Secure SIGHT

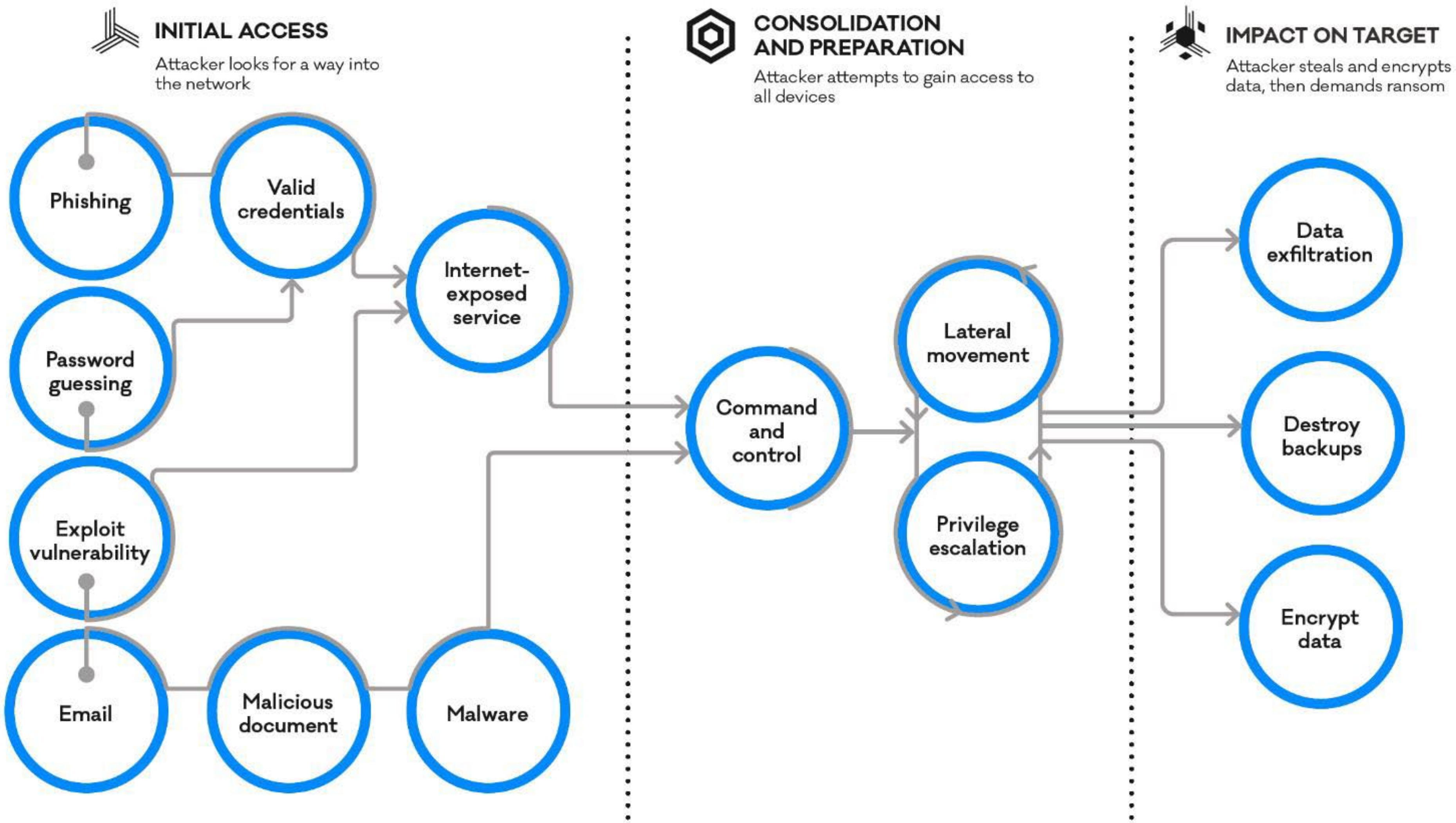
by Secutec

Secure SIGHT

Discover how Internet intelligence can help you make better decisions.

