# Jamf in your security stack

JAMF NATION LIVE

Thijs Xhaflaire

Consulting Engineer, Security
Jamf

# **Session** Outline

1 | Overview Jamf Security solutions and options within Jamf Protect

2 | Why it’s relevant to forward data & the available forwarding options

3 | Solution Integrations & Workflows

4 | Basic Threat Hunting with Jamf Protect and Microsoft Sentinel — Demo!

# Overview of Jamf **Security Solutions**

## Jamf **Protect**

Jamf Protect provides powerful Endpoint Security to macOS, iOS and iPadOS with advanced detection and response capabilities, backed by Jamf Threat Labs.

## Jamf **Connect**

Providing **Cloud-based Identity** and **Zero-trust Network Access** on macOS and Mobile endpoints.

## Jamf **Safe Internet**

Comprehensive content filtering and web threat protection optimized for education and integrated with MDM for simple, powerful student and user protection.

## Jamf **Executive Threat Prevention**

Provides Advanced detection and response capabilities to mobile endpoints and an remote method to detect incidents or activities on mobile devices and the tools needed to respond.

# Overview of Jamf **Security Solutions**

## Jamf **Protect**

Jamf Protect provides powerful Endpoint Security to macOS, iOS and iPadOS with advanced detection and response capabilities, backed by Jamf Threat Labs.

## Jamf **Connect**

Providing **Cloud-based Identity** and **Zero-trust Network Access** on macOS and Mobile endpoints.

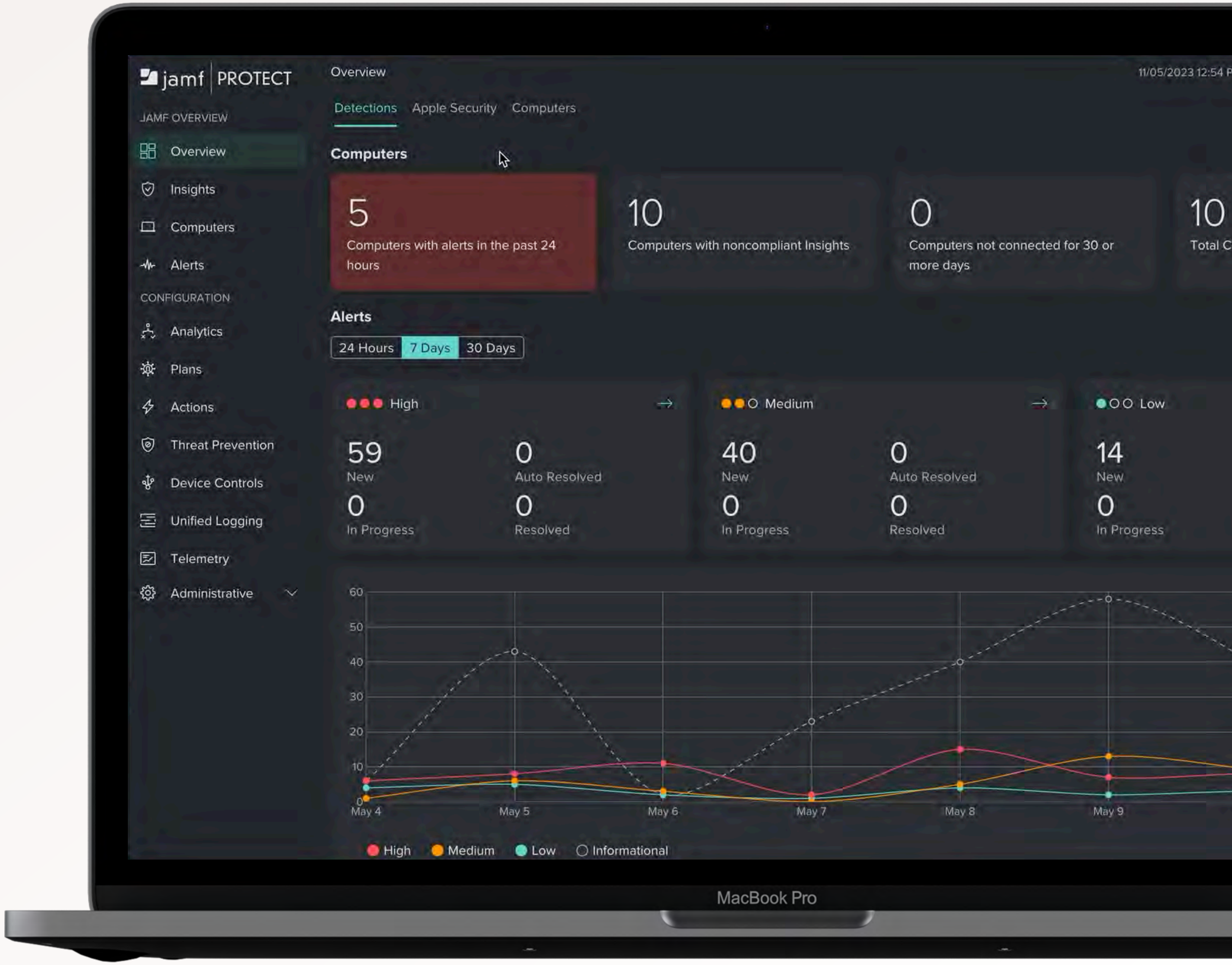
## Jamf **Safe Internet**

Comprehensive content filtering and web threat protection optimized for education and integrated with MDM for simple, powerful student and user protection.

## Jamf **Executive Threat Prevention**

Provides Advanced detection and response capabilities to mobile endpoints and an remote method to detect incidents or activities on mobile devices and the tools needed to respond.

# Jamf **Protect**



jamf | PROTECT

JAMF OVERVIEW

- Overview
- Insights
- Computers
- Alerts

CONFIGURATION

- Analytics
- Plans
- Actions
- Threat Prevention
- Device Controls
- Unified Logging
- Telemetry
- Administrative

Overview

11/05/2023 12:54 F

Detections | Apple Security | Computers

**Computers**

5
Computers with alerts in the past 24 hours

10
Computers with noncompliant Insights

0
Computers not connected for 30 or more days

10
Total C

**Alerts**

24 Hours | 7 Days | 30 Days

●●● High →

59 New | 0 Auto Resolved
0 In Progress | 0 Resolved

●●○ Medium →

40 New | 0 Auto Resolved
0 In Progress | 0 Resolved

●○○ Low

14 New
0 In Progress

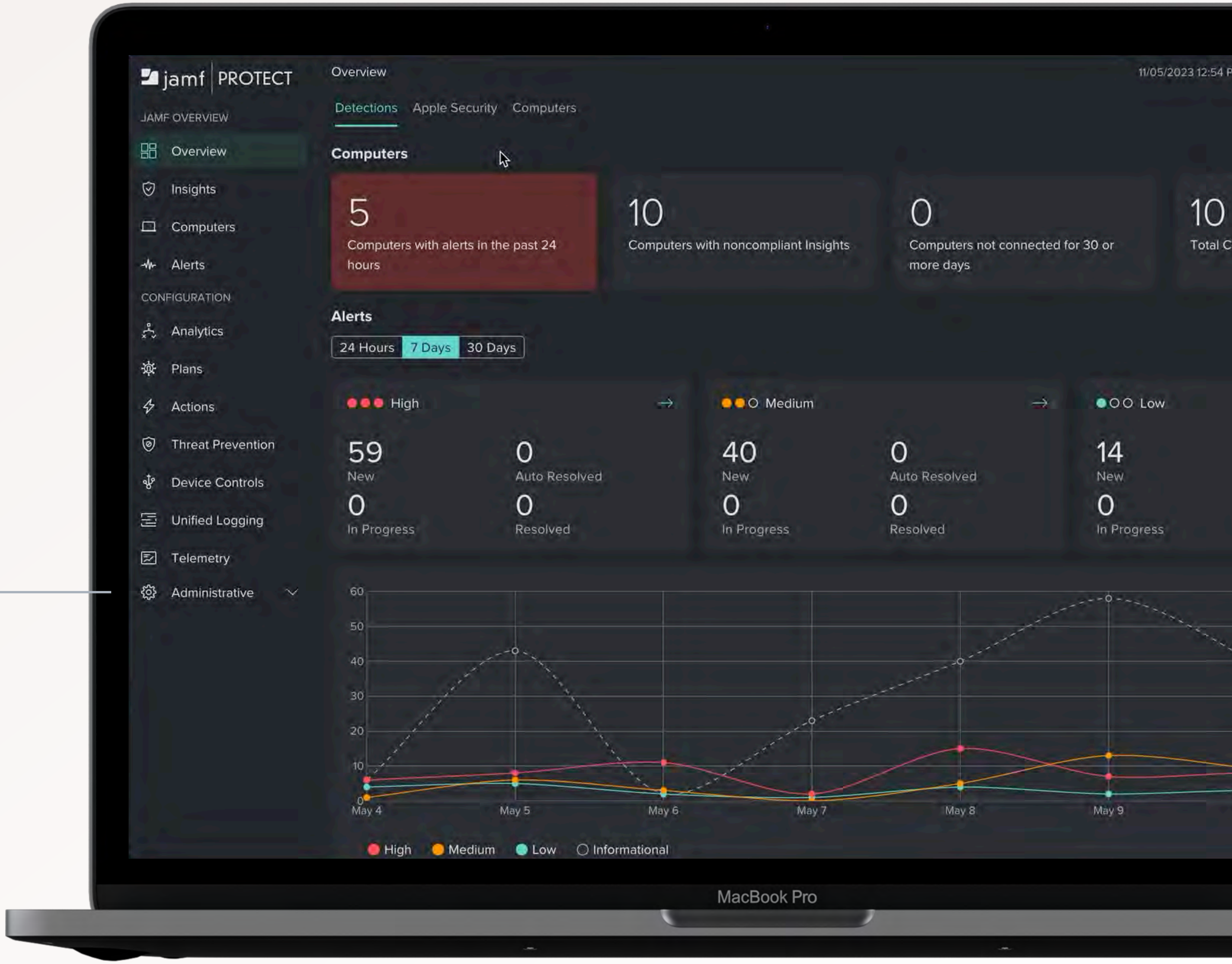
# Jamf **Protect**

Dashboards and Alerts

**Alerts for macOS endpoints available in Jamf Protect, macOS Security Portal**

Dashboards and Alerts

**Network or app-based Threats for macOS and iOS/iPadOS available in Jamf Security Cloud (RADAR)**



Computers

5 Computers with alerts in the past 24 hours

10 Computers with noncompliant Insights

0 Computers not connected for 30 or more days

10 Total C

Alerts

High: 59 New, 0 Auto Resolved, 0 In Progress, 0 Resolved

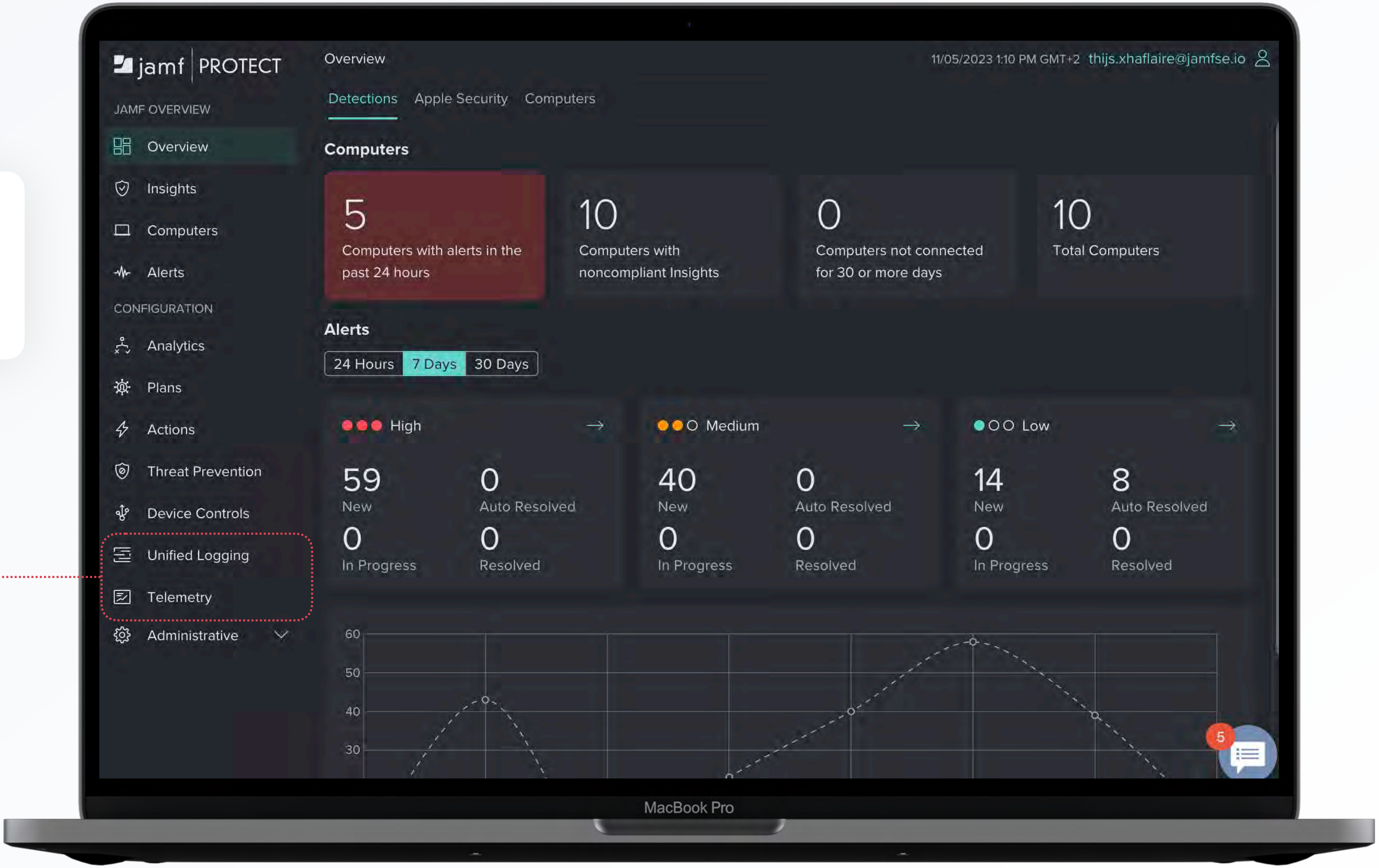
Medium: 40 New, 0 Auto Resolved, 0 In Progress, 0 Resolved

