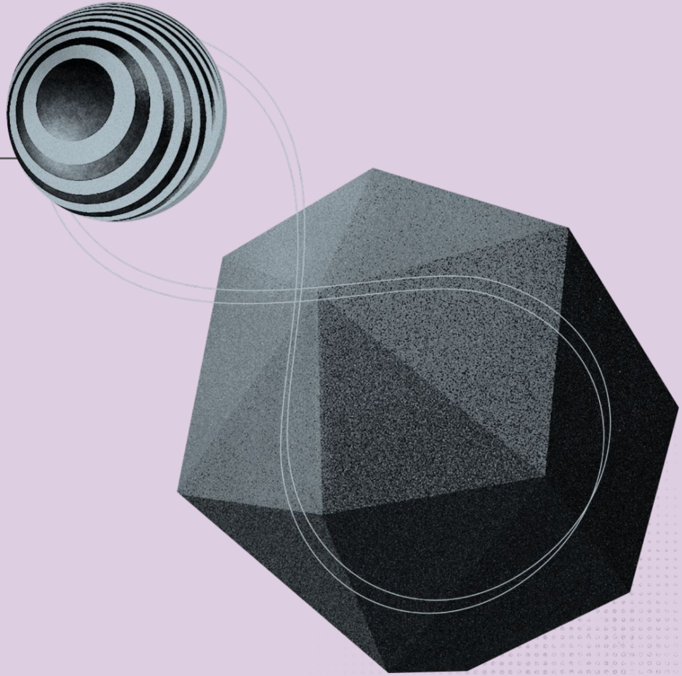
Octavia Hexe

Waseem Albaba

[P] | Prelude

preludesecurity.com

Who are we?



Octavia Hexe

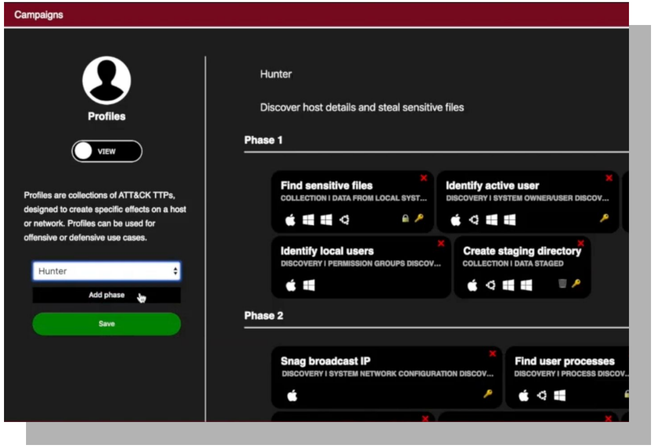
https://twitter.com/VV_X_7
https://haunted.computer/@VVX7

Waseem Albaba

https://twitter.com/gerbsec

[P]

Where we’ve come from



Profiles are collections of ATT&CK TTPs, designed to create specific effects on a host or network. Profiles can be used for offensive or defensive use cases.

Hunter

Hunter

Discover host details and steal sensitive files

Phase 1

Find sensitive files
COLLECTION | DATA FROM LOCAL SYST...

Identify active user
DISCOVERY | SYSTEM OWNER/USER DISCOV...

Identify local users
DISCOVERY | PERMISSION GROUPS DISCOV...

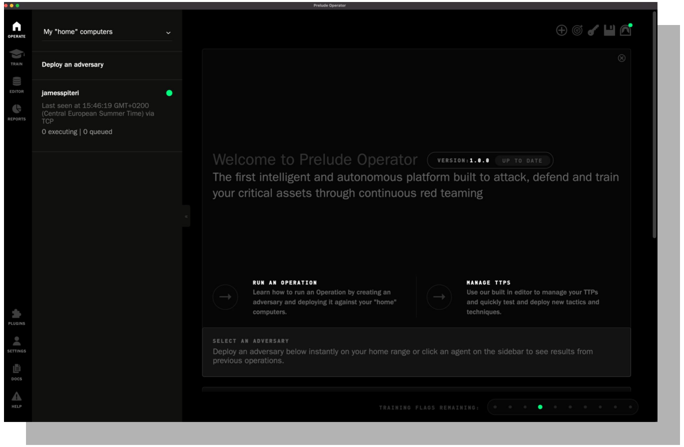
Create staging directory
COLLECTION | DATA STAGED

Phase 2

Snag broadcast IP
DISCOVERY | SYSTEM NETWORK CONFIGURATION DISCOV...

Find user processes
DISCOVERY | PROCESS DISCOV...