Lifecycle of a Ransomware Incident

certnz

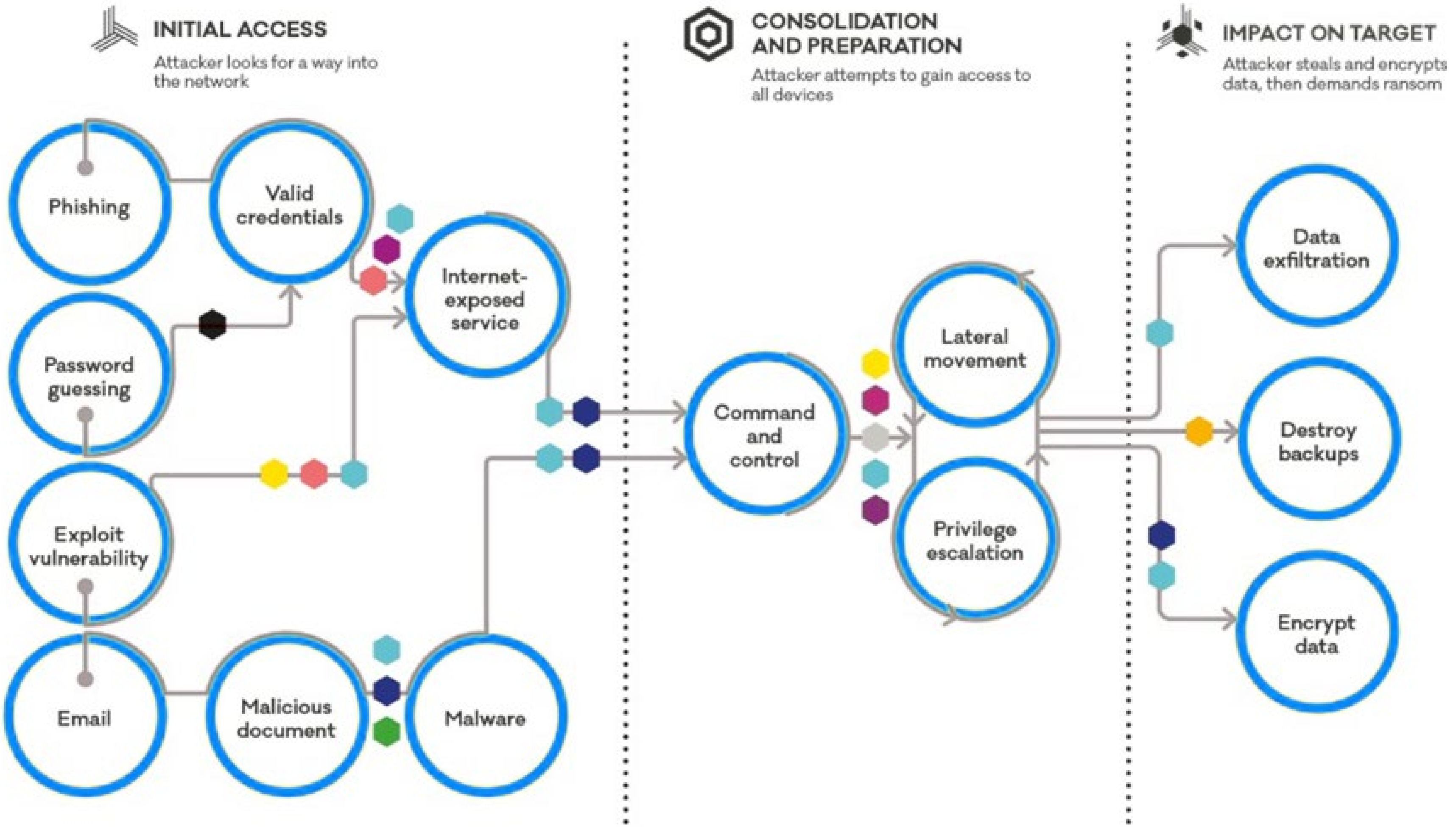


Lifecycle of a Ransomware Incident

certnz

CRITICAL CONTROLS KEY

- 🟥 Internet-exposed services
- 🟧 Backups
- 🟨 Patching
- 🟦 Application allowlisting
- 🟪 MFA
- 🔵 Logging and alerting
- 🩷 Network segmentation
- 🟩 Disable macros
- ⬜ Principle of least privilege
- ⬛ Password manager



INITIAL ACCESS

Attacker looks for a way into the network

CONSOLIDATION AND PREPARATION

Attacker attempts to gain access to all devices

IMPACT ON TARGET

Attacker steals and encrypts data, then demands ransom

Monitoring Components

MONITOR COMPONENTS	ADVANCED	ULTIMATE
Vulnerability Scanning	✓	✓
Account Takeover Fraud Prevention and Monitoring	✓	✓
Active Managed Threat hunting	✓	✓
Managed EDR on Servers	✗	✓

ADVANCED

ULTIMATE

Vulnerability Scanning

- High-level look at possible vulnerabilities
- Coverage for more than 65K vulnerabilities
- SOC alerts – detections immediately reported
- Weekly reports

SIGHT

ADVANCED

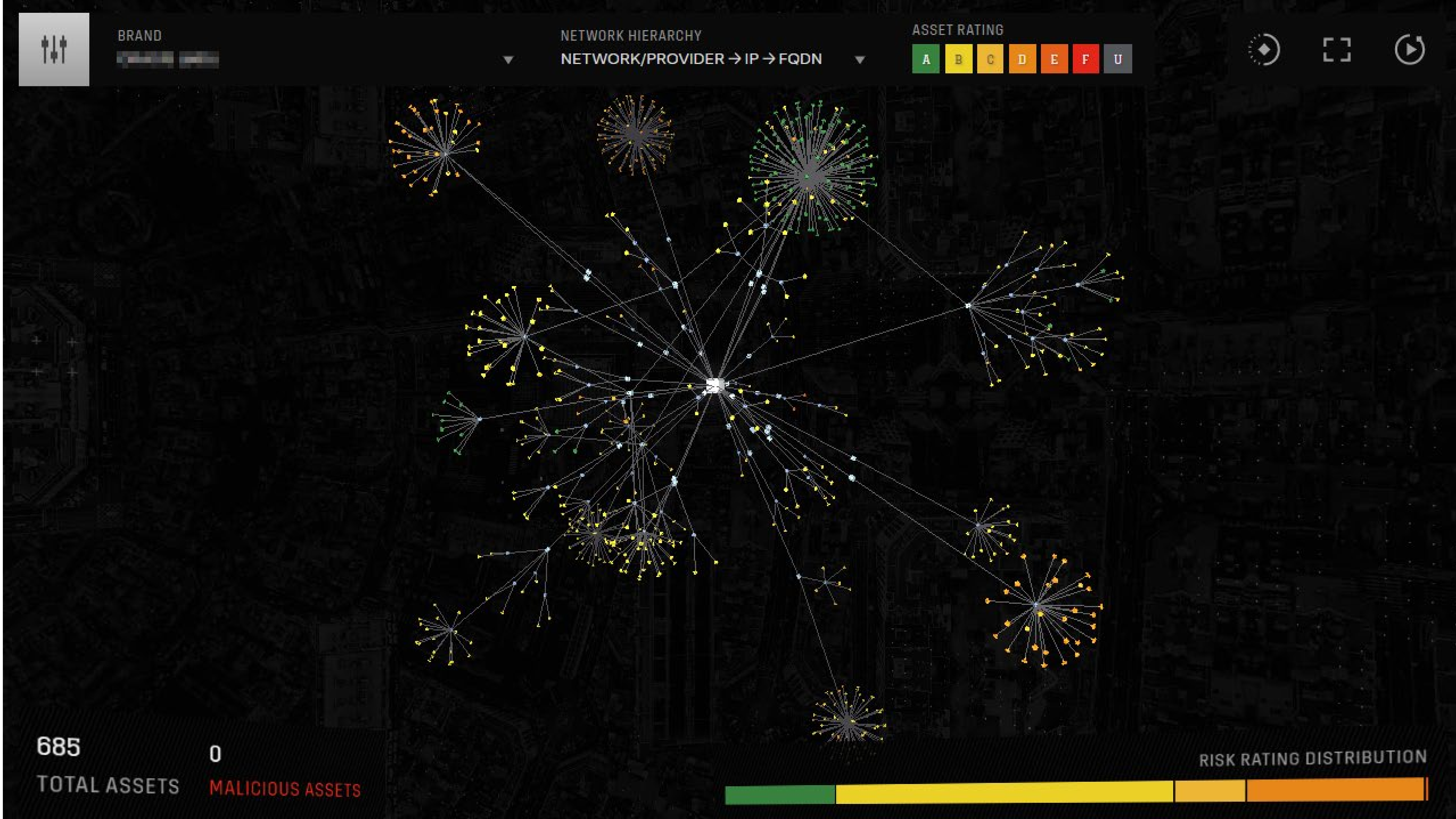
- Weekly Vulnerability Scanning
- Account Takeover Fraud Prevention and Monitoring
- Active Managed Threat hunting

SIGHT

ULTIMATE

- Weekly Vulnerability Scanning
- Account Takeover Fraud Prevention and Monitoring
- Active Managed Threat hunting
- Managed EDR on Servers

Secutec
Cyber security intelligence



BRAND

[redacted]