Low: 14 New, 0 In Progress

# Jamf **Protect**

Requirements

Both **Unified Logging** and **Telemetry** require integrating with a third party solution



jamf | PROTECT

Overview

11/05/2023 1:10 PM GMT+2 thijs.xhaflaire@jamfse.io

Detections | Apple Security | Computers

JAMF OVERVIEW
- Overview
- Insights
- Computers
- Alerts

CONFIGURATION
- Analytics
- Plans
- Actions
- Threat Prevention
- Device Controls
- Unified Logging
- Telemetry
- Administrative

**Computers**

5 Computers with alerts in the past 24 hours

10 Computers with noncompliant Insights

0 Computers not connected for 30 or more days

10 Total Computers

**Alerts**

24 Hours | 7 Days | 30 Days

●●● High →

59 New | 0 Auto Resolved
0 In Progress | 0 Resolved

●●○ Medium →

40 New | 0 Auto Resolved
0 In Progress | 0 Resolved

●○○ Low →

14 New | 8 Auto Resolved
0 In Progress | 0 Resolved

● JAMF NATION LIVE

# Jamf **Protect**

Unified Logging

**Sift through macOS Unified Logging system with Jamf Protect's predicate-based filtering**

**TouchID Authentication Events:**

```
process == "loginwindow" AND
eventMessage CONTAINS[c] "APEventTouchIDMatch"
```

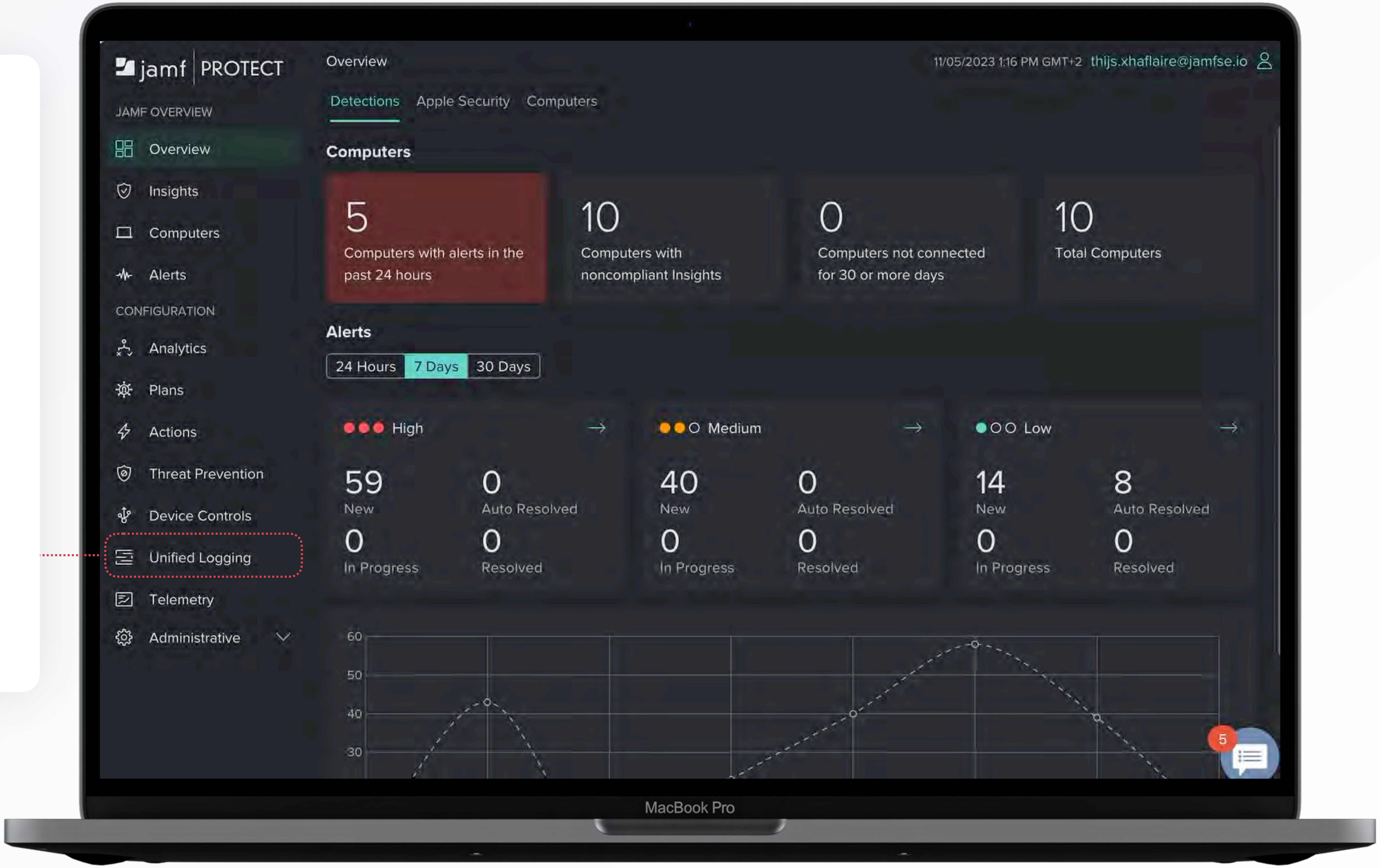
**XProtect Remediator Scan Activity:**

```
subsystem ==
“com.apple.XProtectFramework.PluginAPI” AND
category == "XPEvent.structured"
```

**SAP Privileges:**

```
process == "corp.sap.privileges.helper" AND
eventMessage CONTAINS "SAPCorp"
```

**More examples on [https://github.com/jamf/jamfprotect](https://github.com/jamf/jamfprotect)**



Computers

5 Computers with alerts in the past 24 hours

10 Computers with noncompliant Insights

0 Computers not connected for 30 or more days

10 Total Computers

Alerts

High: 59 New, 0 Auto Resolved, 0 In Progress, 0 Resolved

Medium: 40 New, 0 Auto Resolved, 0 In Progress, 0 Resolved

Low: 14 New, 8 Auto Resolved, 0 In Progress, 0 Resolved

**JAMF NATION LIVE**

*Unified Logging only supports default log level

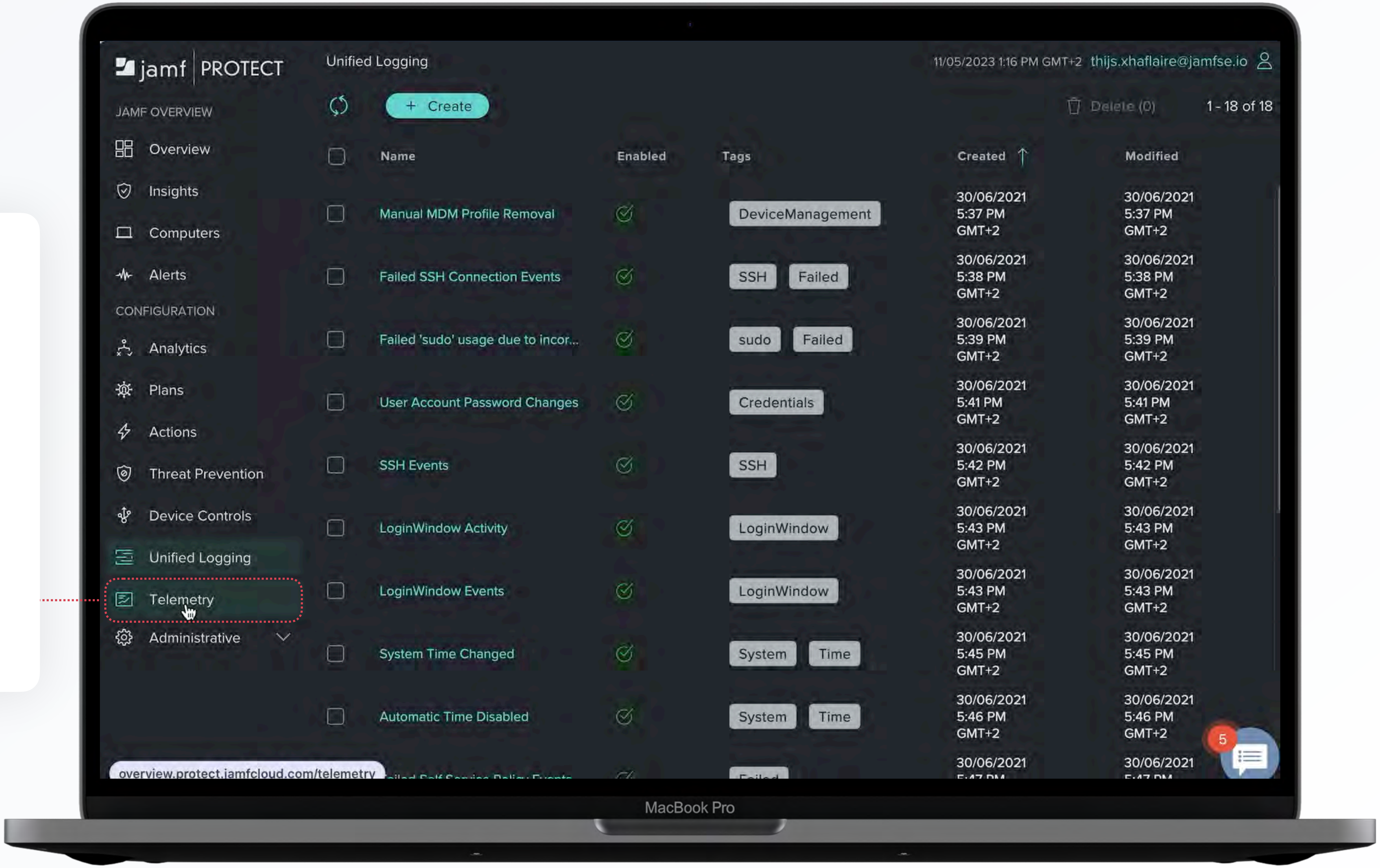
# Jamf Protect

Telemetry

**Get curated User and Device activity feeds and enable your teams with the data they require**

- Collect curated endpoint Telemetry
- Collect System Performance metrics
- Collect and monitor crash, diagnostic and log files