CALDERA



My "home" computers

Deploy an adversary

jamesspiteri
Last seen at 15:46:19 GMT+0200 (Central European Summer Time) via TCP
0 executing | 0 queued

Welcome to Prelude Operator

The first intelligent and autonomous platform built to attack, defend and train your critical assets through continuous red teaming

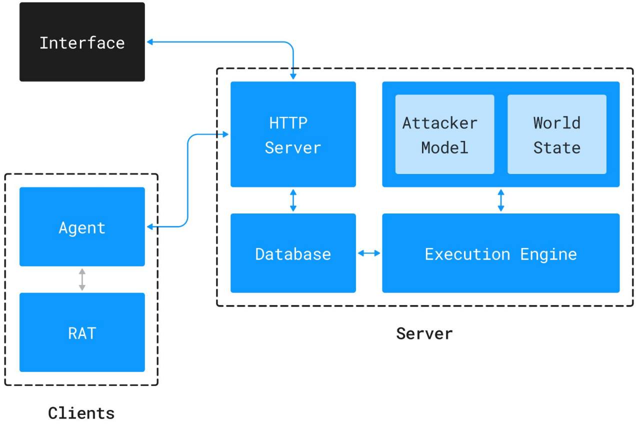
RUN AN OPERATION
Learn how to run an Operation by creating an adversary and deploying it against your "home" computers.

MANAGE TTPS
Use our built in editor to manage your TTPs and quickly test and deploy new tactics and techniques.

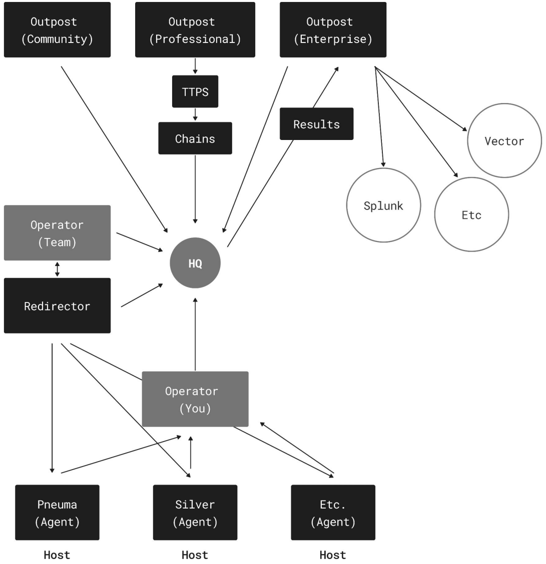
SELECT AN ADVERSARY
Deploy an adversary below instantly on your home range or click an agent on the sidebar to see results from previous operations.

[P] | Prelude

Where we've come from

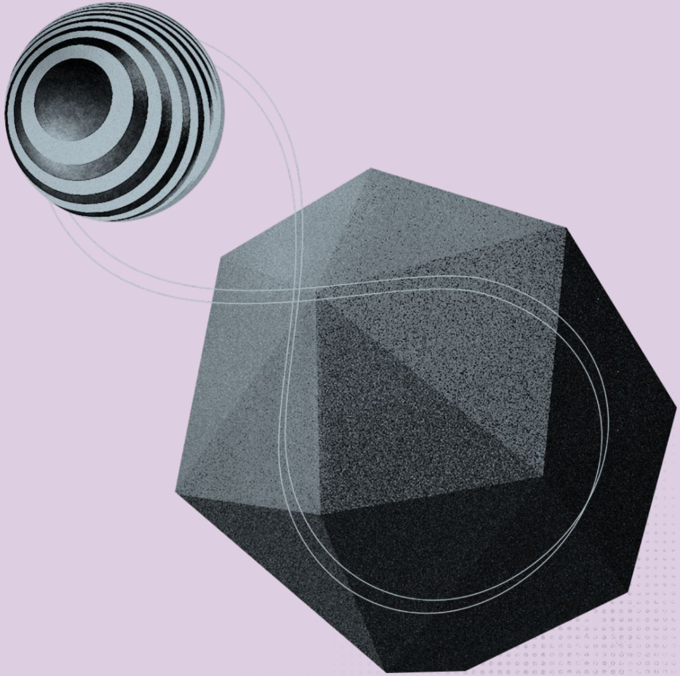


CALDERA



[P] | Prelude

Continuous Security Testing



[P]

Detect

Detect is a continuous security testing service that allows you to ask questions of your infrastructure - at tremendous scale - to understand your security posture at a glance.

[P]

Asking Your Infrastructure Questions

- Rules describe the expected security behavior of an endpoint
- Tests ensure each rule is true
- Probes are processes that run the tests
- Executive dashboard displays the results