NETWORK HIERARCHY

NETWORK/PROVIDER → IP → FQDN

ASSET RATING

A B C D E F U

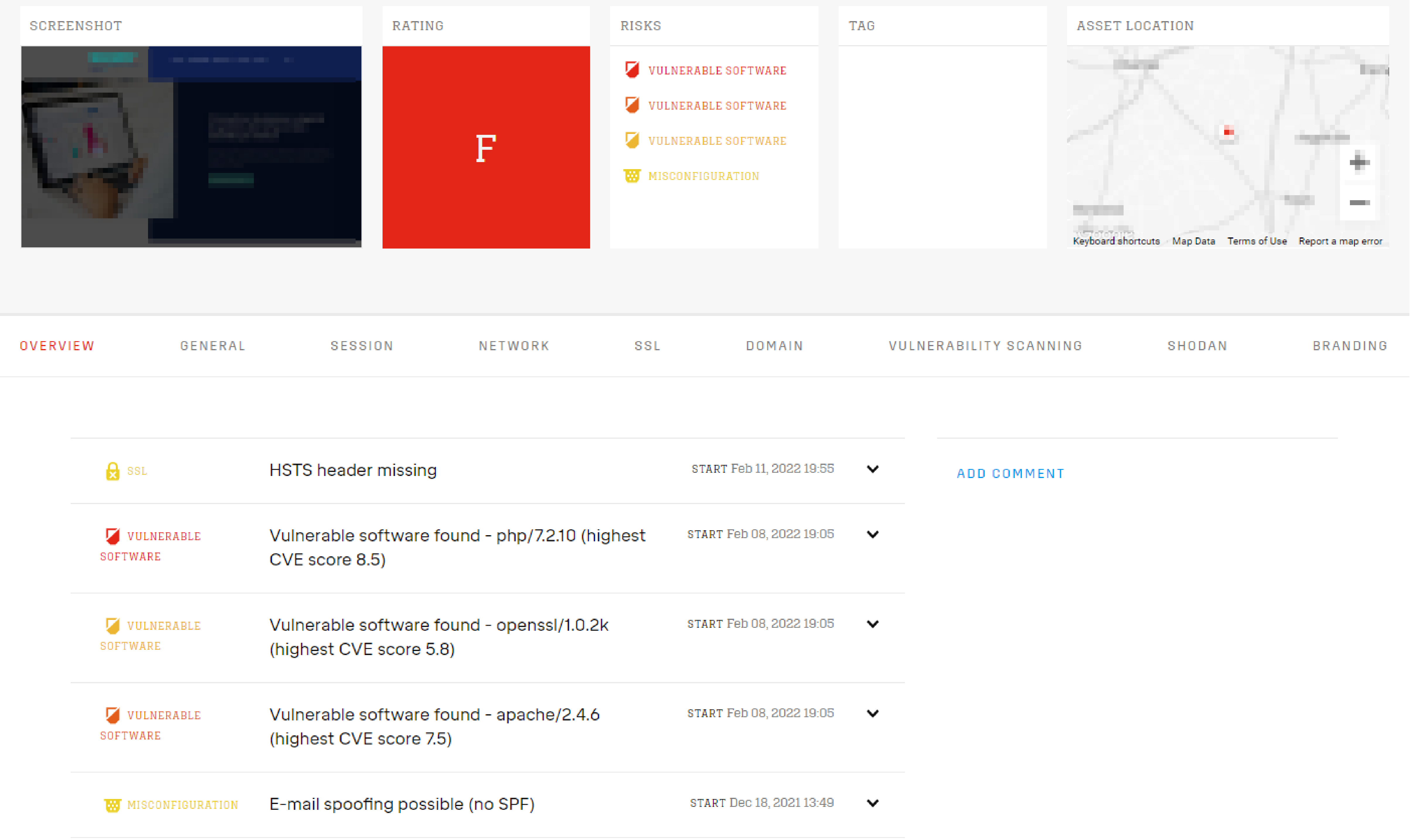
685

TOTAL ASSETS

0

MALICIOUS ASSETS

RISK RATING DISTRIBUTION



SSL	HSTS header missing	START Feb 11, 2022 19:55
VULNERABLE SOFTWARE	Vulnerable software found - php/7.2.10 (highest CVE score 8.5)	START Feb 08, 2022 19:05
VULNERABLE SOFTWARE	Vulnerable software found - openssl/1.0.2k (highest CVE score 5.8)	START Feb 08, 2022 19:05
VULNERABLE SOFTWARE	Vulnerable software found - apache/2.4.6 (highest CVE score 7.5)	START Feb 08, 2022 19:05
MISCONFIGURATION	E-mail spoofing possible (no SPF)	START Dec 18, 2021 13:49

ADVANCED

ULTIMATE

Account Takeover Fraud Prevention and Monitoring

- Recover the most current breached data directly from the criminal underground
- User credentials: email/ username and password
- Dark Web Monitoring

SIGHT
ADVANCED

- Weekly Vulnerability Scanning
- Account Takeover Fraud Prevention and Monitoring
- Active Managed Threat hunting

SIGHT
ULTIMATE

- Weekly Vulnerability Scanning
- Account Takeover Fraud Prevention and Monitoring
- Active Managed Threat hunting
- Managed EDR on Servers