**More examples on [https://github.com/jamf/jamfprotect](https://github.com/jamf/jamfprotect)**

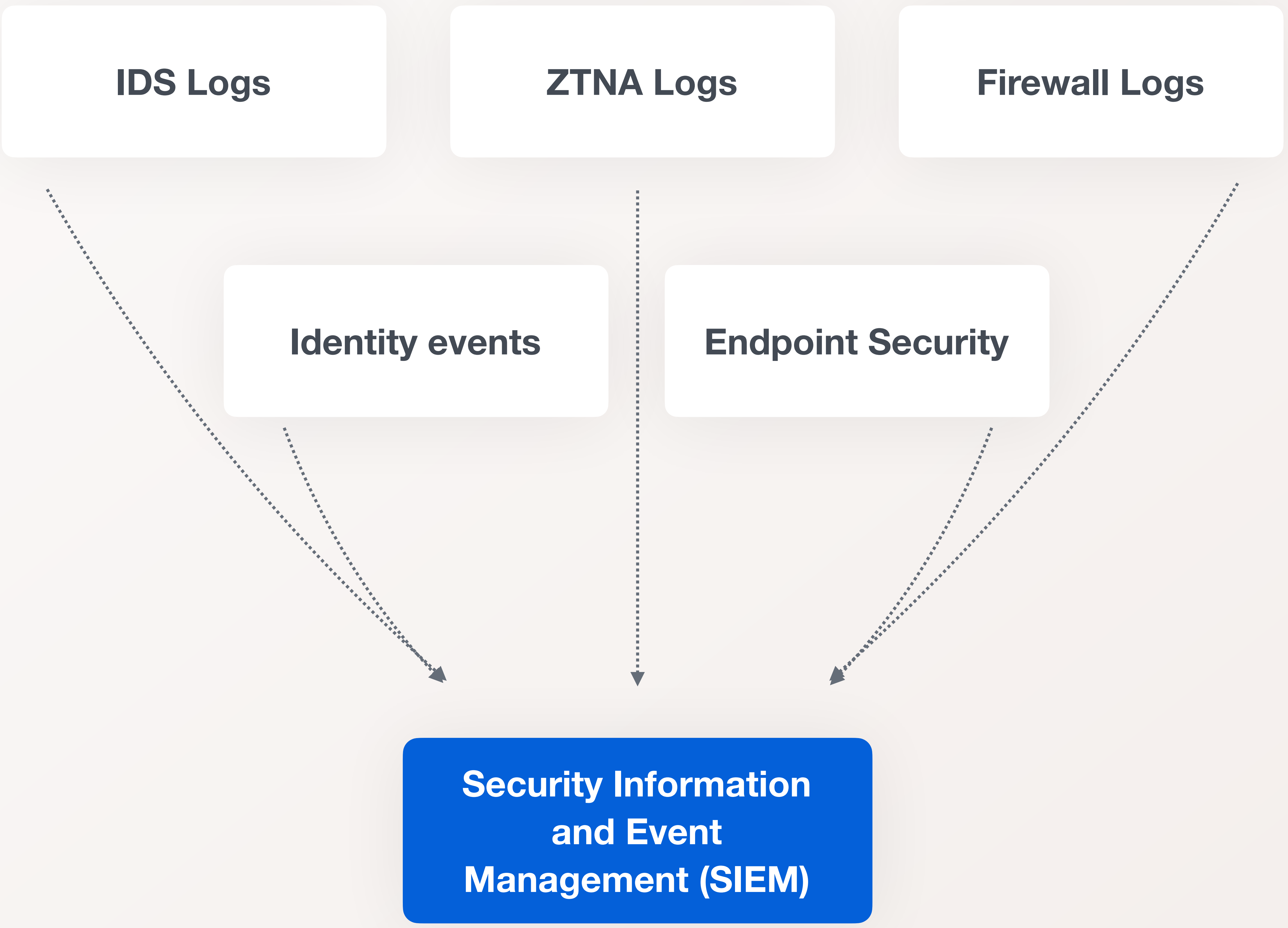


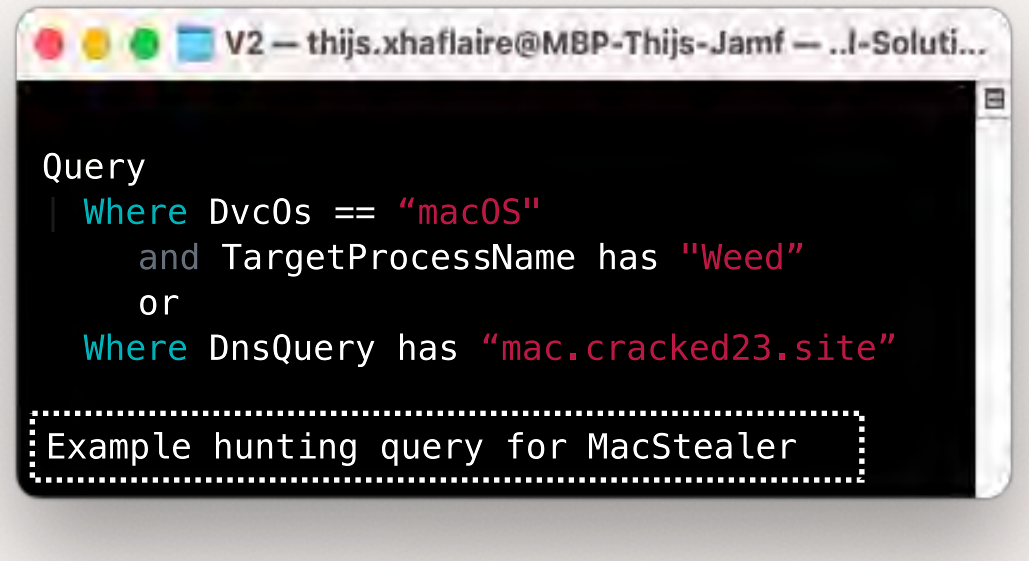
| □ | Name | Enabled | Tags | Created | Modified |
|---|---|---|---|---|---|
| □ | Manual MDM Profile Removal | ✓ | DeviceManagement | 30/06/2021 5:37 PM GMT+2 | 30/06/2021 5:37 PM GMT+2 |
| □ | Failed SSH Connection Events | ✓ | SSH Failed | 30/06/2021 5:38 PM GMT+2 | 30/06/2021 5:38 PM GMT+2 |
| □ | Failed 'sudo' usage due to incor... | ✓ | sudo Failed | 30/06/2021 5:39 PM GMT+2 | 30/06/2021 5:39 PM GMT+2 |
| □ | User Account Password Changes | ✓ | Credentials | 30/06/2021 5:41 PM GMT+2 | 30/06/2021 5:41 PM GMT+2 |
| □ | SSH Events | ✓ | SSH | 30/06/2021 5:42 PM GMT+2 | 30/06/2021 5:42 PM GMT+2 |
| □ | LoginWindow Activity | ✓ | LoginWindow | 30/06/2021 5:43 PM GMT+2 | 30/06/2021 5:43 PM GMT+2 |
| □ | LoginWindow Events | ✓ | LoginWindow | 30/06/2021 5:43 PM GMT+2 | 30/06/2021 5:43 PM GMT+2 |
| □ | System Time Changed | ✓ | System Time | 30/06/2021 5:45 PM GMT+2 | 30/06/2021 5:45 PM GMT+2 |
| □ | Automatic Time Disabled | ✓ | System Time | 30/06/2021 5:46 PM GMT+2 | 30/06/2021 5:46 PM GMT+2 |
|  | Failed Self Service Policy Events | ✓ | Failed | 30/06/2021 | 30/06/2021 |

# Forwarding Security Events — **why it's relevant**

Simplify the process of identifying threats across your fleet, gather forensic details in matter of seconds from various sources and set out manual or automated actions

- Providing a single pane of glass
- Unified searching across events provided by different solutions or platforms
- Setup Security Orchestration, Automation and Response





```
Query
 | Where DvcOs == “macOS"
      and TargetProcessName has "Weed”
      or
   Where DnsQuery has “mac.cracked23.site”

Example hunting query for MacStealer
```

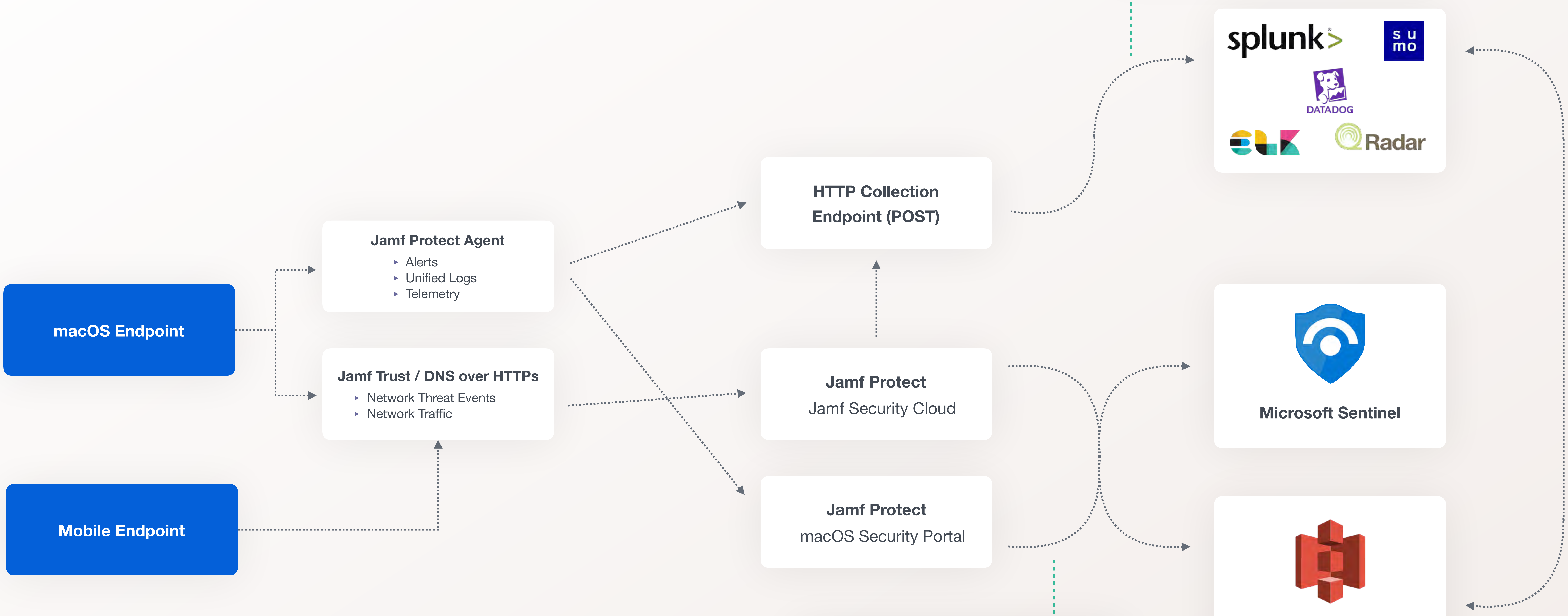
- Fields are mapped against respective schema
- Review security incidents at ease
- Configure automated responses across systems

JAMF NATION LIVE

# Data **Forwarding & Streaming**

Flexible streaming

**Stream events to any third party solution accepting JSON using HTTP POST**



macOS Endpoint

Mobile Endpoint

**Jamf Protect Agent**

- Alerts
- Unified Logs
- Telemetry

**Jamf Trust / DNS over HTTPs**

- Network Threat Events
- Network Traffic

**HTTP Collection Endpoint (POST)**

**Jamf Protect**
Jamf Security Cloud

**Jamf Protect**
macOS Security Portal

Microsoft Sentinel

Amazon S3

Native Integrations

**Forward data using native in-product integrations**

# Event Types

## Jamf Protect
## Alerts

**Alerts**

- Detection and Prevention of known threats
- Gatekeeper and XProtect events
- Behavior-based detections

**Device Controls**

- Mount Events
- Enforced Policies

## Jamf Protect
## Telemetry

**Endpoint Telemetry**

- Login and Authorization events
- User and Group creation and changes
- System Operation Events
- Network and Firewall changes
- Application process executions and security actions by applications
- Terminal and shell script activity
- Inbouw network connections
- Outbound network connections
- Unified Logs

## Jamf Protect
## Network Events

**Threat Events**

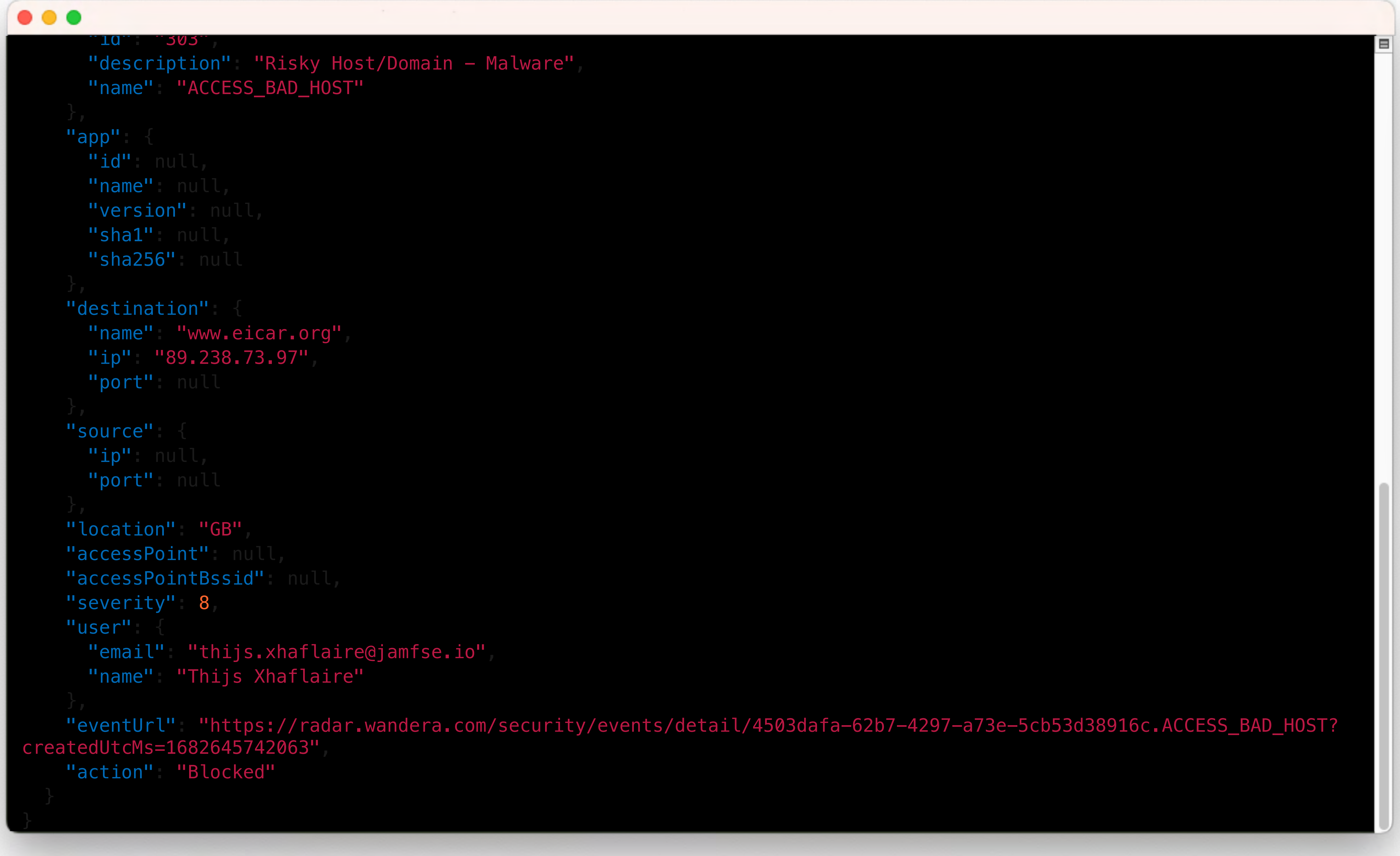
- Phishing
- Malware Network Traffic
- Spam
- Cryptojacking
- Vulnerable & out-of-date OS