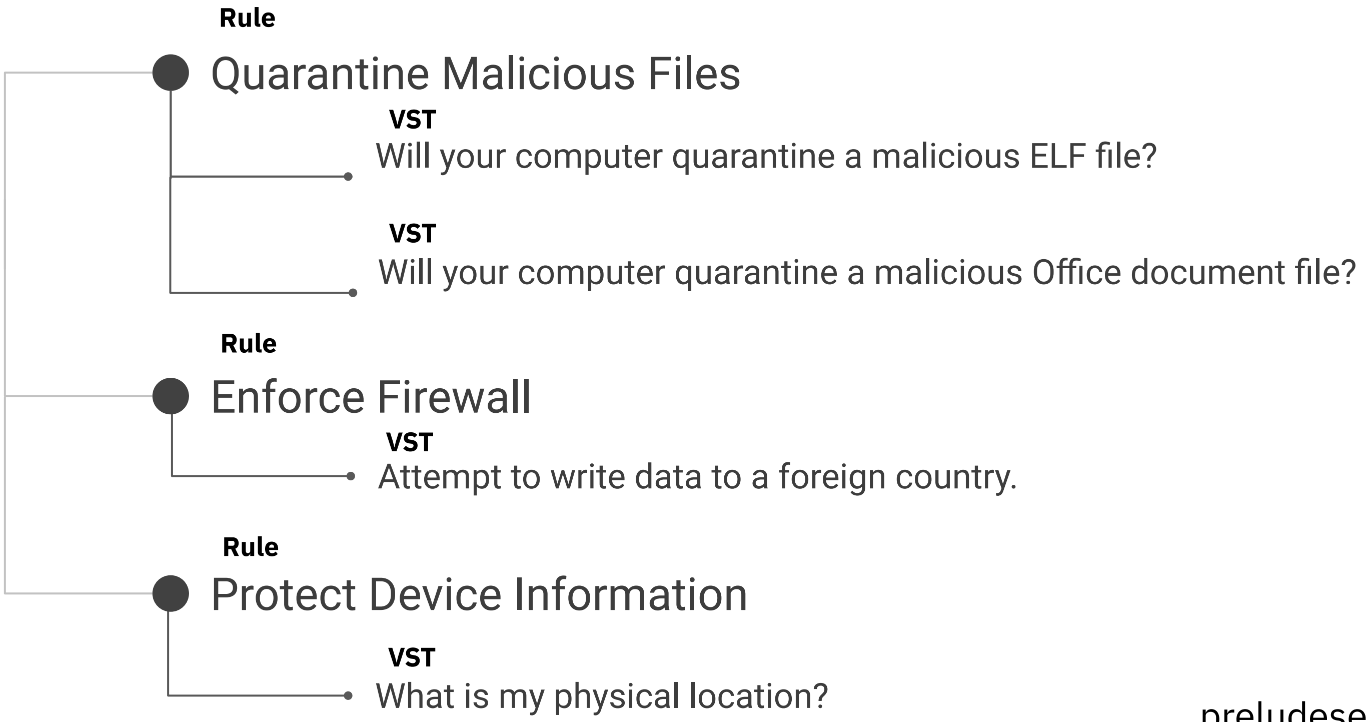
What is a Rule?

A rule is a statement that would confine the surface area of an endpoint, if true, resulting in a more secure device.

What is a Rule?

- Specific to the operating system of the endpoint
- Rules must be true in all cases, regardless of context
- Rules apply at the operating system level

Everybody loves rules



Rule

Quarantine Malicious Files

VST

Will your computer quarantine a malicious ELF file?

VST

Will your computer quarantine a malicious Office document file?

Rule

Enforce Firewall

VST

Attempt to write data to a foreign country.

Rule

Protect Device Information

VST

What is my physical location?

What is a Test?

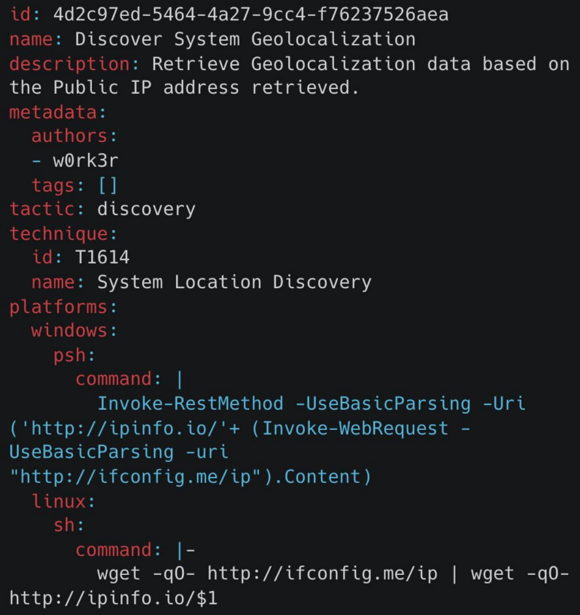
Security tests are production-ready versions of TTPs. Tests have characteristics that encourage scale and safety.

What is a Test?

- For each rule, tests prove whether it is being enforced (or not).
- A test should not be all encompassing but instead verify a specific implementation of the rule.
- Use known, malicious or exploitable code in their implementation.

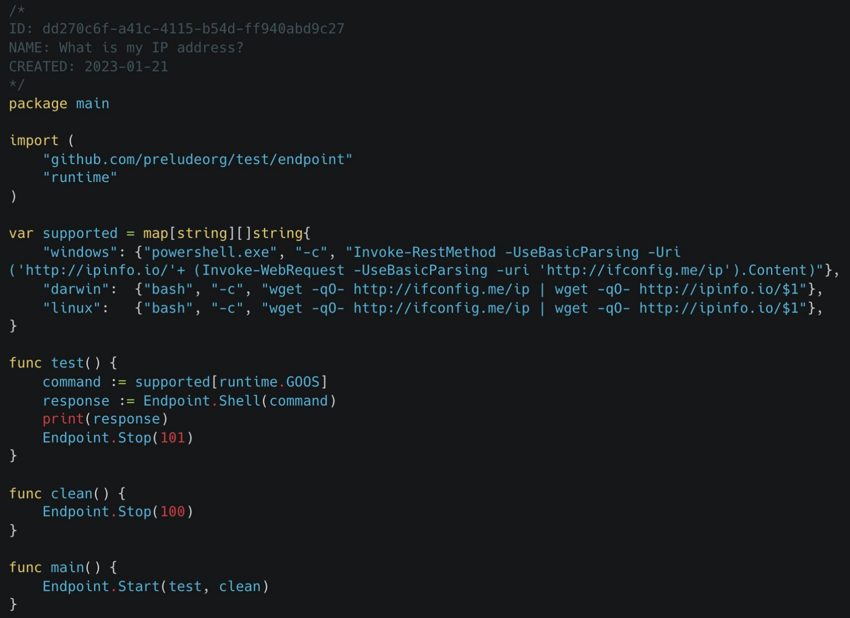
TTPs ➳ Verified Security Tests (VSTs)