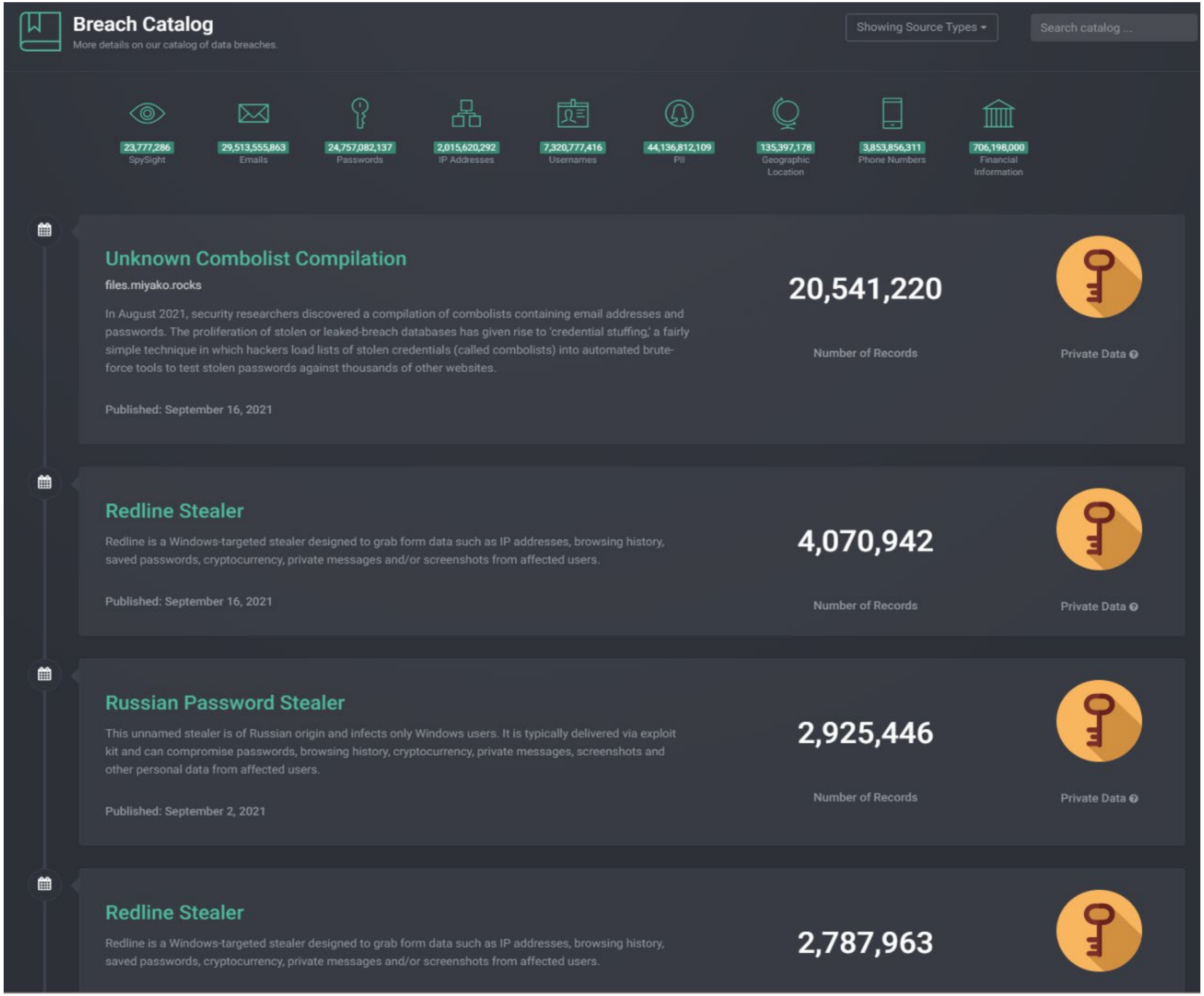
Secutec
Cyber security intelligence

137+ BILLION
Recovered Breach Assets

24+ BILLION
Total Passwords

29+ BILLION
Emails

50+
Breach Sources Collected Per Week



Breach Catalog

More details on our catalog of data breaches.

23,777,286	29,513,555,863	24,757,082,137	2,015,620,292	7,320,777,416	44,136,812,109	135,397,178	3,853,856,311	706,198,000
SpySight	Emails	Passwords	IP Addresses	Usernames	PII	Geographic Location	Phone Numbers	Financial Information

Unknown Combolist Compilation

files.miyako.rocks

In August 2021, security researchers discovered a compilation of combolists containing email addresses and passwords. The proliferation of stolen or leaked-breach databases has given rise to 'credential stuffing,' a fairly simple technique in which hackers load lists of stolen credentials (called combolists) into automated brute-force tools to test stolen passwords against thousands of other websites.

Published: September 16, 2021

20,541,220
Number of Records

Private Data

Redline Stealer

Redline is a Windows-targeted stealer designed to grab form data such as IP addresses, browsing history, saved passwords, cryptocurrency, private messages and/or screenshots from affected users.

Published: September 16, 2021

4,070,942
Number of Records

Private Data

Russian Password Stealer

This unnamed stealer is of Russian origin and infects only Windows users. It is typically delivered via exploit kit and can compromise passwords, browsing history, cryptocurrency, private messages, screenshots and other personal data from affected users.

Published: September 2, 2021

2,925,446
Number of Records

Private Data

Redline Stealer

Redline is a Windows-targeted stealer designed to grab form data such as IP addresses, browsing history, saved passwords, cryptocurrency, private messages and/or screenshots from affected users.

2,787,963

ADVANCED

ULTIMATE

Active Managed Threat hunting

- Weekly parsing of all connections to find suspicious connections
- 70% of all continental internet traffic
- 99% visibility on all malicious connections
- 35 Security Vendor Feeds

SIGHT

ADVANCED

- Weekly Vulnerability Scanning
- Account Takeover Fraud Prevention and Monitoring
- Active Managed Threat hunting

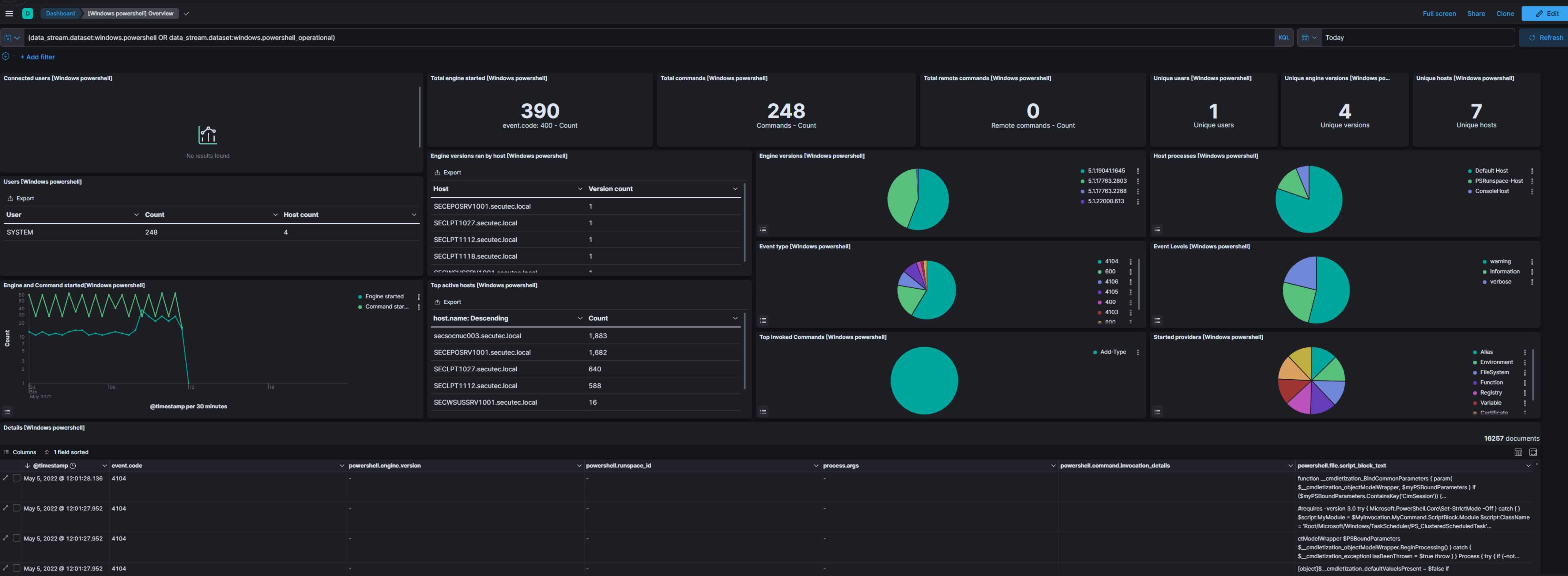
SIGHT

ULTIMATE

- Weekly Vulnerability Scanning
- Account Takeover Fraud Prevention and Monitoring
- Active Managed Threat hunting
- Managed EDR on Servers

Secutec

Cyber security intelligence



(data_stream.dataset:windows.powershell OR data_stream.dataset:windows.powershell_operational)

Connected users [Windows powershell]

No results found

Total engine started [Windows powershell]

390
event.code: 400 - Count

Total commands [Windows powershell]

248
Commands - Count

Total remote commands [Windows powershell]

0
Remote commands - Count

Unique users [Windows powershell]

1
Unique users

Unique engine versions [Windows po...