**Network Traffic**

- Network Traffic using SecureDNS
- Content Filtering

# Event Types — JSON

## Jamf Protect — Web Threats



```
      "id": "303",
      "description": "Risky Host/Domain - Malware",
      "name": "ACCESS_BAD_HOST"
    },
    "app": {
      "id": null,
      "name": null,
      "version": null,
      "sha1": null,
      "sha256": null
    },
    "destination": {
      "name": "www.eicar.org",
      "ip": "89.238.73.97",
      "port": null
    },
    "source": {
      "ip": null,
      "port": null
    },
    "location": "GB",
    "accessPoint": null,
    "accessPointBssid": null,
    "severity": 8,
    "user": {
      "email": "thijs.xhaflaire@jamfse.io",
      "name": "Thijs Xhaflaire"
    },
    "eventUrl": "https://radar.wandera.com/security/events/detail/4503dafa-62b7-4297-a73e-5cb53d38916c.ACCESS_BAD_HOST?
createdUtcMs=1682645742063",
    "action": "Blocked"
  }
}
```

### Common fields of interest

```
{
    "event": {
      "device": {
        "deviceId": "e9671102-5ccf-4e66-a6b3-
b117ba257d5f",
        "os": "macOS 13.2.1",
        "deviceName": "Mac (13.2.1)",
        "userDeviceName": "acme-C1MT80UUH3QD",
        "externalId":
"0c221ae4-50af-5e39-8275-4424cc87ab8e"
      },
      "severity": 8,
      "user": {
        "email": "thijs.xhaflaire@jamfse.io",
        "name": "Thijs Xhaflaire"
      },
      "eventUrl": "https://radar.wandera.com/security/
events/detail/4503dafa-62b7-4297-
a73e-5cb53d38916c.ACCESS_BAD_HOST?
createdUtcMs=1682645742063",
      "action": "Blocked"
    }
 }
```

### Specific fields of interest

```
{
    "event": {
      "eventType": {
        "id": "303",
        "description": "Risky Host/Domain - Malware",
        "name": "ACCESS_BAD_HOST"
      },
      "destination": {
        "name": "www.eicar.org",
        "ip": "89.238.73.97",
        "port": null
      },
      "source": {
        "ip": null,
        "port": null
      }
    }
}
```

JAMF NATION LIVE

# Solution Integrations

## Third party integrations maintained by Jamf

### Jamf Protect for Microsoft Sentinel

- Data Connector
- Workbooks
- Analytic Rules

Member of Microsoft Intelligent Security Association

Microsoft

## Third party integrations maintained by vendor

### Jamf Protect Google Chronicle Integration

- UDM Mappings
- EDR Logs
- Parser

Chronicle

## To be released by Jamf

### Jamf Protect Technical Add-on

- Splunk CIM
- Dashboards
- Macro's

splunk>

### Jamf Protect Elastic Integration

- ECS Mappings
- Dashboards

### Jamf Protect Sumo Logic Integration

- CSE Mappings
- Dashboards

sumo logic

# Solution **Integrations**

## Third party integrations maintained by Jamf

### Jamf Protect for Microsoft Sentinel

Member of Microsoft Intelligent Security Association
Microsoft

- Data Connector
- Workbooks
- Analytic Rules

### Jamf Protect Technical Add-on

splunk>

- Splunk CIM
- Dashboards
- Macro's

## Third party integrations maintained by vendor

### Jamf Protect Google Chronicle Integration

Chronicle

- UDM Mappings
- EDR Logs
- Parser

## To be released by Jamf

### Jamf Protect Elastic Integration

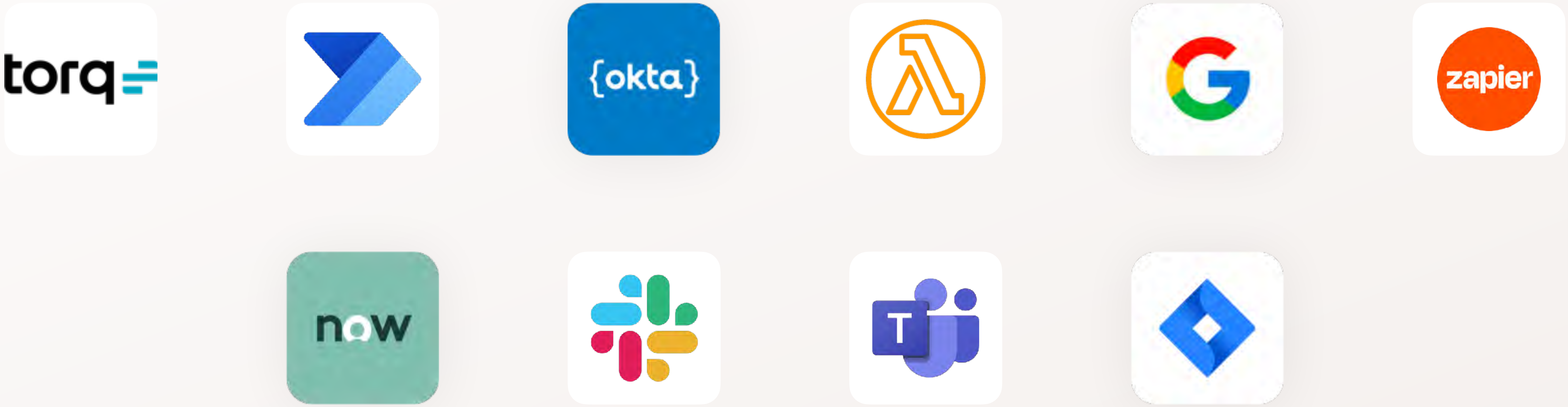
- ECS Mappings
- Dashboards

### Jamf Protect Sumo Logic Integration

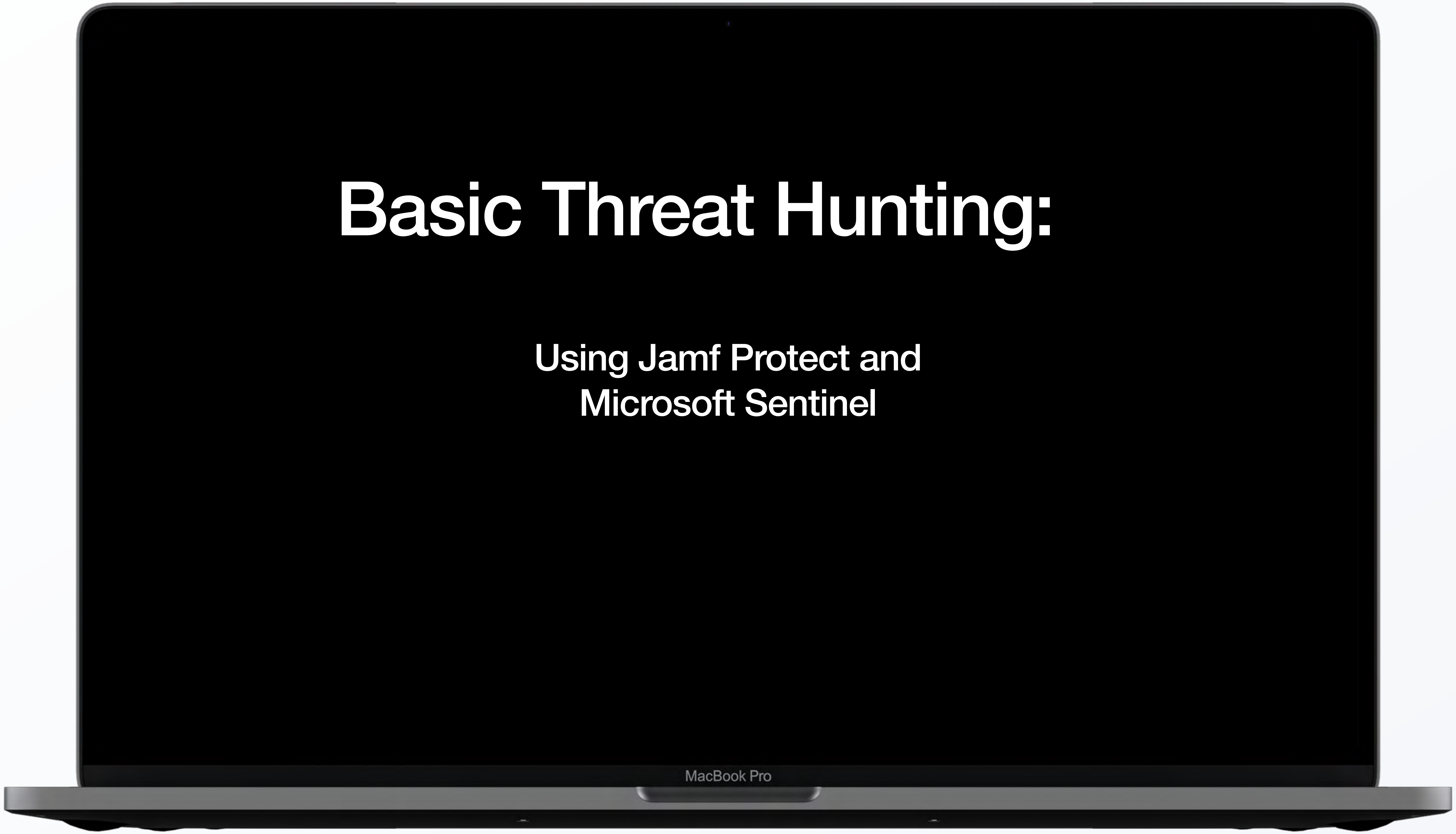
sumo logic

- CSE Mappings
- Dashboards

# Solution **Workflows**

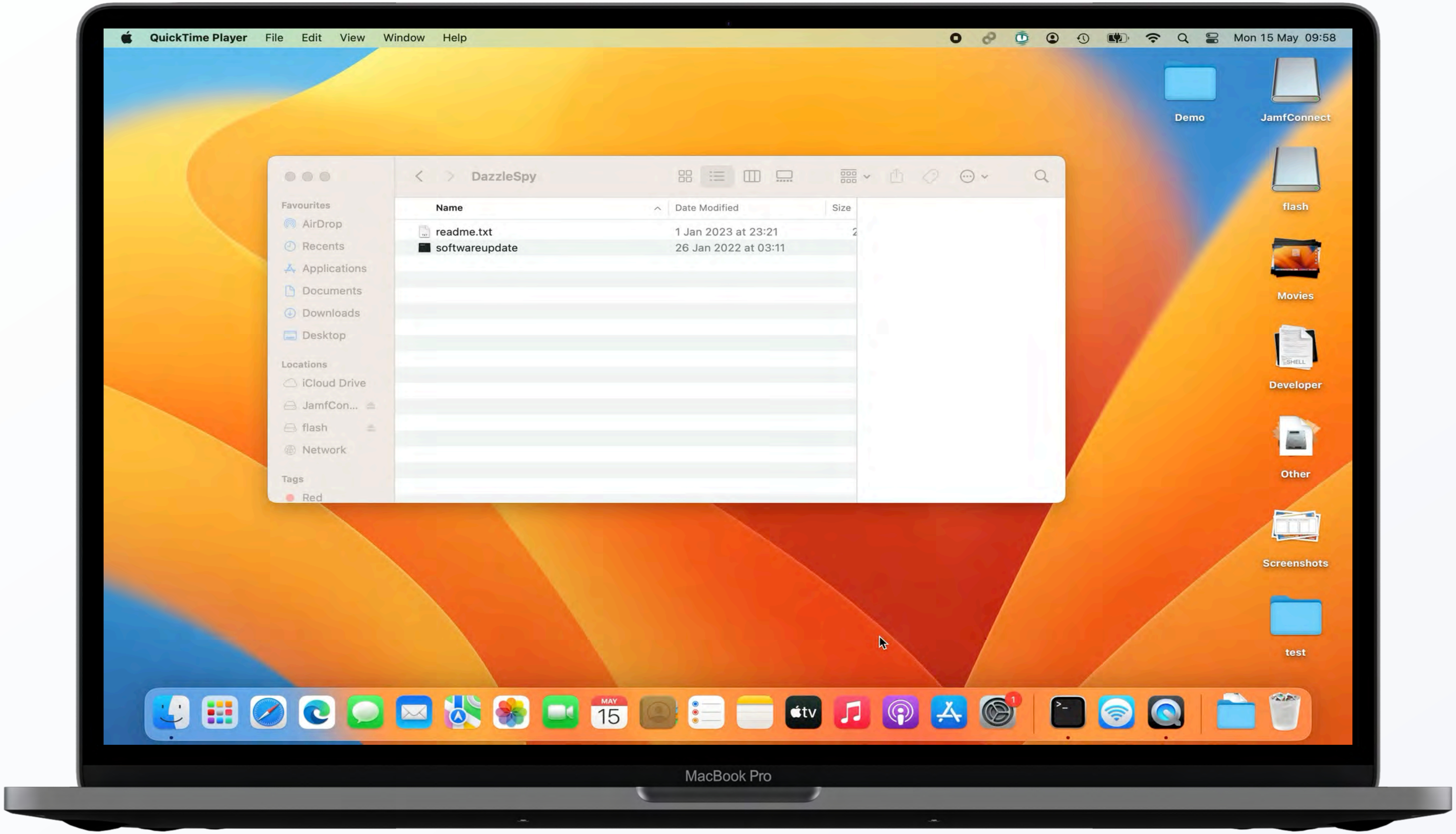


**Examples available on:**
https://github.com/jamf/jamfprotect



# Basic Threat Hunting:

Using Jamf Protect and
Microsoft Sentinel



| Name | Date Modified | Size |
|---|---|---|
| readme.txt | 1 Jan 2023 at 23:21 | 2 |
| softwareupdate | 26 Jan 2022 at 03:11 | |

