



# Assume Breach

Achieve Resilience

Marko Haarala  
Security Lead Finland & Baltic's



# The “Assume Breach” problem



# Maturity curve of Cyber Security Professional



I can prevent the bad things



# Maturity curve of Cyber Security Professional



I can detect the bad things

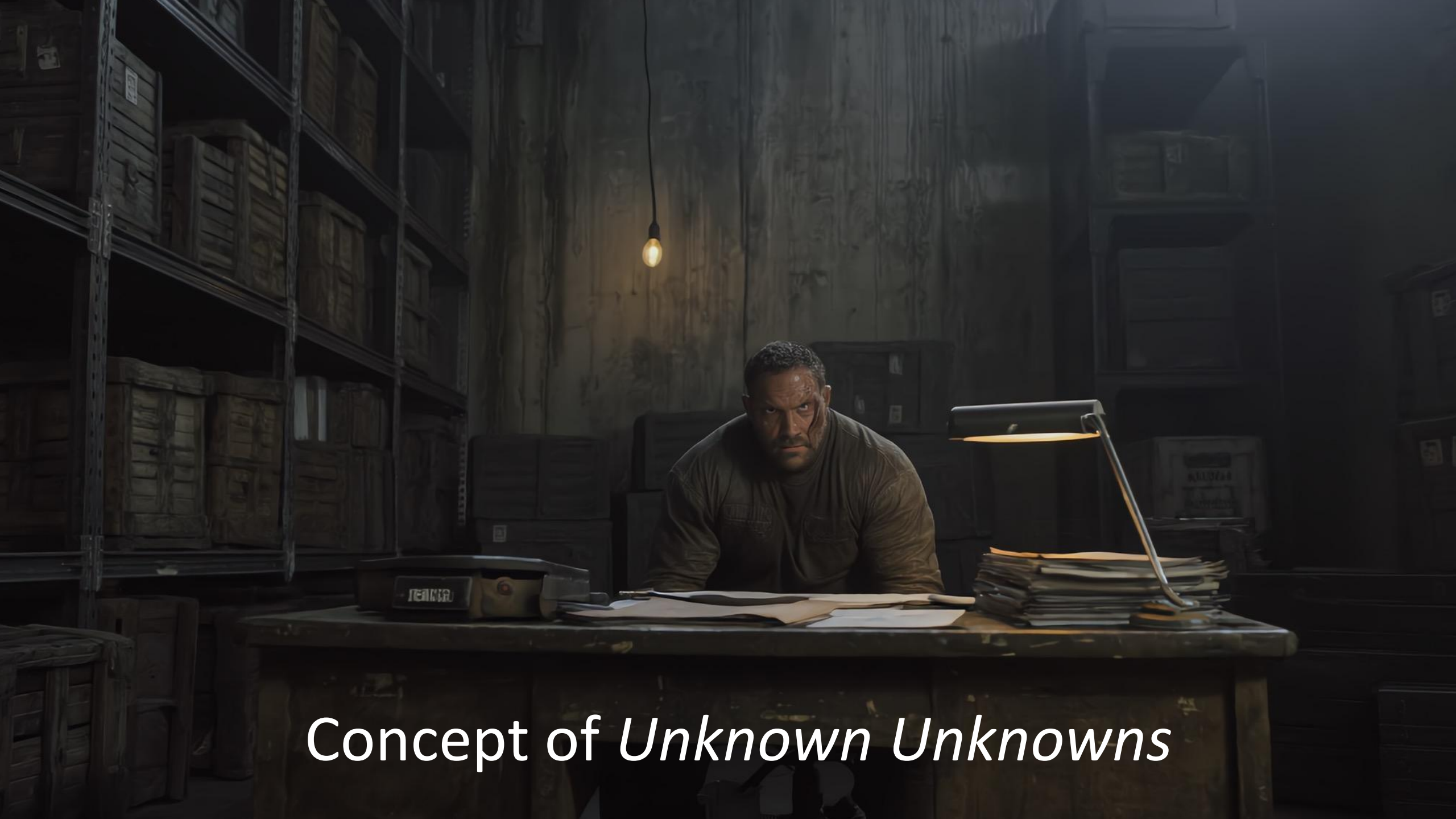
# Maturity curve of Cyber Security Professional