4
Unique versions

Unique hosts [Windows powershell]

7
Unique hosts

Users [Windows powershell]

Export

User	Count	Host count
SYSTEM	248	4

Engine versions ran by host [Windows powershell]

Export

Host	Version count
SECEPOSRV1001.secutec.local	1
SECLPT1027.secutec.local	1
SECLPT1112.secutec.local	1
SECLPT1118.secutec.local	1
SECWSUSSRV1001.secutec.local	1

Engine versions [Windows powershell]

Host processes [Windows powershell]

Event type [Windows powershell]

Event Levels [Windows powershell]

Engine and Command started[Windows powershell]

Top active hosts [Windows powershell]

Export

host.name: Descending	Count
secsocnuc003.secutec.local	1,883
SECEPOSRV1001.secutec.local	1,682
SECLPT1027.secutec.local	640
SECLPT1112.secutec.local	588
SECWSUSSRV1001.secutec.local	16

Top Invoked Commands [Windows powershell]

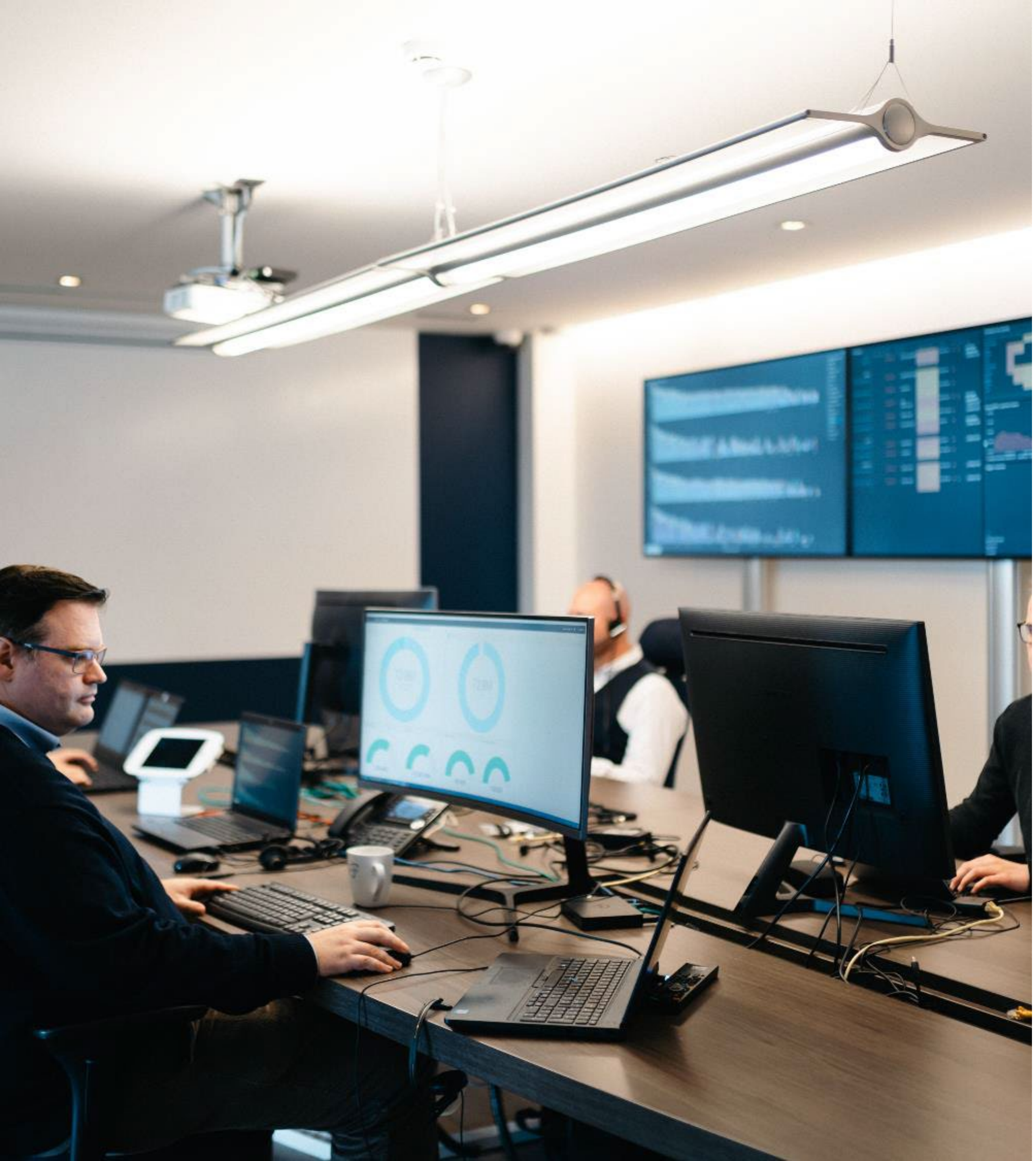
Started providers [Windows powershell]

Details [Windows powershell]

16257 documents

Columns 1 field sorted

@timestamp	event.code	powershell.engine.version	powershell.runspace_id	process.args	powershell.command.invocation_details	powershell.file.script_block_text
May 5, 2022 @ 12:01:28.136	4104	-	-	-		function __cmdletization_BindCommonParameters { param($__cmdletization_objectModelWrapper, $myPSBoundParameters) if ($myPSBoundParameters.ContainsKey('CimSession')) {...
May 5, 2022 @ 12:01:27.952	4104	-	-	-		#requires -version 3.0 try { Microsoft.PowerShell.Core\Set-StrictMode -Off } catch { } $script:MyModule = $MyInvocation.MyCommand.ScriptBlock.Module $script:ClassName = 'Root/Microsoft/Windows/TaskScheduler/PS_ClusteredScheduledTask'...
May 5, 2022 @ 12:01:27.952	4104	-	-	-		ctModelWrapper $PSBoundParameters $__cmdletization_objectModelWrapper.BeginProcessing() } catch { $__cmdletization_exceptionHasBeenThrown = $true throw } } Process { try { if (-not...
May 5, 2022 @ 12:01:27.952	4104	-	-	-		[object]$__cmdletization_defaultValueIsPresent = $false if