JAMF NATION LIVE

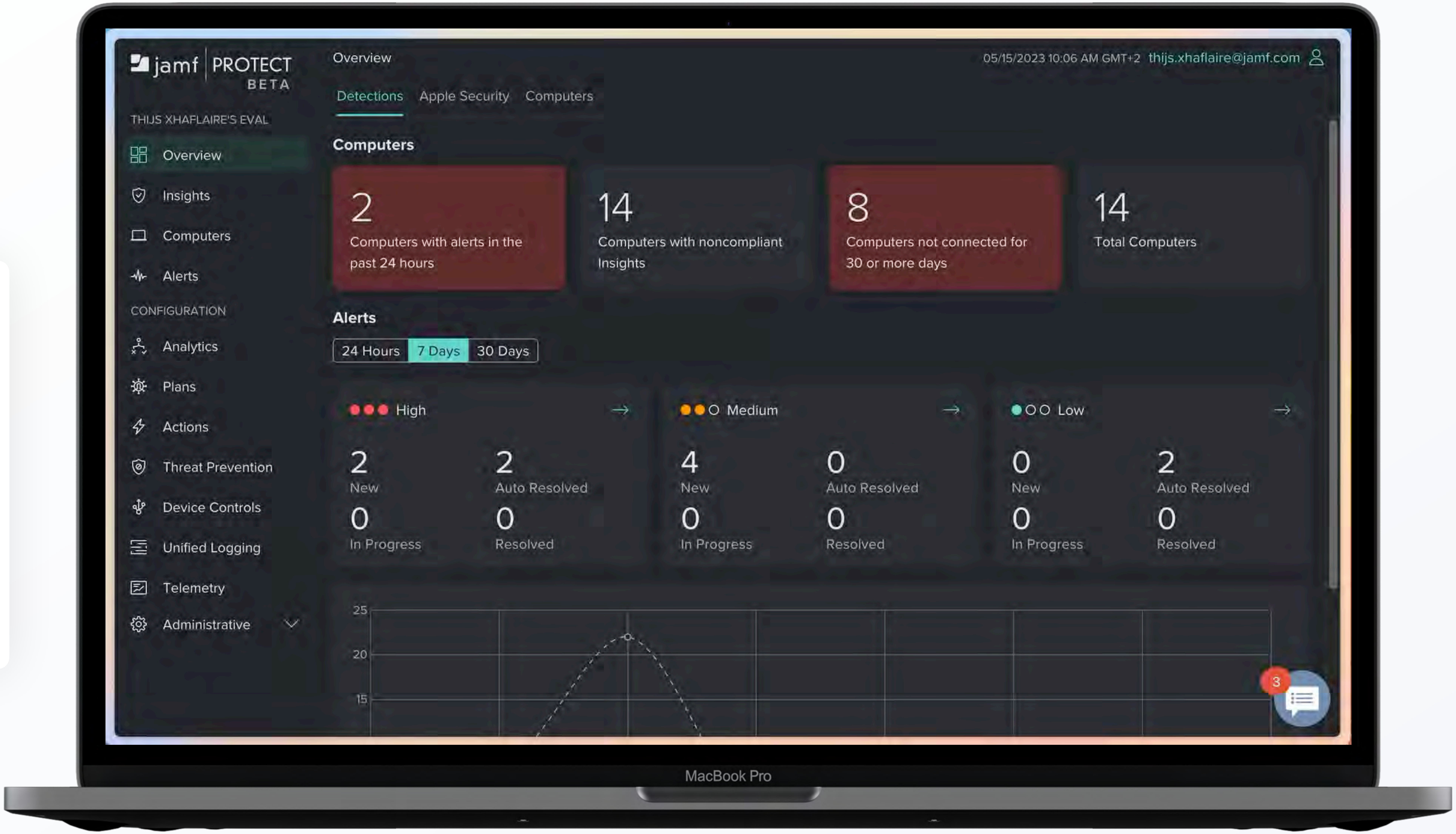
Computer 1

### Threat has been detected

**Security Admin receives and inspects alert in either**

- Jamf Protect macOS Security Portal
- Microsoft Sentinel Workbook or Incidents

Let's take note of the **SHA1 hash** value of the binary



Overview

05/15/2023 10:06 AM GMT+2 thijs.xhaflaire@jamf.com

**Computers**

2 Computers with alerts in the past 24 hours

14 Computers with noncompliant Insights

8 Computers not connected for 30 or more days

14 Total Computers

**Alerts**

●●● High
2 New
2 Auto Resolved
0 In Progress
0 Resolved

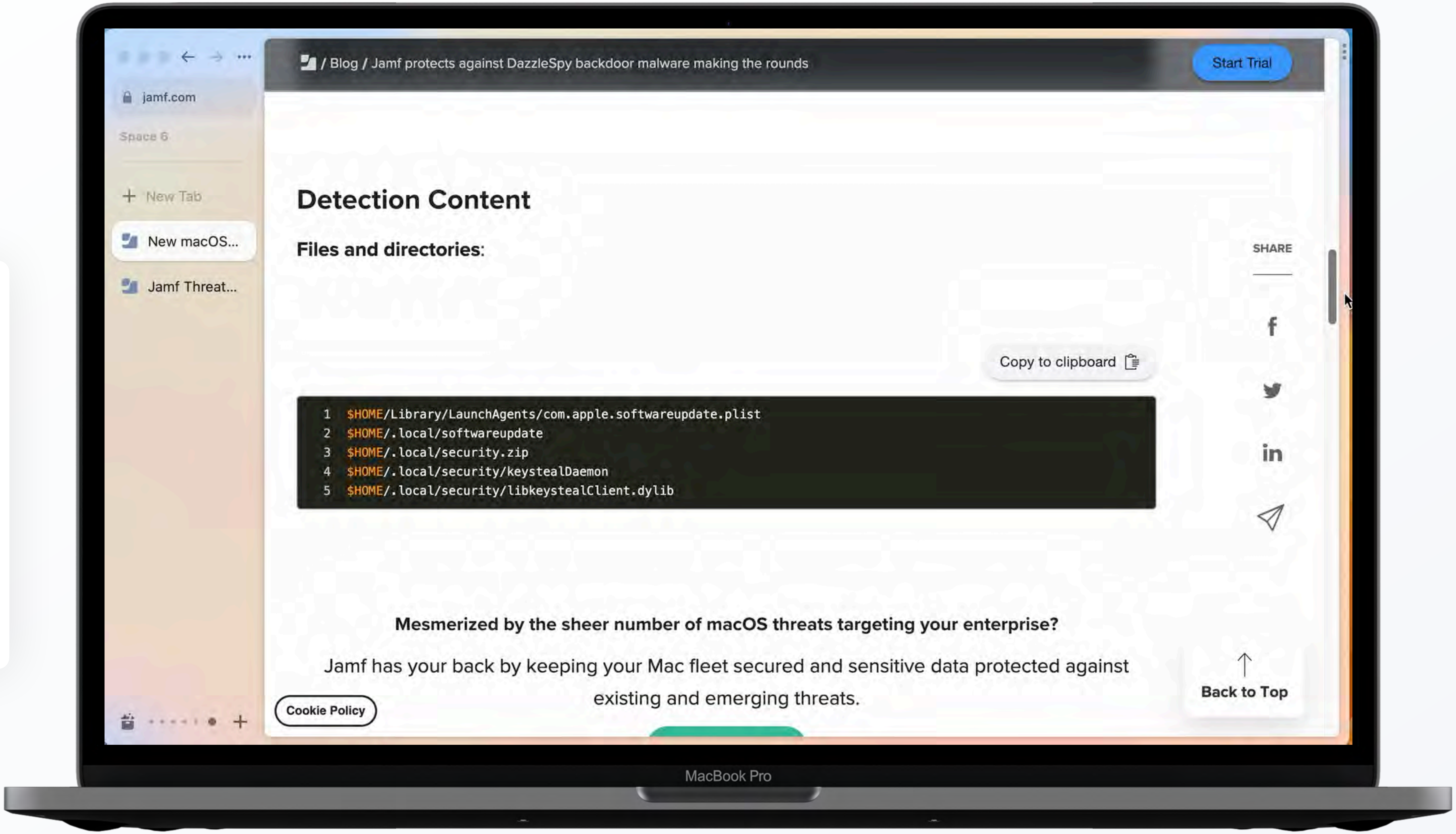
●●○ Medium
4 New
0 Auto Resolved
0 In Progress
0 Resolved

●○○ Low
0 New
2 Auto Resolved
0 In Progress
0 Resolved

●JAMF NATION LIVE

## Indicators of Compromise

```
SHA1 hash of Mach-O
Executable

ee0678e58868ebd6603cc2e0
6a134680d2012c1b

Command And Control (C2)
IPs

88.218.192.128

Related Files

/
com.apple.softwareupdate.pl
ist
./local/softwareupdate
```



## Detection Content

### Files and directories:

```
$HOME/Library/LaunchAgents/com.apple.softwareupdate.plist
$HOME/.local/softwareupdate
$HOME/.local/security.zip
$HOME/.local/security/keystealDaemon
$HOME/.local/security/libkeystealClient.dylib
```

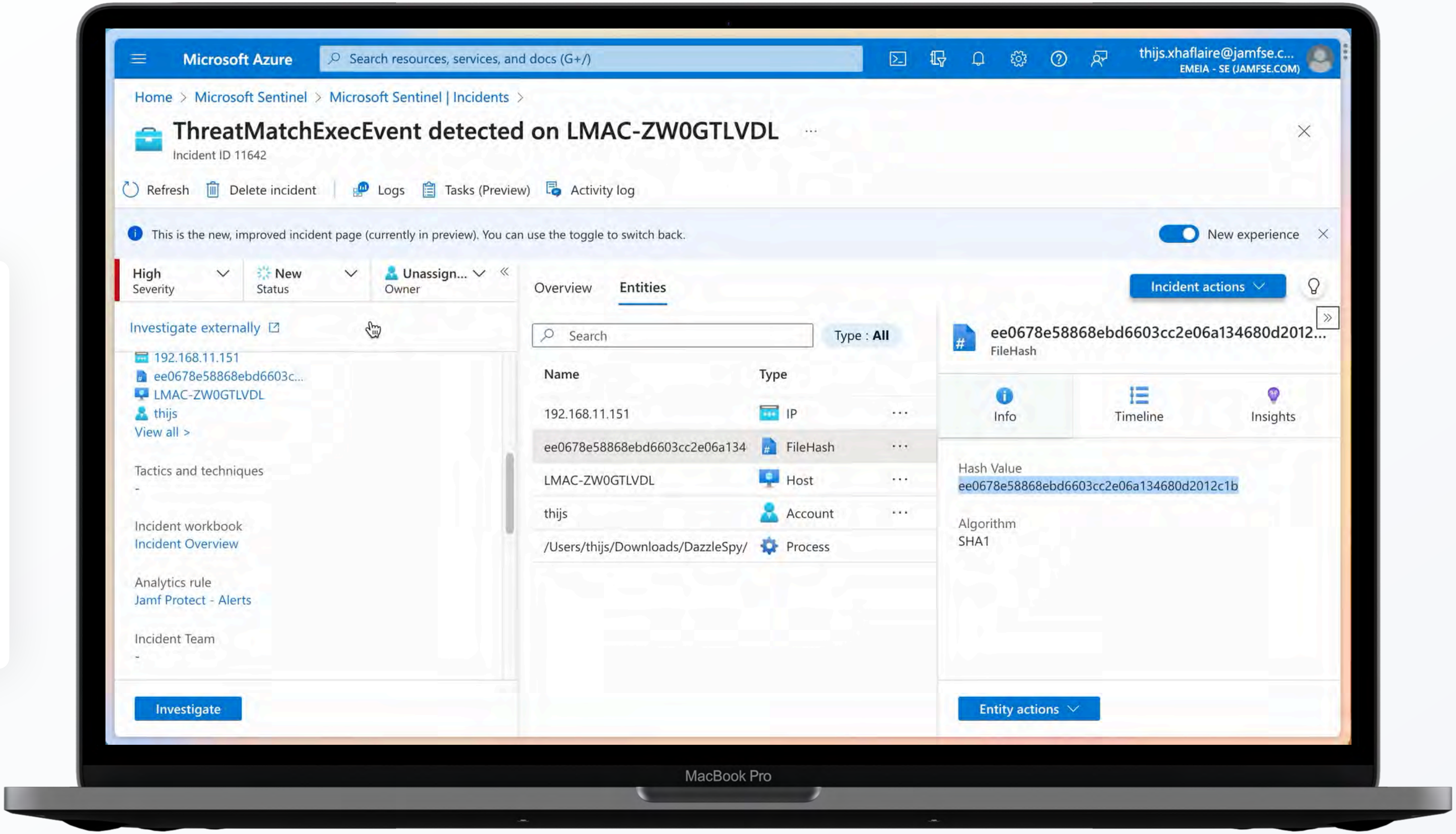
**Mesmerized by the sheer number of macOS threats targeting your enterprise?**

Jamf has your back by keeping your Mac fleet secured and sensitive data protected against existing and emerging threats.

## Let’s start our hunt

Remember we took note of that **SHA1** hash value of the binary?

Let’s start our hunt based on using that hash



Microsoft Azure
Search resources, services, and docs (G+/)
thijs.xhaflaire@jamfse.c...
EMEIA - SE (JAMFSE.COM)
Home > Microsoft Sentinel > Microsoft Sentinel | Incidents >

ThreatMatchExecEvent detected on LMAC-ZW0GTLVDL

Incident ID 11642

This is the new, improved incident page (currently in preview). You can use the toggle to switch back.

Severity: High
Status: New
Owner: Unassign...