I cannot even see or understand  
the bad things







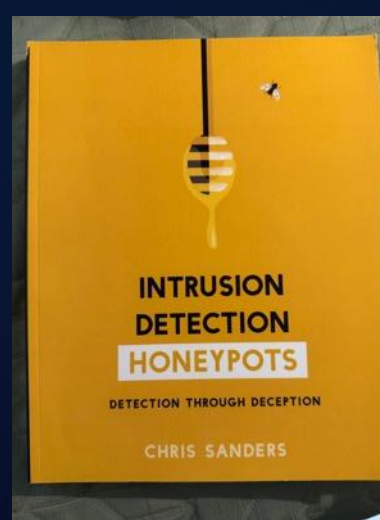
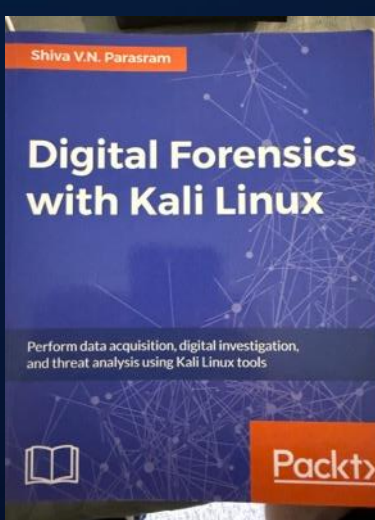
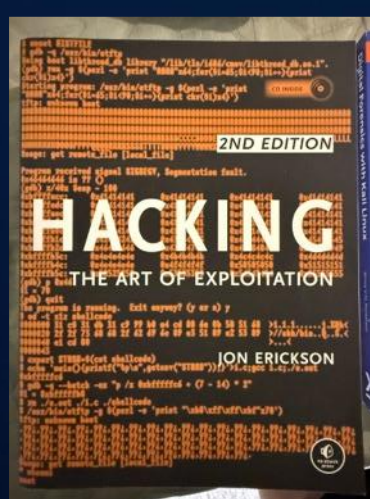
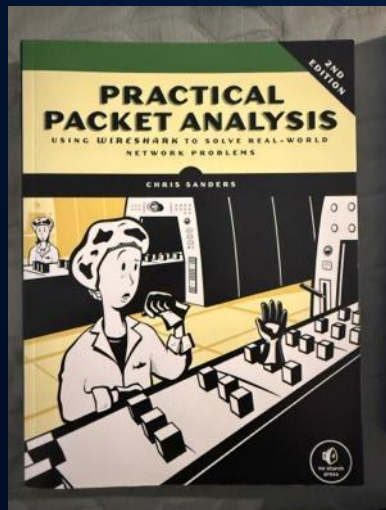
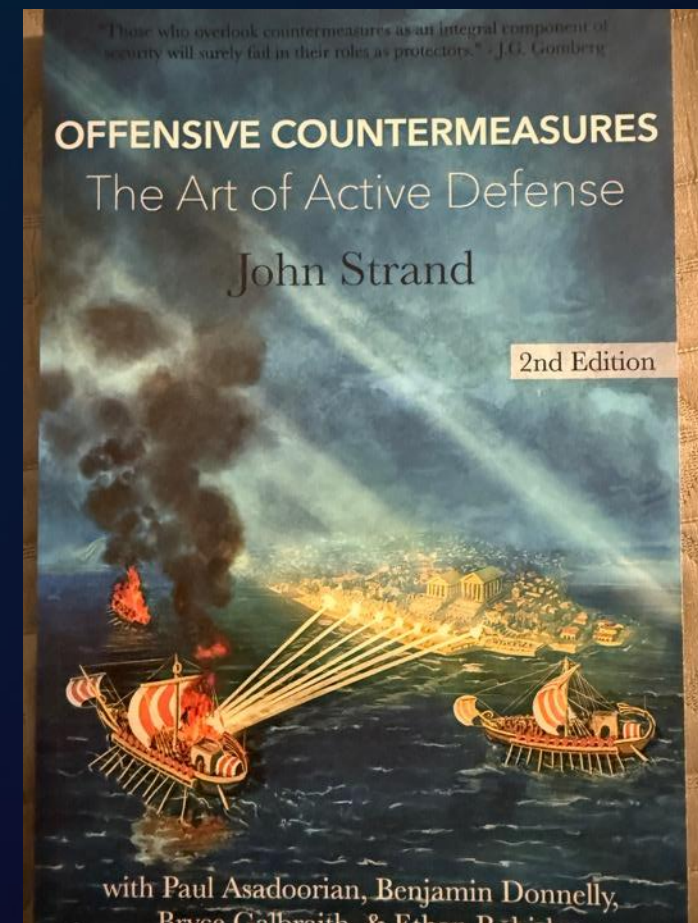
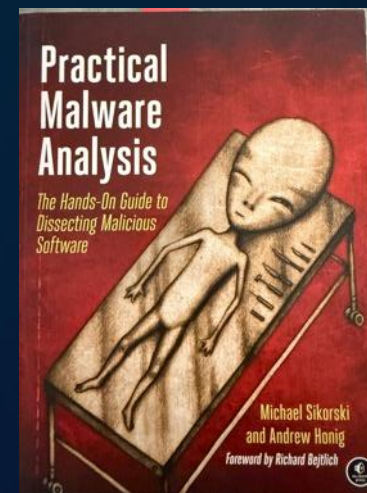
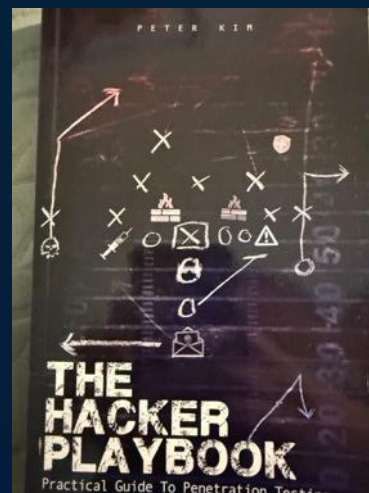
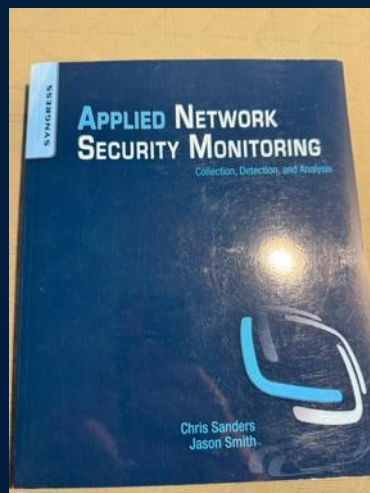
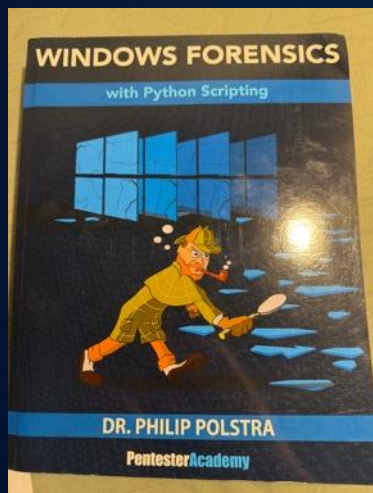
Concept of *Unknown Unknowns*