Example of TTP in Operator (and Caldera)



```
id: 4d2c97ed-5464-4a27-9cc4-f76237526aea
name: Discover System Geolocalization
description: Retrieve Geolocalization data based on
the Public IP address retrieved.
metadata:
  authors:
  - w0rk3r
  tags: []
tactic: discovery
technique:
  id: T1614
  name: System Location Discovery
platforms:
  windows:
    psh:
      command: |
        Invoke-RestMethod -UseBasicParsing -Uri
('http://ipinfo.io/'+ (Invoke-WebRequest -
UseBasicParsing -uri
"http://ifconfig.me/ip").Content)
  linux:
    sh:
      command: |-
        wget -qO- http://ifconfig.me/ip | wget -qO-
http://ipinfo.io/$1
```

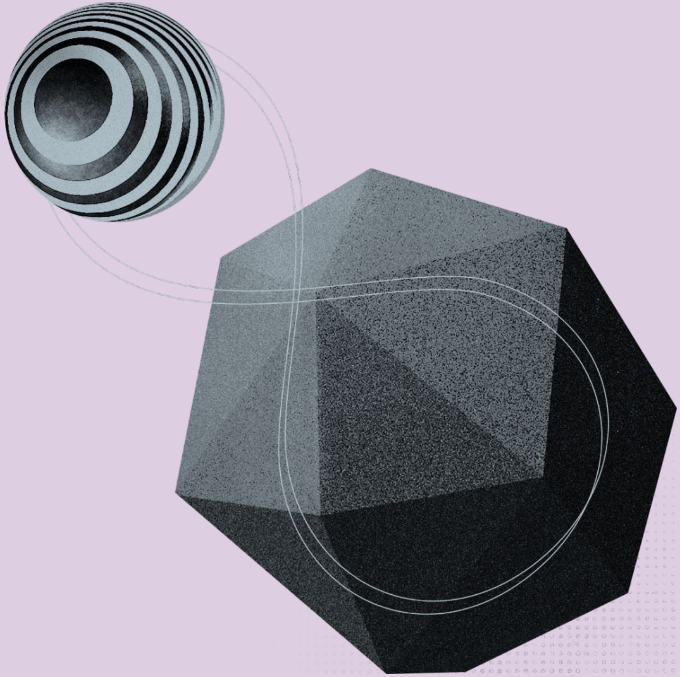
Verified Security Test (VST)



```
/*
ID: dd270c6f-a41c-4115-b54d-ff940abd9c27
NAME: What is my IP address?
CREATED: 2023-01-21
*/
package main

import (
    "github.com/preludeorg/test/endpoint"
    "runtime"
)

var supported = map[string][]string{
    "windows": {"powershell.exe", "-c", "Invoke-RestMethod -UseBasicParsing -Uri
('http://ipinfo.io/'+ (Invoke-WebRequest -UseBasicParsing -uri 'http://ifconfig.me/ip').Content)"},
    "darwin":  {"bash", "-c", "wget -qO- http://ifconfig.me/ip | wget -qO- http://ipinfo.io/$1"},
    "linux":   {"bash", "-c", "wget -qO- http://ifconfig.me/ip | wget -qO- http://ipinfo.io/$1"},
}

func test() {
    command := supported[runtime.GOOS]
    response := Endpoint.Shell(command)
    print(response)
    Endpoint.Stop(101)
}

func clean() {
    Endpoint.Stop(100)
}

func main() {
    Endpoint.Start(test, clean)
}
```