Tactics and techniques
-

Incident workbook
Incident Overview

Analytics rule
Jamf Protect - Alerts

Incident Team
-

| Name | Type |
|---|---|
| 192.168.11.151 | IP |
| ee0678e58868ebd6603cc2e06a134 | FileHash |
| LMAC-ZW0GTLVDL | Host |
| thijs | Account |
| /Users/thijs/Downloads/DazzleSpy/ | Process |

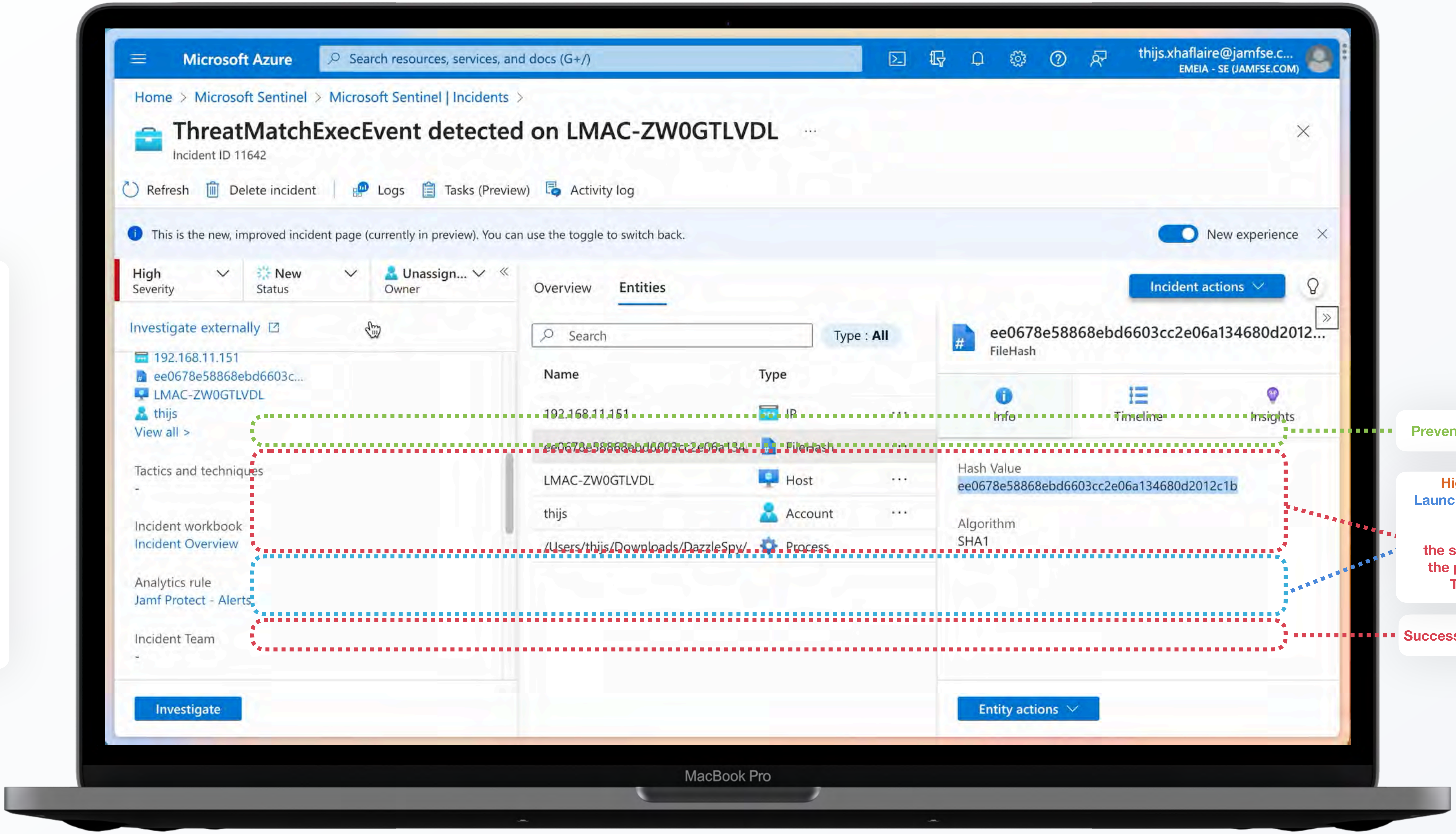
ee0678e58868ebd6603cc2e06a134680d2012...
FileHash

Hash Value
ee0678e58868ebd6603cc2e06a134680d2012c1b

Algorithm
SHA1

## Let’s start our hunt

```
Remember we took note of
that SHA1 hash value of
the binary?

Let’s start our hunt
based on using that hash
```



Microsoft Azure — Search resources, services, and docs (G+/) — thijs.xhaflaire@jamfse.c... EMEIA - SE (JAMFSE.COM)

Home > Microsoft Sentinel > Microsoft Sentinel | Incidents >

ThreatMatchExecEvent detected on LMAC-ZW0GTLVDL

Incident ID 11642

This is the new, improved incident page (currently in preview). You can use the toggle to switch back.

High — Severity

New — Status

Unassign... — Owner

192.168.11.151
ee0678e58868ebd6603c...
LMAC-ZW0GTLVDL
thijs
View all >

Tactics and techniques
-

Incident workbook
Incident Overview

Analytics rule
Jamf Protect - Alerts

Incident Team
-

Type : **All**

| Name | Type |
|---|---|
| 192.168.11.151 | IP |
| ee0678e58868ebd6603cc2e06a134 | FileHash |
| LMAC-ZW0GTLVDL | Host |
| thijs | Account |
| /Users/thijs/Downloads/DazzleSpy/ | Process |

ee0678e58868ebd6603cc2e06a134680d2012...
FileHash

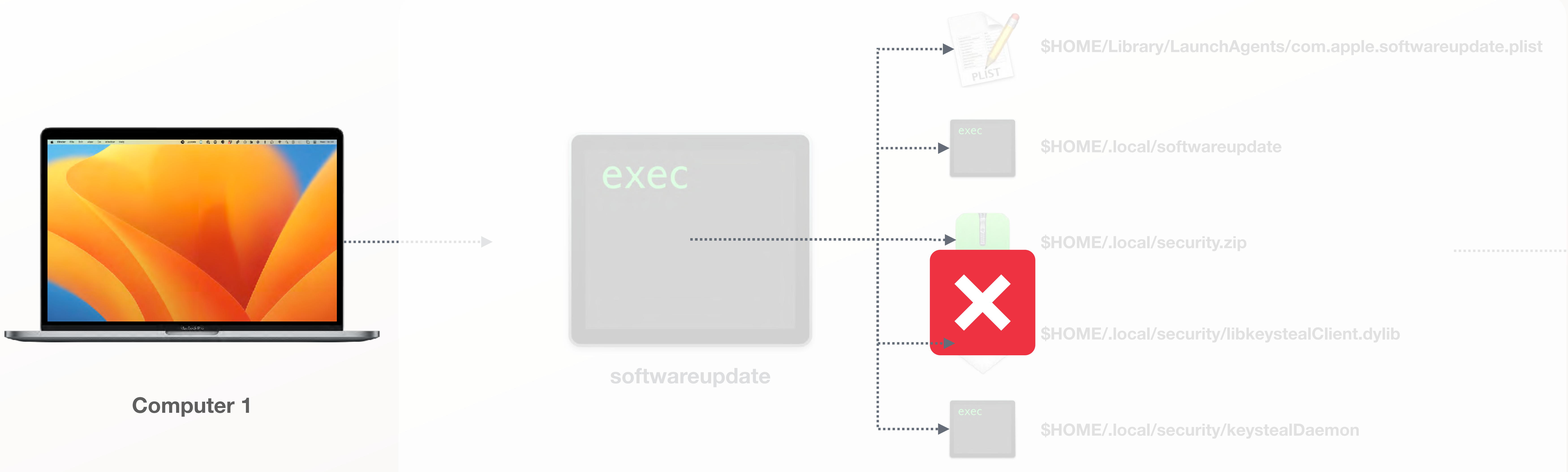
Hash Value
ee0678e58868ebd6603cc2e06a134680d2012c1b

Algorithm
SHA1

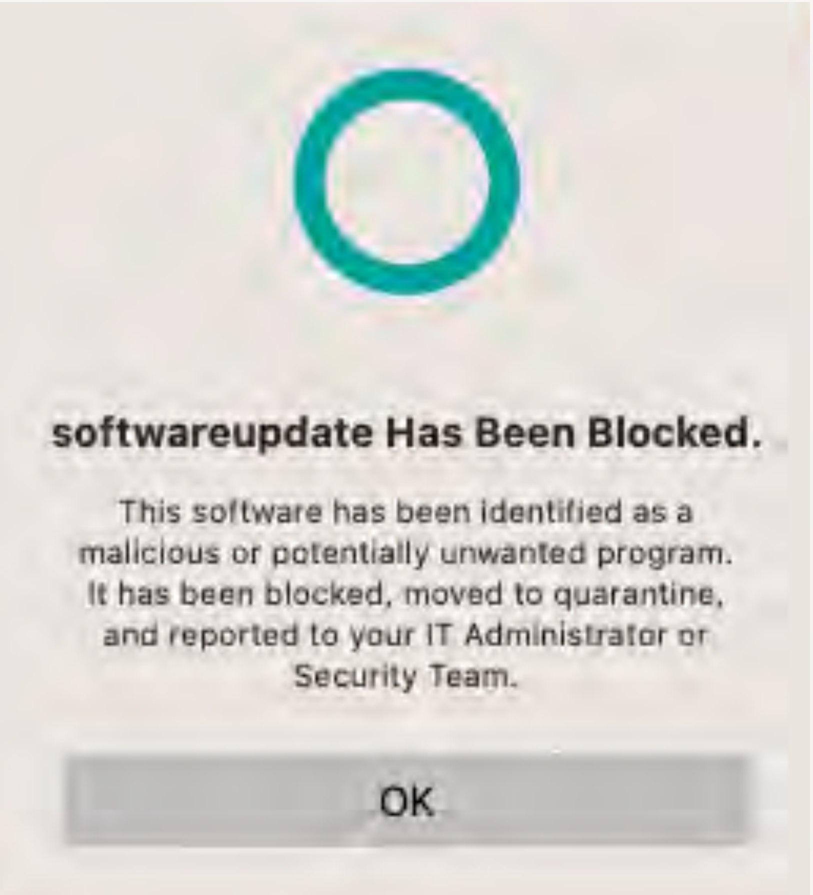
Prevented by Jamf Protect

Highly Suspicious LaunchAgent loaded onto the system and executes the softwareupdate and the process generates Traffic to C2 IPs

Successful Process Creation


Computer 1
exec
softwareupdate
$HOME/Library/LaunchAgents/com.apple.softwareupdate.plist
exec
$HOME/.local/softwareupdate
$HOME/.local/security.zip
$HOME/.local/security/libkeystealClient.dylib
exec
$HOME/.local/security/keystealDaemon

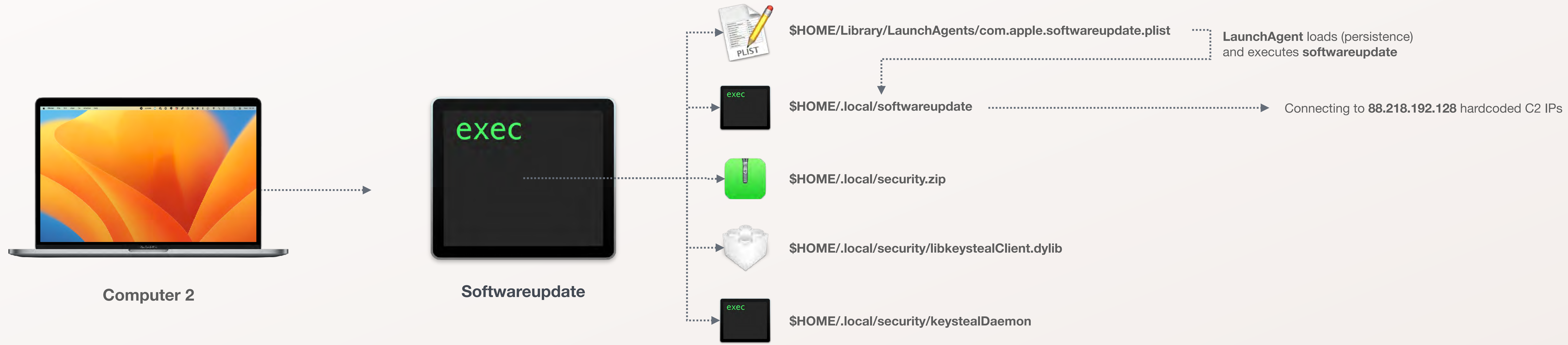
10:58AM — User executes **softwareupdate** binary



**softwareupdate Has Been Blocked.**

This software has been identified as a malicious or potentially unwanted program. It has been blocked, moved to quarantine, and reported to your IT Administrator or Security Team.