ULTIMATE

Managed EDR on Servers

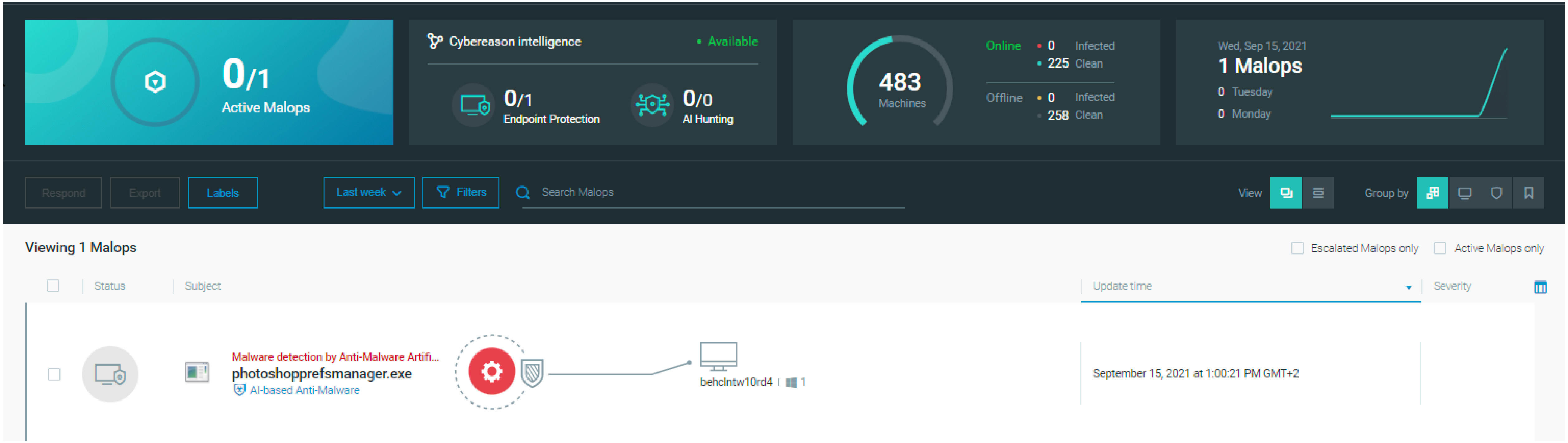
- Detect suspicious activity on your network
- EDR in monitoring mode

SIGHT

ULTIMATE

- **Weekly Vulnerability Scanning**
- **Account Takeover Fraud Prevention and Monitoring**
- **Active Managed Threat hunting**
- **Managed EDR on Servers**

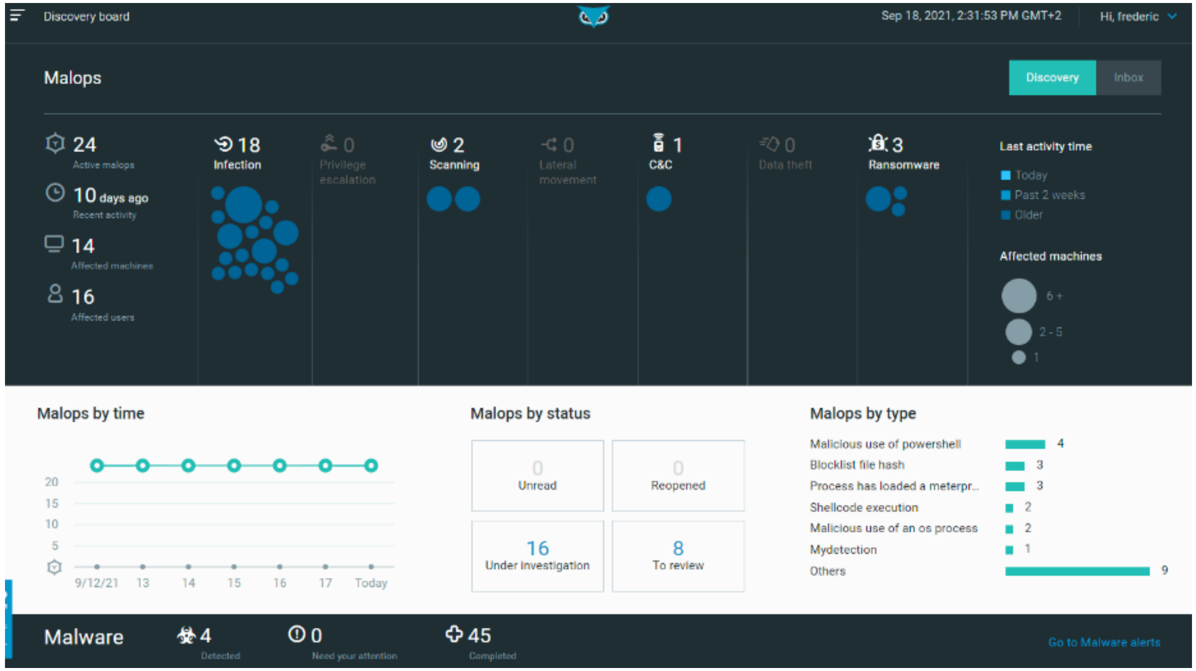
Secutec
Cyber security intelligence



Viewing 1 Malops

□ Escalated Malops only □ Active Malops only

□	Status	Subject		Update time	Severity
□		Malware detection by Anti-Malware Artifi... photoshopprefsmanager.exe AI-based Anti-Malware	behclntw10rd4 | 1	September 15, 2021 at 1:00:21 PM GMT+2	