Endpoint

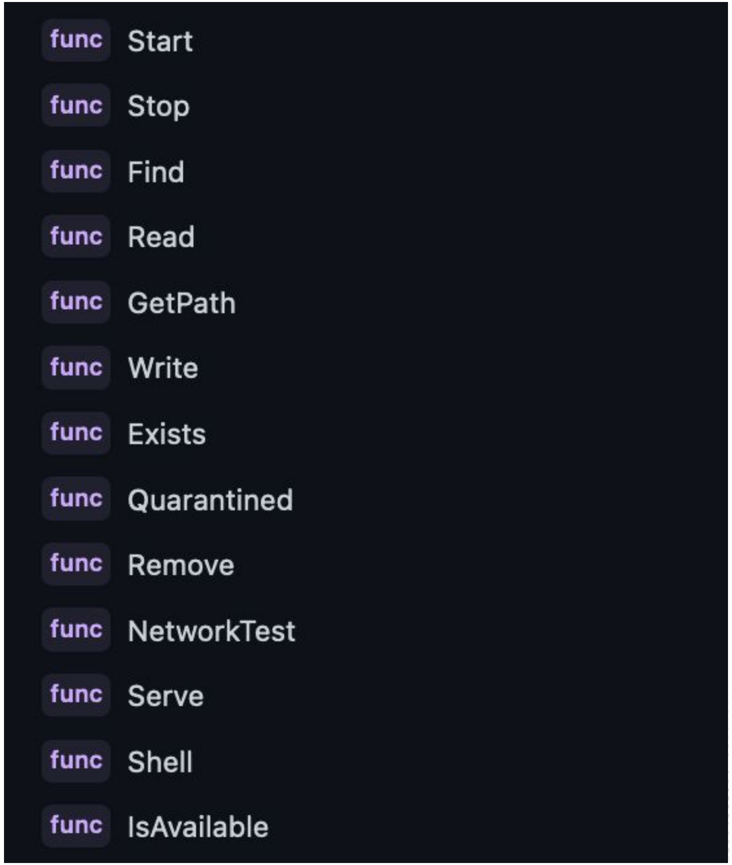
We wrote the code, so you don’t have to



[P]

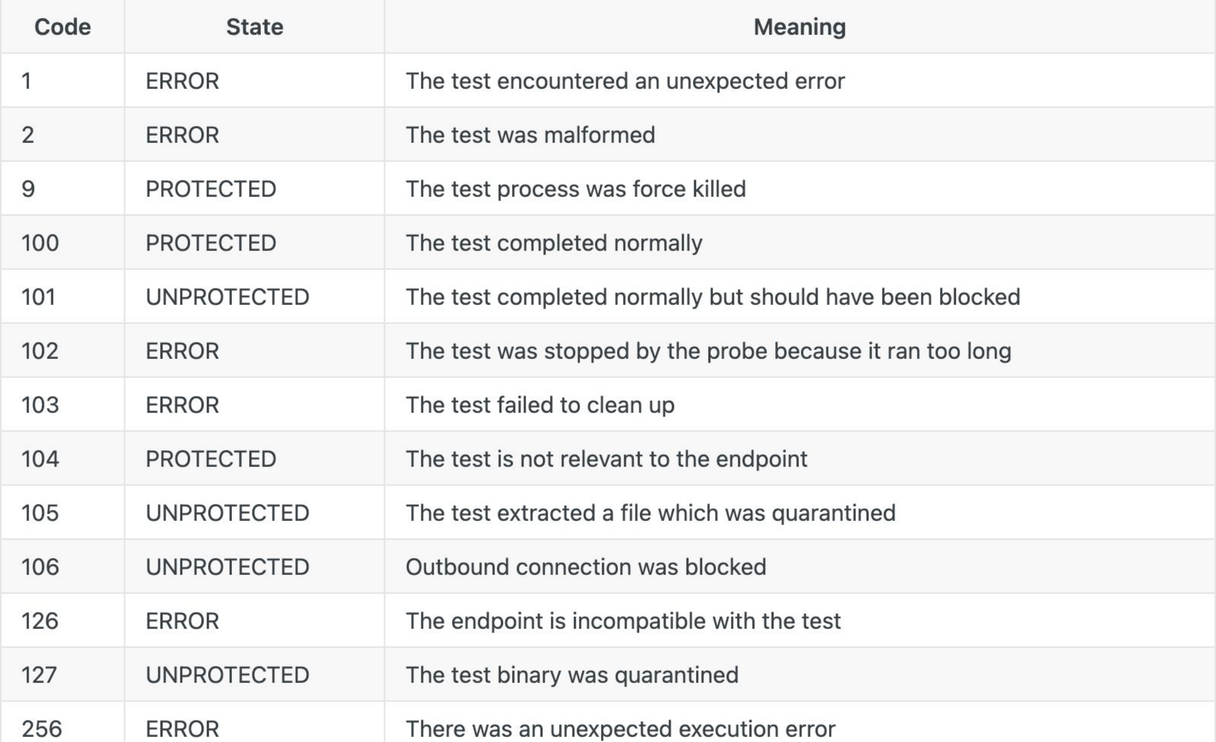
Wide variety of functions to choose from

Think pwn-tools



```
func Start
func Stop
func Find
func Read
func GetPath
func Write
func Exists
func Quarantined
func Remove
func NetworkTest
func Serve
func Shell
func IsAvailable
```

Exit Codes That Scale



Code	State	Meaning
1	ERROR	The test encountered an unexpected error
2	ERROR	The test was malformed
9	PROTECTED	The test process was force killed
100	PROTECTED	The test completed normally
101	UNPROTECTED	The test completed normally but should have been blocked
102	ERROR	The test was stopped by the probe because it ran too long
103	ERROR	The test failed to clean up
104	PROTECTED	The test is not relevant to the endpoint
105	UNPROTECTED	The test extracted a file which was quarantined
106	UNPROTECTED	Outbound connection was blocked
126	ERROR	The endpoint is incompatible with the test
127	UNPROTECTED	The test binary was quarantined
256	ERROR	There was an unexpected execution error

What is a Probe?