**10:58AM** - Prevented process execution by Jamf Protect as there was a signature match

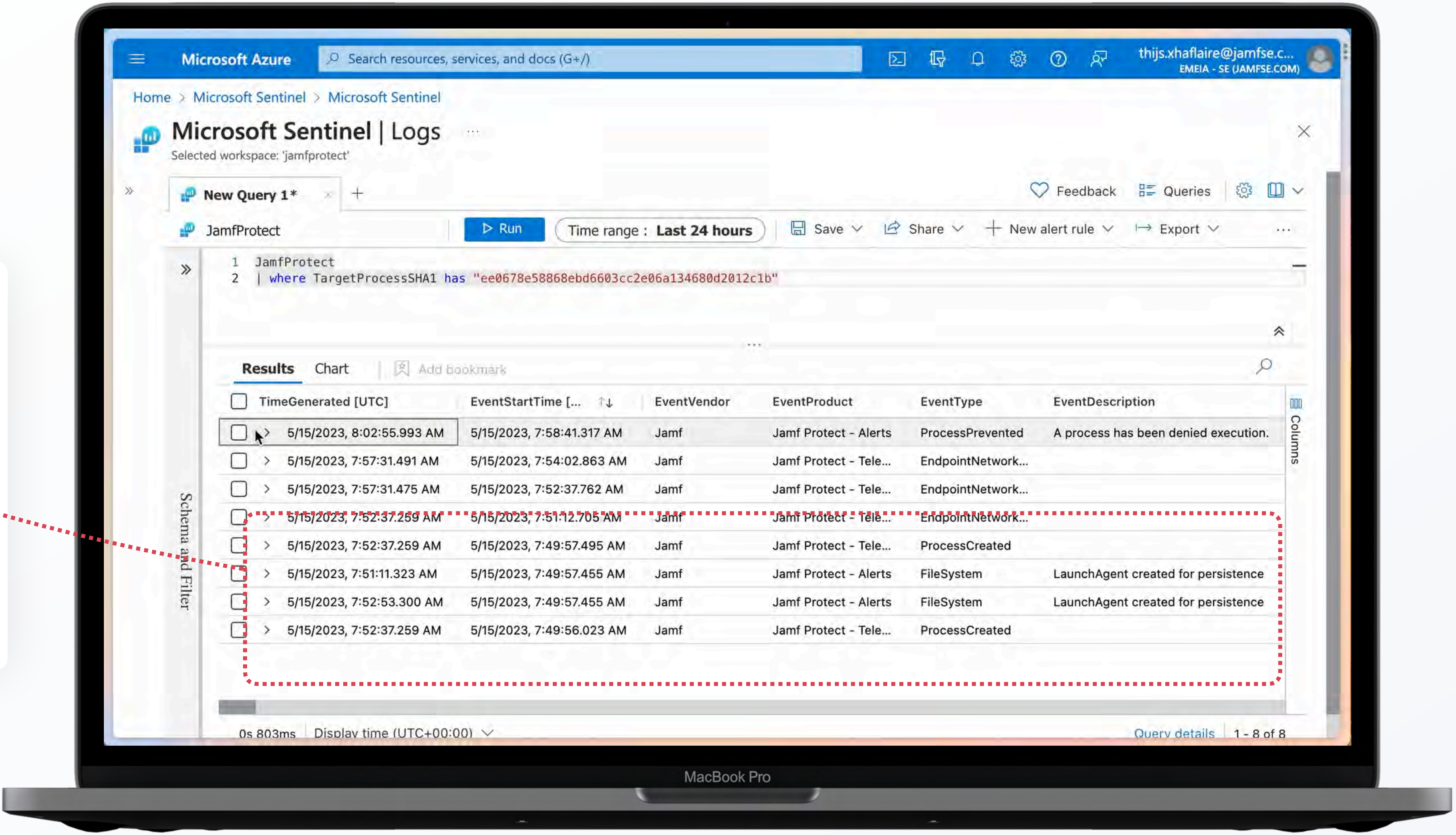

Computer 2
exec
Softwareupdate
$HOME/Library/LaunchAgents/com.apple.softwareupdate.plist
LaunchAgent loads (persistence) and executes softwareupdate
exec
$HOME/.local/softwareupdate
Connecting to 88.218.192.128 hardcoded C2 IPs
$HOME/.local/security.zip
$HOME/.local/security/libkeystealClient.dylib
exec
$HOME/.local/security/keystealDaemon

**10:48AM** — User executes **softwareupdate** binary

### Investigation

Let’s **inspect** the first event matching to the **SHA1 hash**

**ProcessCreated** event, user executing the malicious **softwareupdate** binary from the download folder


Microsoft Azure
Search resources, services, and docs (G+/)
thijs.xhaflaire@jamfse.c...
EMEIA - SE (JAMFSE.COM)
Home > Microsoft Sentinel > Microsoft Sentinel
Microsoft Sentinel | Logs
Selected workspace: 'jamfprotect'
New Query 1*
Feedback
Queries
JamfProtect
Run
Time range : Last 24 hours
Save
Share
New alert rule
Export
Results
Chart
Add bookmark
Schema and Filter
Columns
MacBook Pro

```
JamfProtect
| where TargetProcessSHA1 has "ee0678e58868ebd6603cc2e06a134680d2012c1b"
```

| TimeGenerated [UTC] | EventStartTime [... | EventVendor | EventProduct | EventType | EventDescription |
|---|---|---|---|---|---|
| 5/15/2023, 8:02:55.993 AM | 5/15/2023, 7:58:41.317 AM | Jamf | Jamf Protect - Alerts | ProcessPrevented | A process has been denied execution. |
| 5/15/2023, 7:57:31.491 AM | 5/15/2023, 7:54:02.863 AM | Jamf | Jamf Protect - Tele... | EndpointNetwork... | |
| 5/15/2023, 7:57:31.475 AM | 5/15/2023, 7:52:37.762 AM | Jamf | Jamf Protect - Tele... | EndpointNetwork... | |
| 5/15/2023, 7:52:37.259 AM | 5/15/2023, 7:51:12.705 AM | Jamf | Jamf Protect - Tele... | EndpointNetwork... | |
| 5/15/2023, 7:52:37.259 AM | 5/15/2023, 7:49:57.495 AM | Jamf | Jamf Protect - Tele... | ProcessCreated | |
| 5/15/2023, 7:51:11.323 AM | 5/15/2023, 7:49:57.455 AM | Jamf | Jamf Protect - Alerts | FileSystem | LaunchAgent created for persistence |
| 5/15/2023, 7:52:53.300 AM | 5/15/2023, 7:49:57.455 AM | Jamf | Jamf Protect - Alerts | FileSystem | LaunchAgent created for persistence |
| 5/15/2023, 7:52:37.259 AM | 5/15/2023, 7:49:56.023 AM | Jamf | Jamf Protect - Tele... | ProcessCreated | |

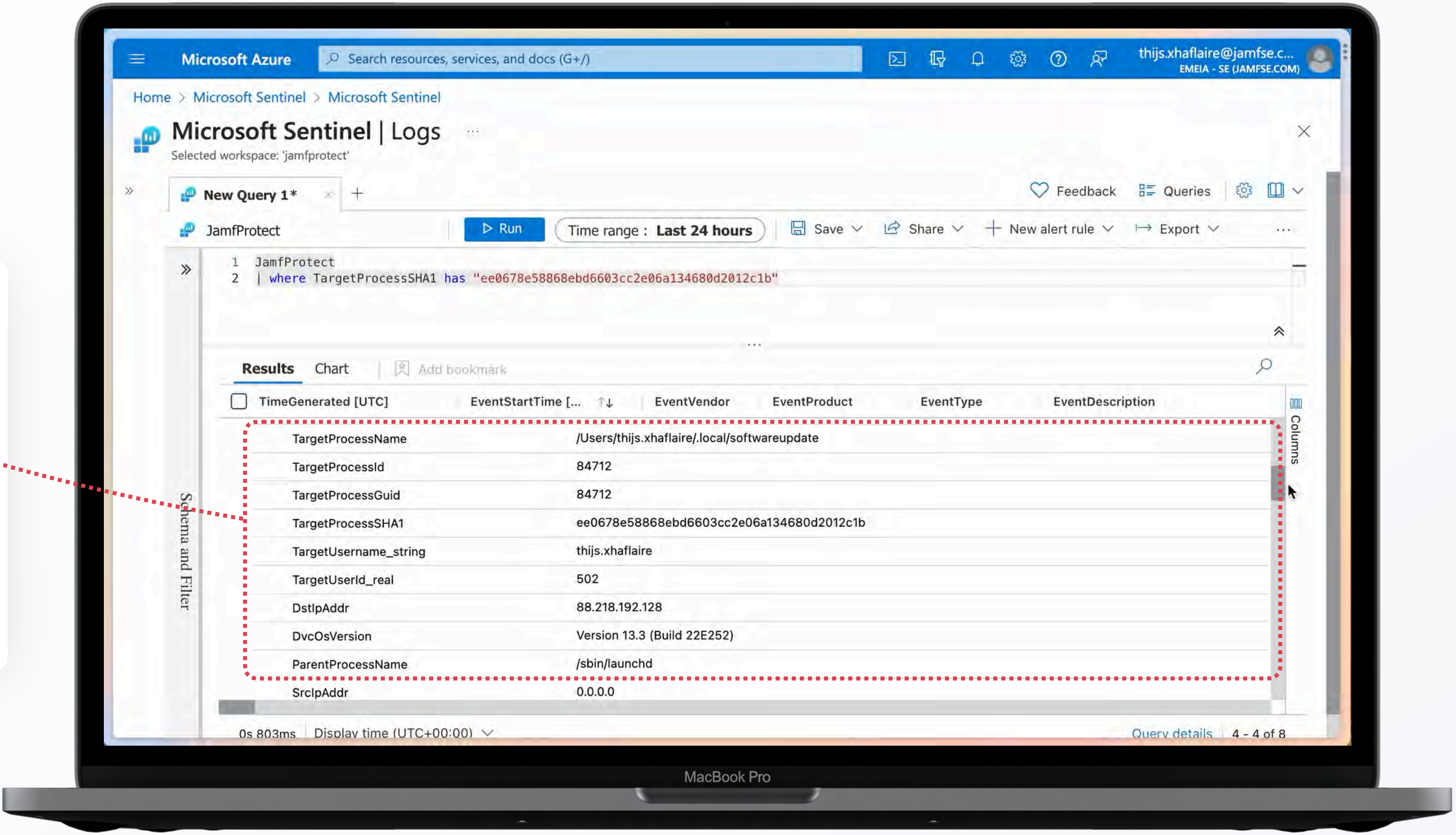
0s 803ms | Display time (UTC+00:00)   Query details | 1 - 8 of 8

### Investigation

**Network** event, the earlier shown **LaunchAgent** is executing the **TargetProcessName** and the **softwareupdate** process is creating a network connection to **DstIpAddr**

## C2 IP IoC

```
88.218.192[.]128:5633
```



Microsoft Azure
Search resources, services, and docs (G+/)
thijs.xhaflaire@jamfse.c...
EMEIA - SE (JAMFSE.COM)
Home > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel | Logs

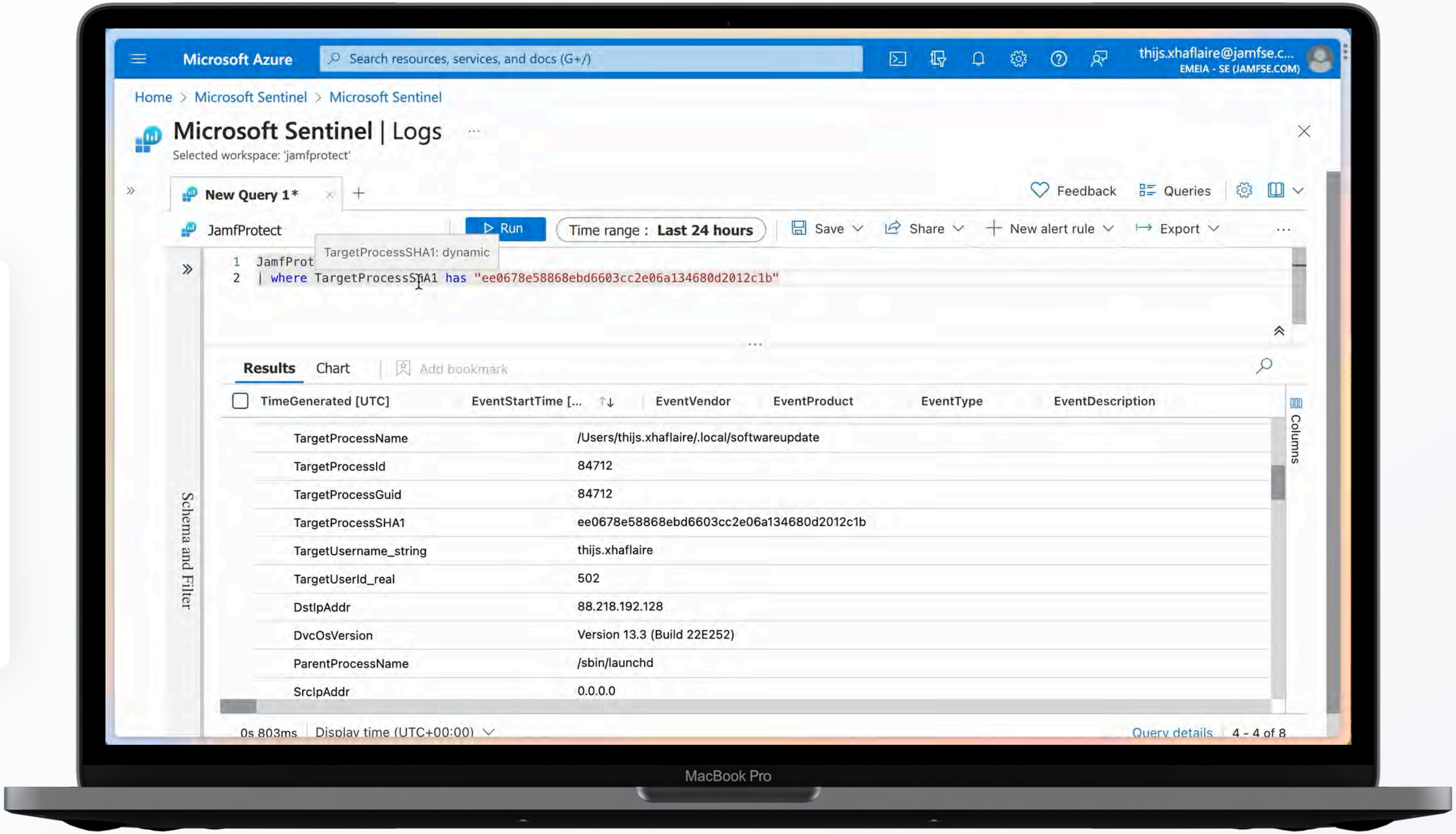
Selected workspace: 'jamfprotect'

```
JamfProtect
| where TargetProcessSHA1 has "ee0678e58868ebd6603cc2e06a134680d2012c1b"
```

| | |
|---|---|
| TargetProcessName | /Users/thijs.xhaflaire/.local/softwareupdate |
| TargetProcessId | 84712 |
| TargetProcessGuid | 84712 |
| TargetProcessSHA1 | ee0678e58868ebd6603cc2e06a134680d2012c1b |
| TargetUsername_string | thijs.xhaflaire |
| TargetUserId_real | 502 |
| DstIpAddr | 88.218.192.128 |
| DvcOsVersion | Version 13.3 (Build 22E252) |
| ParentProcessName | /sbin/launchd |
| SrcIpAddr | 0.0.0.0 |