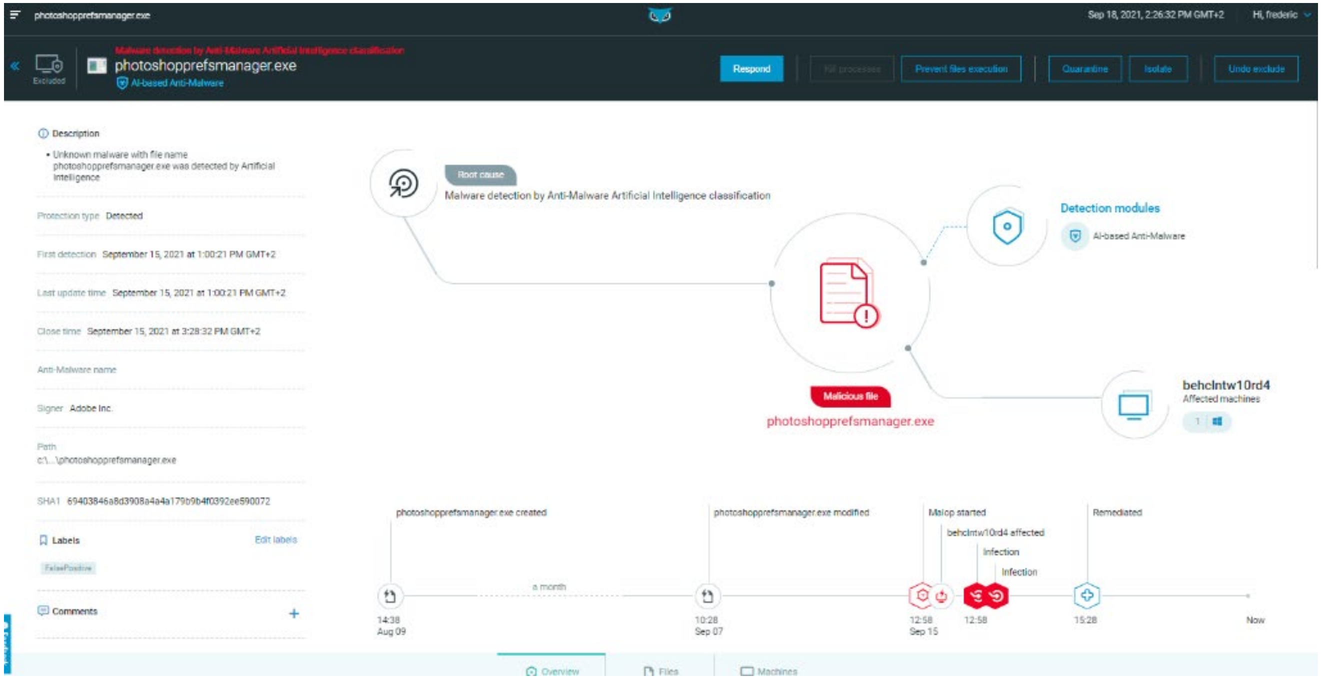


Malops by status

0 Unread	0 Reopened
16 Under investigation	8 To review

Malops by type

Malicious use of powershell	4
Blocklist file hash	3
Process has loaded a meterpr...	3
Shellcode execution	2
Malicious use of an os process	2
Mydetection	1
Others	9


photoshopprefsmanager.exe
Sep 18, 2021, 2:26:32 PM GMT+2
Hi, frederic
Excluded
Malware detection by Anti-Malware Artificial Intelligence classification
photoshopprefsmanager.exe
AI-based Anti-Malware
Respond
Kill processes
Prevent files execution
Quarantine
Isolate
Undo exclude

Description

- Unknown malware with file name photoshopprefsmanager.exe was detected by Artificial Intelligence

Protection type Detected

First detection September 15, 2021 at 1:00:21 PM GMT+2

Last update time September 15, 2021 at 1:00:21 PM GMT+2

Close time September 15, 2021 at 3:28:32 PM GMT+2

Anti-Malware name

Signer Adobe Inc.