A probe is a low-resource process that requires no special privileges to run.

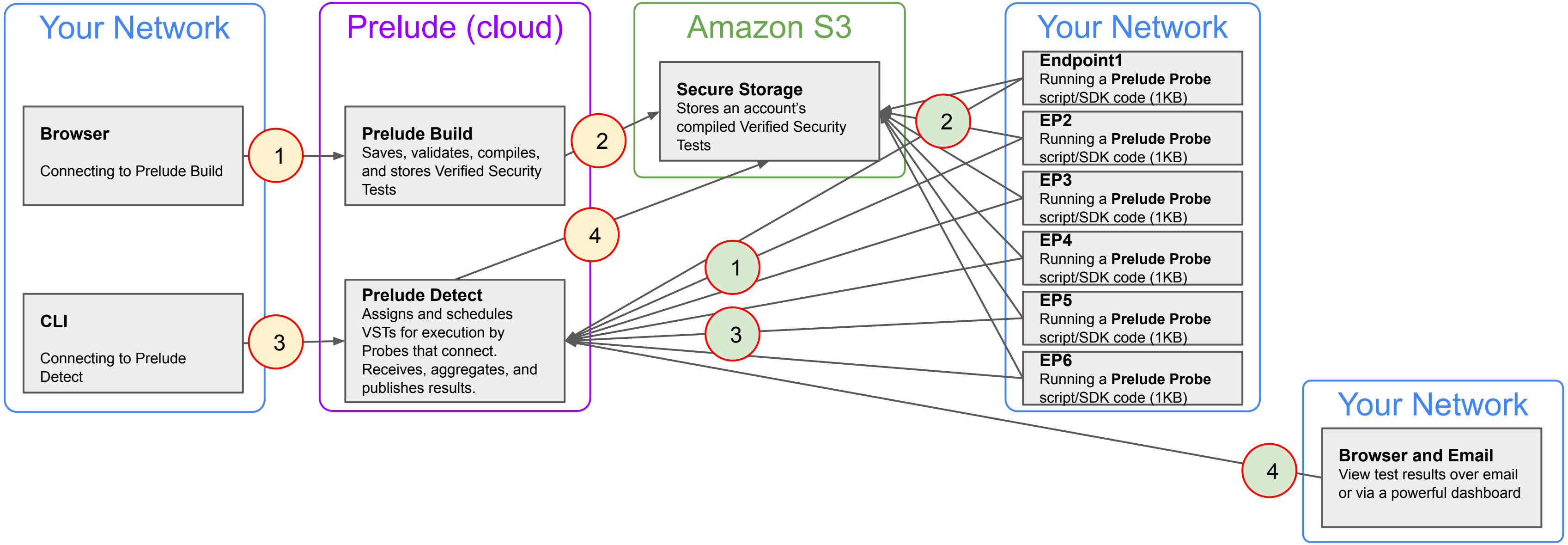
Probes: Not agents. Not agentless. Agent*ish*.

- Accept, run, and return the results of your VST
- 1-50 KB on disk
- Can run anywhere code runs
- Open-source

Name	**Runtime**	**Supported (DOS)**	**Size**
Raindrop	PowerShell	windows-x86_64	1kb
Nocturnal	Bash	linux-x86_64, linux-arm64,darwin-x86_64, darwin-arm64	900B