### Investigation

We could even start our hunt by searching on the **C2 destination IPs** to search for matching events and if any other devices are reaching out to the **C2 IPs/Domains**


Microsoft Azure
Search resources, services, and docs (G+/)
thijs.xhaflaire@jamfse.c...
EMEIA - SE (JAMFSE.COM)
Home > Microsoft Sentinel > Microsoft Sentinel
Microsoft Sentinel | Logs
Selected workspace: 'jamfprotect'
New Query 1*
Feedback
Queries
JamfProtect
Run
Time range : Last 24 hours
Save
Share
New alert rule
Export
TargetProcessSHA1: dynamic
Results
Chart
Add bookmark
Columns
Schema and Filter
0s 803ms
Display time (UTC+00:00)
Query details
4 - 4 of 8
MacBook Pro

```
JamfProt
| where TargetProcessSHA1 has "ee0678e58868ebd6603cc2e06a134680d2012c1b"
```

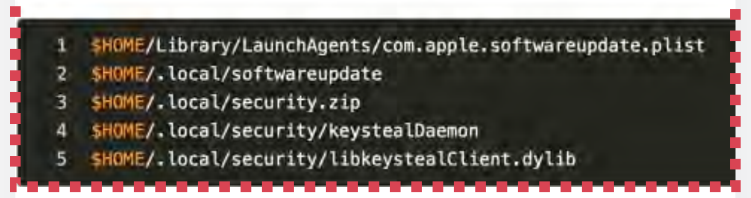
| TimeGenerated [UTC] | EventStartTime [... | EventVendor | EventProduct | EventType | EventDescription |
|---|---|---|---|---|---|

| | |
|---|---|
| TargetProcessName | /Users/thijs.xhaflaire/.local/softwareupdate |
| TargetProcessId | 84712 |
| TargetProcessGuid | 84712 |
| TargetProcessSHA1 | ee0678e58868ebd6603cc2e06a134680d2012c1b |
| TargetUsername_string | thijs.xhaflaire |
| TargetUserId_real | 502 |
| DstIpAddr | 88.218.192.128 |
| DvcOsVersion | Version 13.3 (Build 22E252) |
| ParentProcessName | /sbin/launchd |
| SrcIpAddr | 0.0.0.0 |

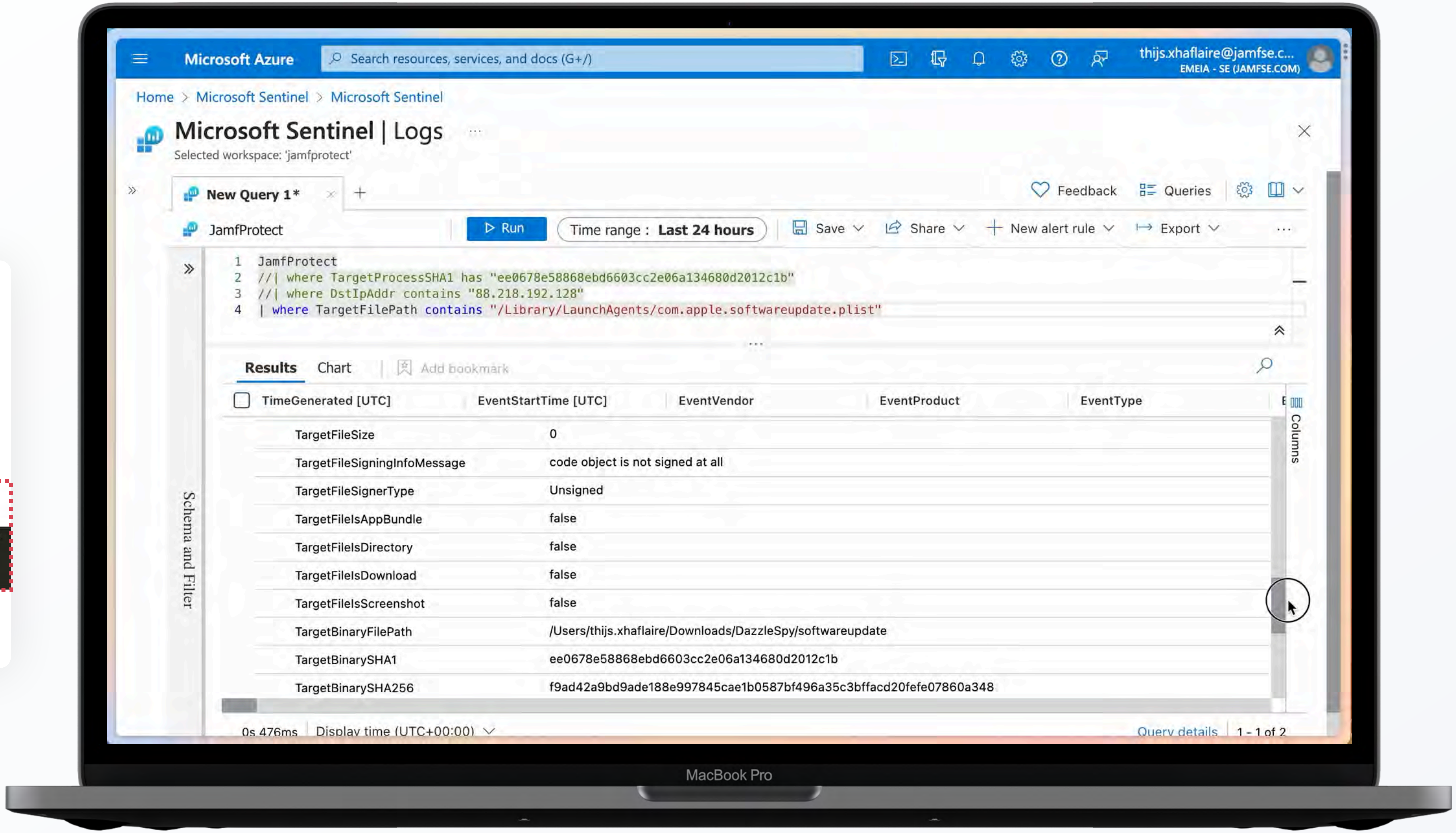
### Investigation

Or search for events that do match the IOC's files and directories

## Files/Directories IoC



```
$HOME/Library/LaunchAgents/com.apple.softwareupdate.plist
$HOME/.local/softwareupdate
$HOME/.local/security.zip
$HOME/.local/security/keystealDaemon
$HOME/.local/security/libkeystealClient.dylib
```


Microsoft Azure
Search resources, services, and docs (G+/)
thijs.xhaflaire@jamfse.c...
EMEIA - SE (JAMFSE.COM)
Home > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel | Logs

Selected workspace: 'jamfprotect'

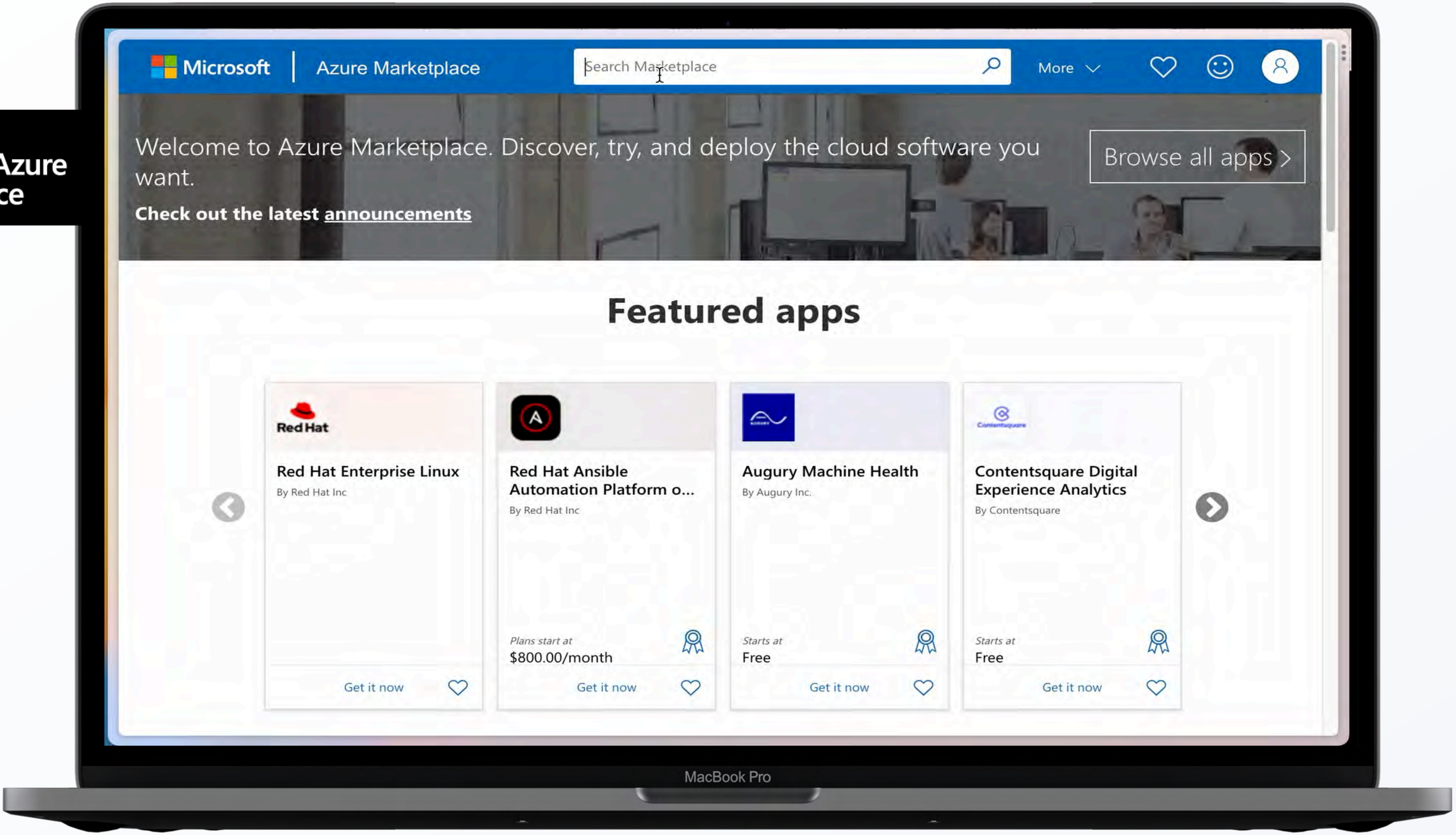
```
JamfProtect
//| where TargetProcessSHA1 has "ee0678e58868ebd6603cc2e06a134680d2012c1b"
//| where DstIpAddr contains "88.218.192.128"
| where TargetFilePath contains "/Library/LaunchAgents/com.apple.softwareupdate.plist"
```

□ TimeGenerated [UTC] | EventStartTime [UTC] | EventVendor | EventProduct | EventType

| | |
|---|---|
| TargetFileSize | 0 |
| TargetFileSigningInfoMessage | code object is not signed at all |
| TargetFileSignerType | Unsigned |
| TargetFileIsAppBundle | false |
| TargetFileIsDirectory | false |
| TargetFileIsDownload | false |
| TargetFileIsScreenshot | false |
| TargetBinaryFilePath | /Users/thijs.xhaflaire/Downloads/DazzleSpy/softwareupdate |
| TargetBinarySHA1 | ee0678e58868ebd6603cc2e06a134680d2012c1b |
| TargetBinarySHA256 | f9ad42a9bd9ade188e997845cae1b0587bf496a35c3bffacd20fefe07860a348 |

0s 476ms | Display time (UTC+00:00) | Query details | 1 - 1 of 2

Get it from
Microsoft Azure
Marketplace



Microsoft | Azure Marketplace

Welcome to Azure Marketplace. Discover, try, and deploy the cloud software you want.

Check out the latest announcements

## Featured apps

Red Hat Enterprise Linux
By Red Hat Inc

Red Hat Ansible Automation Platform o...
By Red Hat Inc
*Plans start at*
$800.00/month

Augury Machine Health
By Augury Inc.
*Starts at*
Free

Contentsquare Digital Experience Analytics
By Contentsquare
*Starts at*
Free

# Session **recap**

**Features** and **relevance of event forwarding**

Flexible **data forwarding** and **streaming** options

**Integrations** and **add-ons**

Threat Hunting with **Jamf Protect** and a **SIEM**

# How **Dyson uses Jamf** in their security stack

JAMF NATION LIVE

**Gary Bidwell**

**Apple Solutions Architect**
Dyson

# Thanks 🍻