Path
c:\...\photoshopprefsmanager.exe

SHA1 69403846a8d3908a4a4a179b9b4f0392ee590072

Labels Edit labels

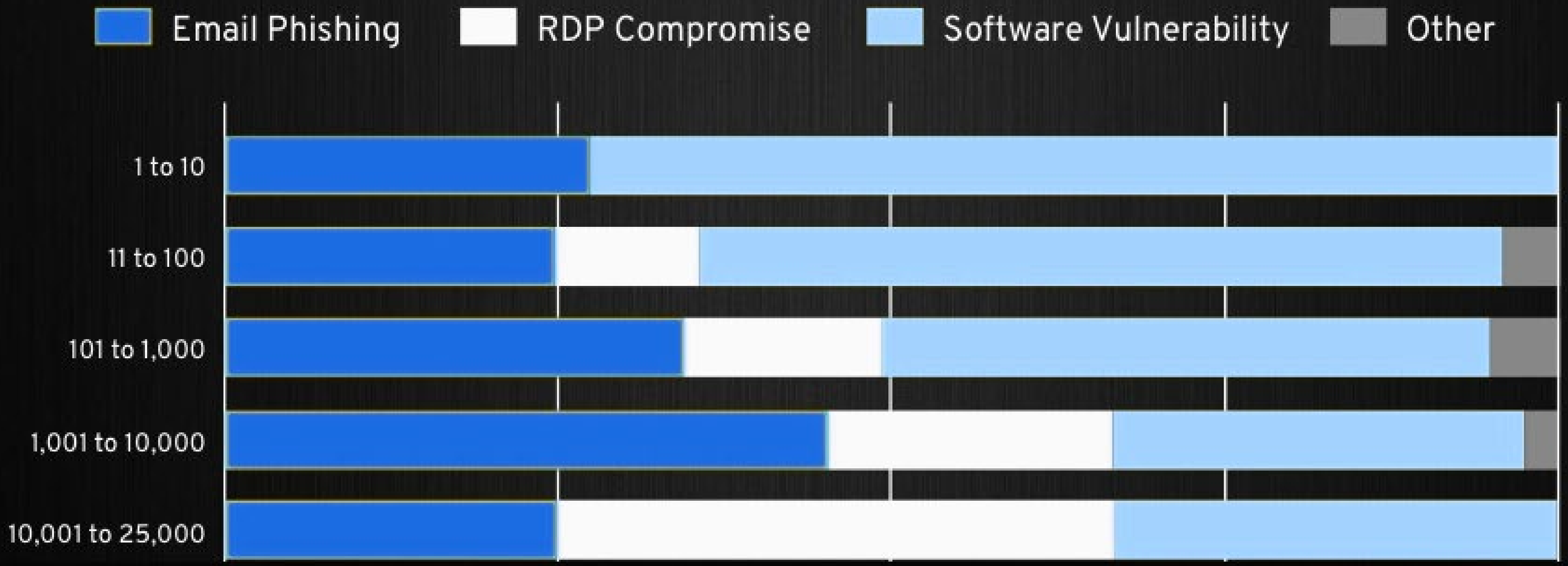
FalsePositive

Comments +

Secutec negotiation services

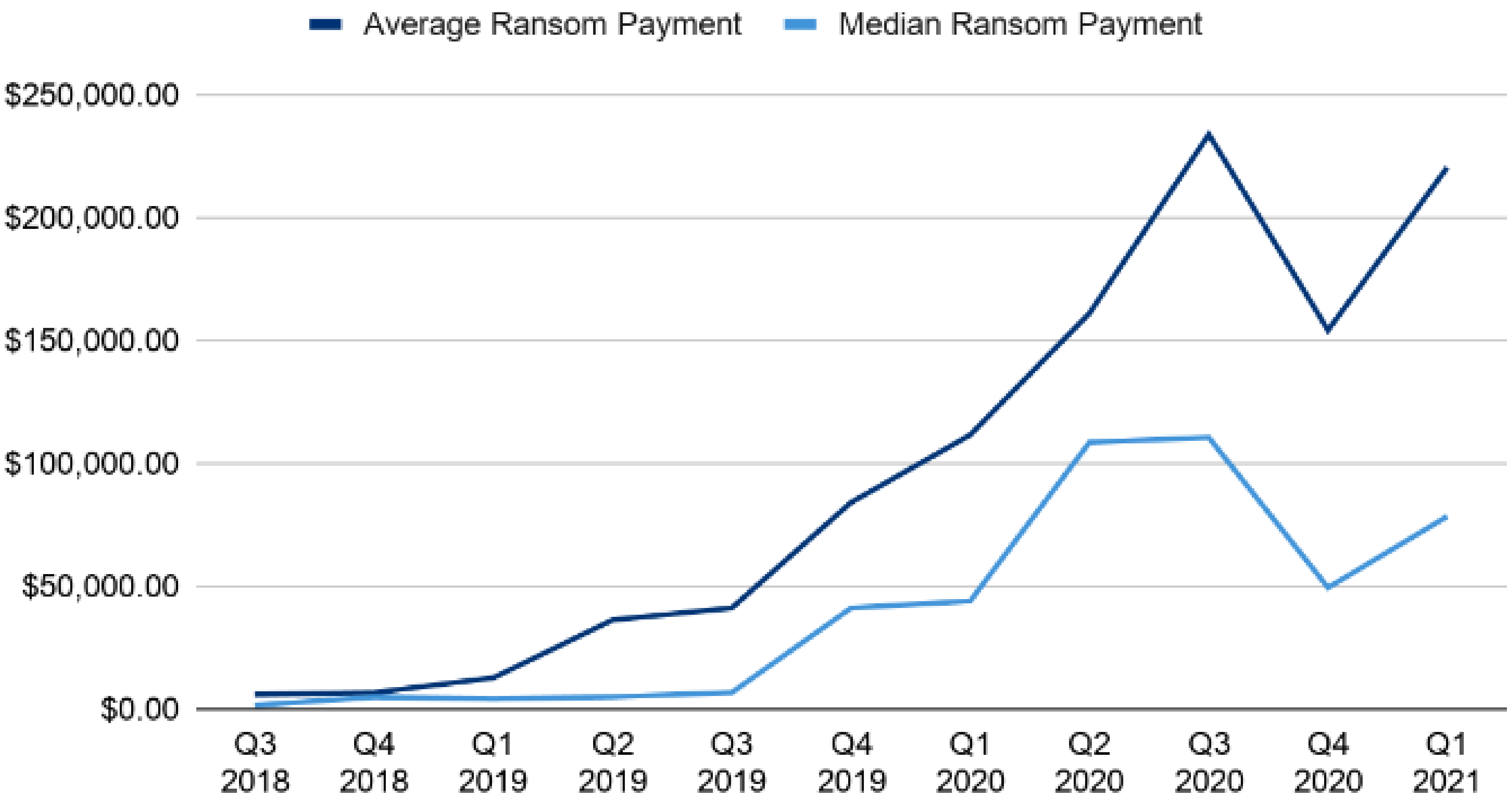
Secutec
Cyber security intelligence

ATTACK VECTOR BY COMPANY SIZE



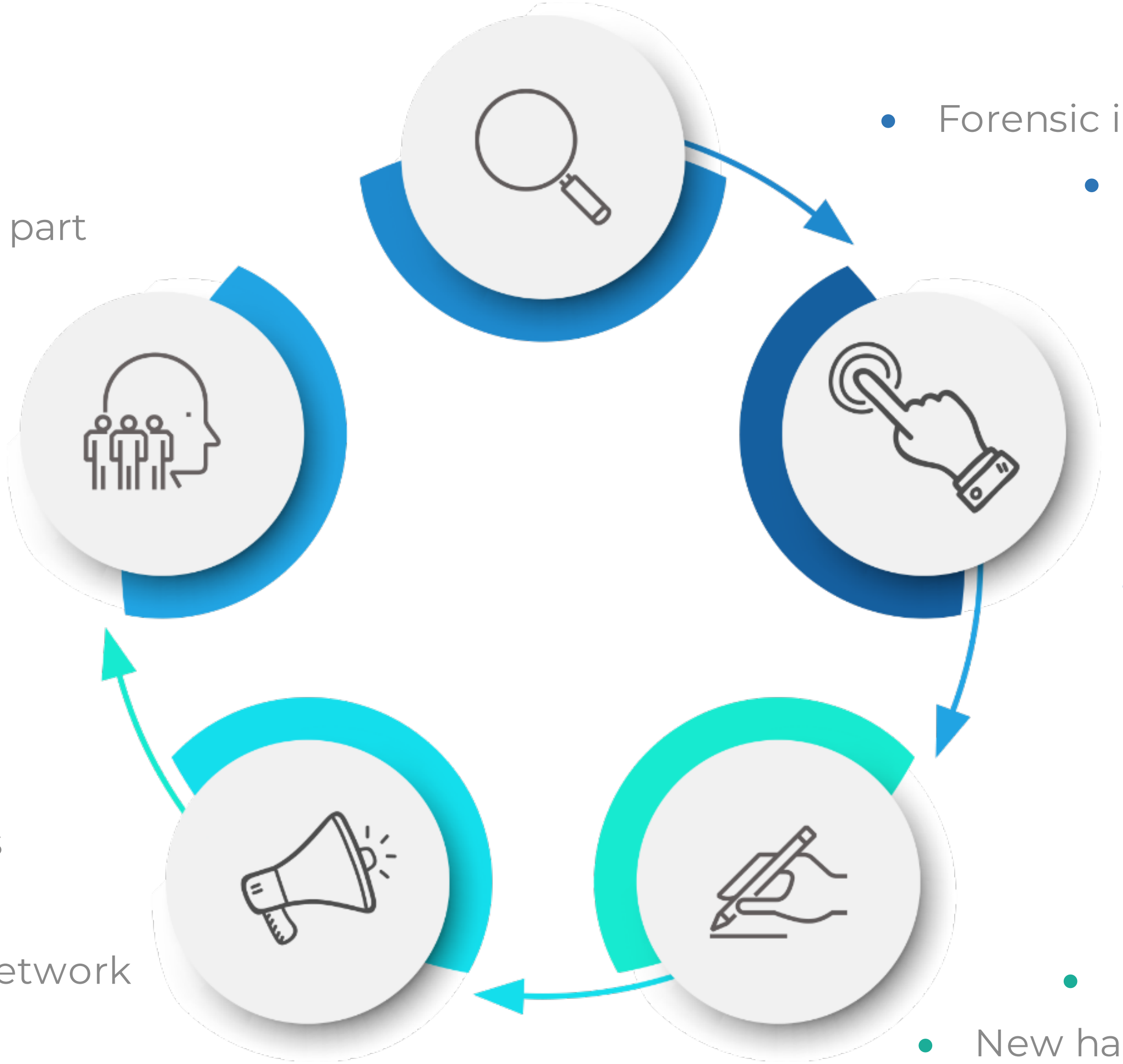
Attack Vector by Company Size Q1 2021 COVEWARE

Ransom Payments By Quarter



DIE RESULTER

When Ransomware hits your company



- First 48 hours
- Identify devices
- Forensic investigation (onsite)
- Info on the Darknet

- Start negotiation
- Monitoring network
- Prioritize critical devices

- Clear strategy
- Methodology of recovery
- New hardware onsite in 24h/ 48h

- PR and communications
- Inform authorities
- 1 month to rebuild the network

- Never forget the human part
- Best teambuilding!

Secure SIGHT

Questions?

Interested in a demo for your Company? sales@secutec.be

Contact us

Secutec
Cyber security intelligence

Secutec

Cyber security intelligence