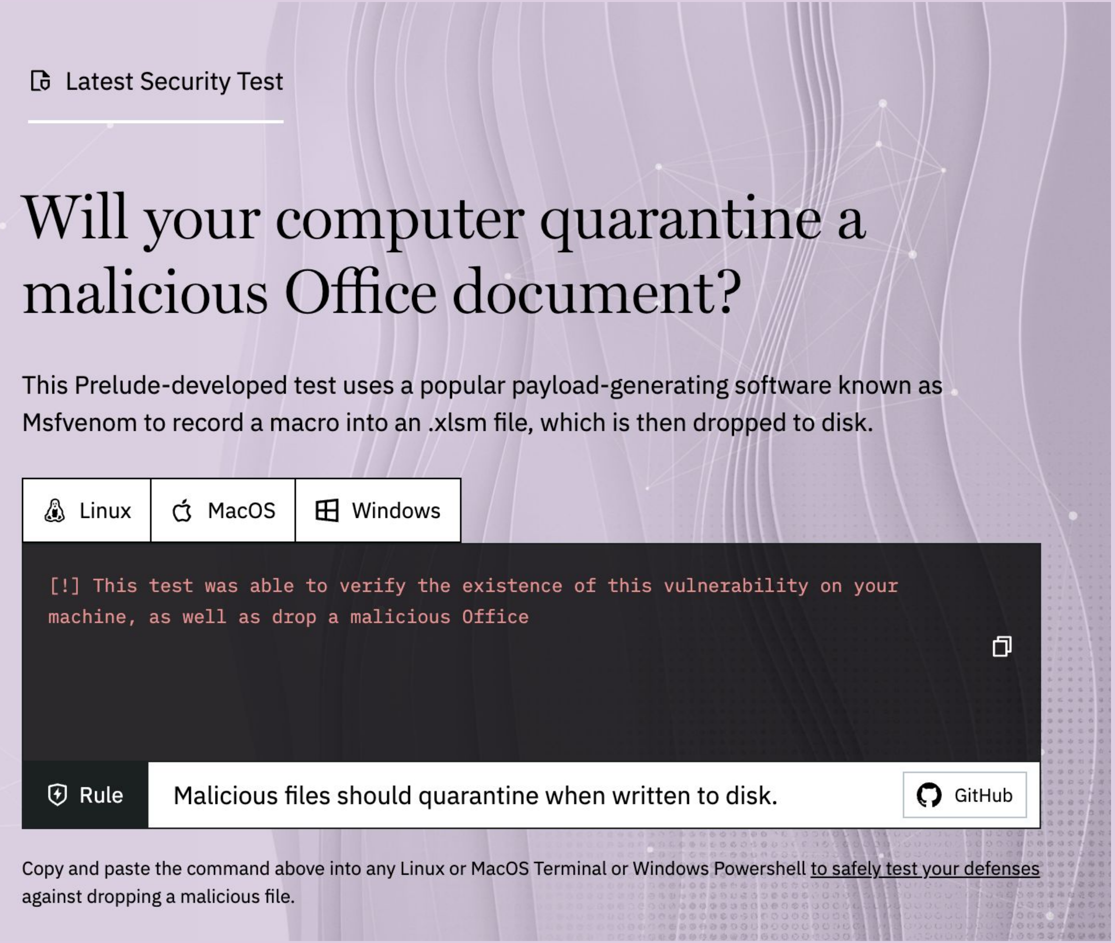
[P]

Tying it all together


Your Network
Browser
Connecting to Prelude Build
CLI
Connecting to Prelude Detect
1
3
Prelude (cloud)
Prelude Build
Saves, validates, compiles, and stores Verified Security Tests
Prelude Detect
Assigns and schedules VSTs for execution by Probes that connect. Receives, aggregates, and publishes results.
2
4
Amazon S3
Secure Storage
Stores an account's compiled Verified Security Tests
2
1
3
Your Network
Endpoint1
Running a Prelude Probe script/SDK code (1KB)
EP2
Running a Prelude Probe script/SDK code (1KB)
EP3
Running a Prelude Probe script/SDK code (1KB)
EP4
Running a Prelude Probe script/SDK code (1KB)
EP5
Running a Prelude Probe script/SDK code (1KB)
EP6
Running a Prelude Probe script/SDK code (1KB)
4
Your Network
Browser and Email
View test results over email or via a powerful dashboard

Running your first VST

Try it now at preludesecurity.com



Will your computer quarantine a malicious Office document?

This Prelude-developed test uses a popular payload-generating software known as Msfvenom to record a macro into an .xlsm file, which is then dropped to disk.

```
[!] This test was able to verify the existence of this vulnerability on your
machine, as well as drop a malicious Office
```

Malicious files should quarantine when written to disk.

Copy and paste the command above into any Linux or MacOS Terminal or Windows Powershell to safely test your defenses against dropping a malicious file.

Getting Started

Fork and clone this repo:
https://github.com/VVX7/Prelude-Detect-Workshop

[P]

preludesecurity.com

What we’ll do

1. Create an account
2. Register an endpoint
3. Enable tests
4. Deploy a probe
5. Create a test
6. Explore Detect dashboard

[P]

Prelude CLI

The Prelude Command Line Interface supplies programmatic access to the full suite of Prelude APIs. It is written in Python and will run on any macOS or Linux machine with Python installed.

[P]

preludesecurity.com

Prelude CLI

- The Prelude CLI is the primary driver for managing Detect
- Commands generally will follow the format
  ```
  prelude [service] [function] [arguments]
  ```
- Interactive mode
  ```
  prelude --interactive
  ```

[P]

Registering Endpoints

Endpoints are simply hosts running a Prelude probe.

[P]

Registering Endpoints

- Create an endpoint token

```
prelude detect create-endpoint
```

- Endpoint identifiers should be unique
- Tags are optional
- A Prelude account is required to register endpoints

[P]

Enabling Tests

Enabling a security test makes it available for execution on active probes.

[P]

Enabling Tests

- Enable a test

```
prelude detect enable-test
```

- Tests scheduled daily, weekly, or monthly
- View the test queue

```
prelude detect queue
```

Deploying Probes

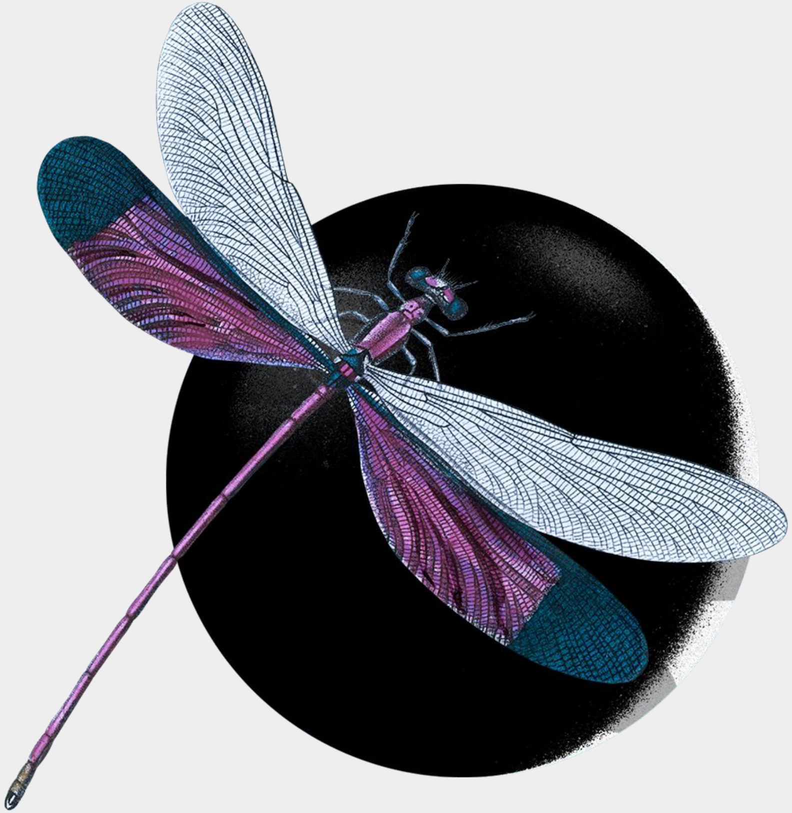
Ephemeral probes are lightweight processes with the smallest footprint possible.

Deploying Probes

- Probes require an environment variable, PRELUDE_TOKEN, to be set before they are started.
- Ephemeral probes - installation free
- Persistent probes - install as service

Creating Tests

Security tests are production-ready versions of TTPs. Tests have characteristics that encourage scale and safety.



[P]

Creating Tests

- Create a test

```
prelude build create-test
```

- Files can be embedded in a test
- Uploading a file sends it to Compute where it's automatically cross-compiled

Exploring Dashboards

Recommendations and insights aimed at enhancing the security of your hosts.

[P]

preludesecurity.com

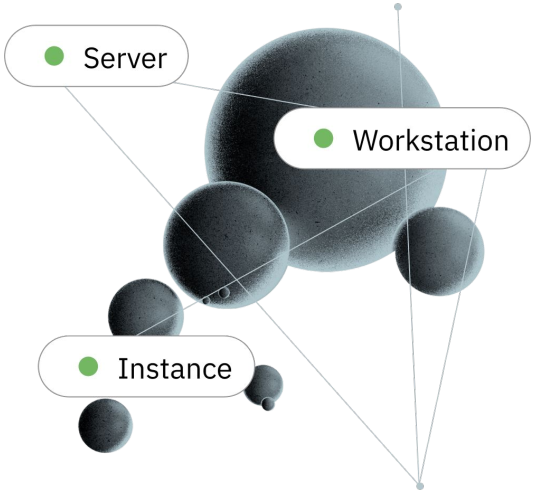
Exploring Dashboards

https://platform.preludesecurity.com/detect

- Health Check
- Malware Protection
- Emerging Threats
- Decision View
- Hosts View

Getting Started ↴

platform.preludesecurity.com



Resources

Documentation

- Prelude Detect
- Prelude CLI

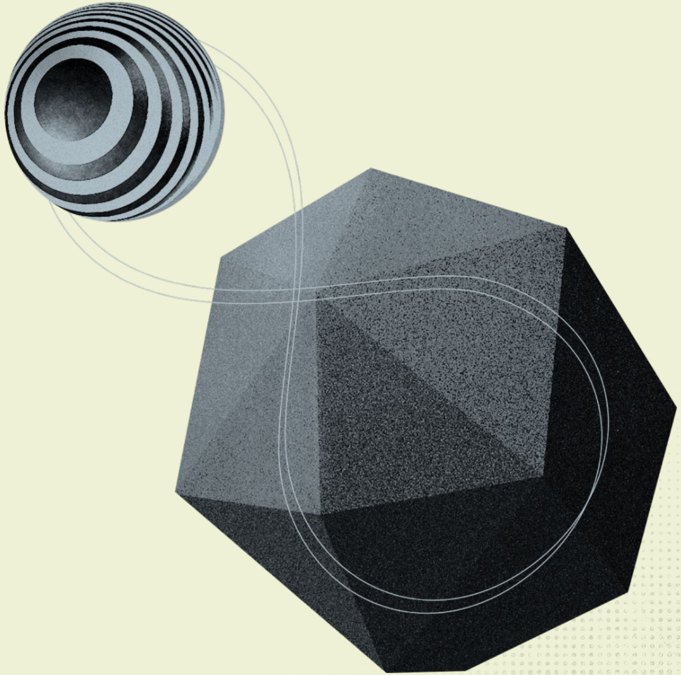
GitHub

- Verified Security Tests (VSTs)
    - Prelude Build
- Probes

Community

- Join our Discord

Thank you!



[P]