How can you find the *Unknown Unknowns*?



# Education is free and you'll need it!



# Steps towards continuous forensic OSQuery



Investigate ⓘ

Query Script

Devices ⓘ

Filters

Catalog query

⚠️ (Deprecated) Forensic Snapshot Windows 0.0.5

⚠️ (Deprecated) Forensic Snapshot Windows 0.0.6

🖥️ Direct Logons for Service/Computer Accounts Monitoring

🖥️ Domain Information Modification Monitoring

👤 Forensic Snapshot Linux 0.0.9

🍏 Forensic Snapshot MacOS 0.0.8

🖥️ Forensic Snapshot Windows 0.0.9

🖥️ Information Search on Central Processing Unit

🖥️ 👤 🍏 Inventory System Information

🖥️ 👤 🍏 Kernel Information Monitoring

SHA256 Hash Of Running Processes

Process Running Without A Binary On Disk

PowerShell History

Listening Ports

Processes

1 ▾

2

```
SELECT pid, name AS process_name, path AS process_path
FROM processes;
```



# In practice – get the tools you need

BMF-ENGINE in group Video Production 2.0

✓ Definitions Up To Date 94

Hostname	BMF-ENGINE	Group	Video Production 2.0
Operating System	Windows 11, SP 0.0 (Build 26100.6584)	Policy	Video Production 2.0
Connector Version	8.5.0.30551 <a href="#">Show download URL</a>	Internal IP	10.10.11.88
Install Date	2025-04-04 10:18:44 EEST	External IP	176.93.253.104
Connector GUID	23b06ebd-ed7c-451b-bfce-04c25b6dd582	Last Seen	2025-09-30 09:41:22 EEST
Processor ID	BFEBFBFF000B0671	BP Signature Version	113012
BP Signature Last Updated	2025-09-30 09:36:09 EEST	Definition Version	TETRA 64 bit (daily version: 95521)
Definitions Last Updated	2025-09-30 09:34:10 EEST	Update Server	tetra-defs.eu.amp.cisco.com
Host Firewall Status	Not Enabled	Host Firewall Configuration	None
Cisco Secure Client ID	N/A	Cisco Security Risk Score	94 (Updated : 2025-09-29 11:06:11 EEST)

✓ Take Forensic Snapshot View Snapshot Investigate in Orbital

Events Device Trajectory Diagnostics View changes

Scan... Diagnose... Move to Group... Uninstall Connector Delete

# What the box is running

AMP Forensic Snapshot — null 2025-09-30 09:44:22 EEST

Autoexec Items

MITRE | ATT&CK

1,068

Bitlocker Encryption Monit...

2

DNS Cache Table Monitori...

57

Installed Programs On Win...

282

Listening Ports

MITRE | ATT&CK

26

Loaded Modules Hashes

MITRE | ATT&CK

2,031

Loaded Modules Processes

MITRE | ATT&CK

183

Loaded Modules vs. Proce...

MITRE | ATT&CK

9,463

Logon Sessions

MITRE | ATT&CK

10

Mapped Drives

MITRE | ATT&CK

2

Network Connections - Pr...

MITRE | ATT&CK

23

Network Interfaces

4

Network Profiles Registry ...

15

OS Version

9

Powershell History

MITRE | ATT&CK

500

Prefetch Directory

MITRE | ATT&CK

502

Autoexec Items

Tactics

< 1 of 11 >

1 – 100 of 1,068 records

Search

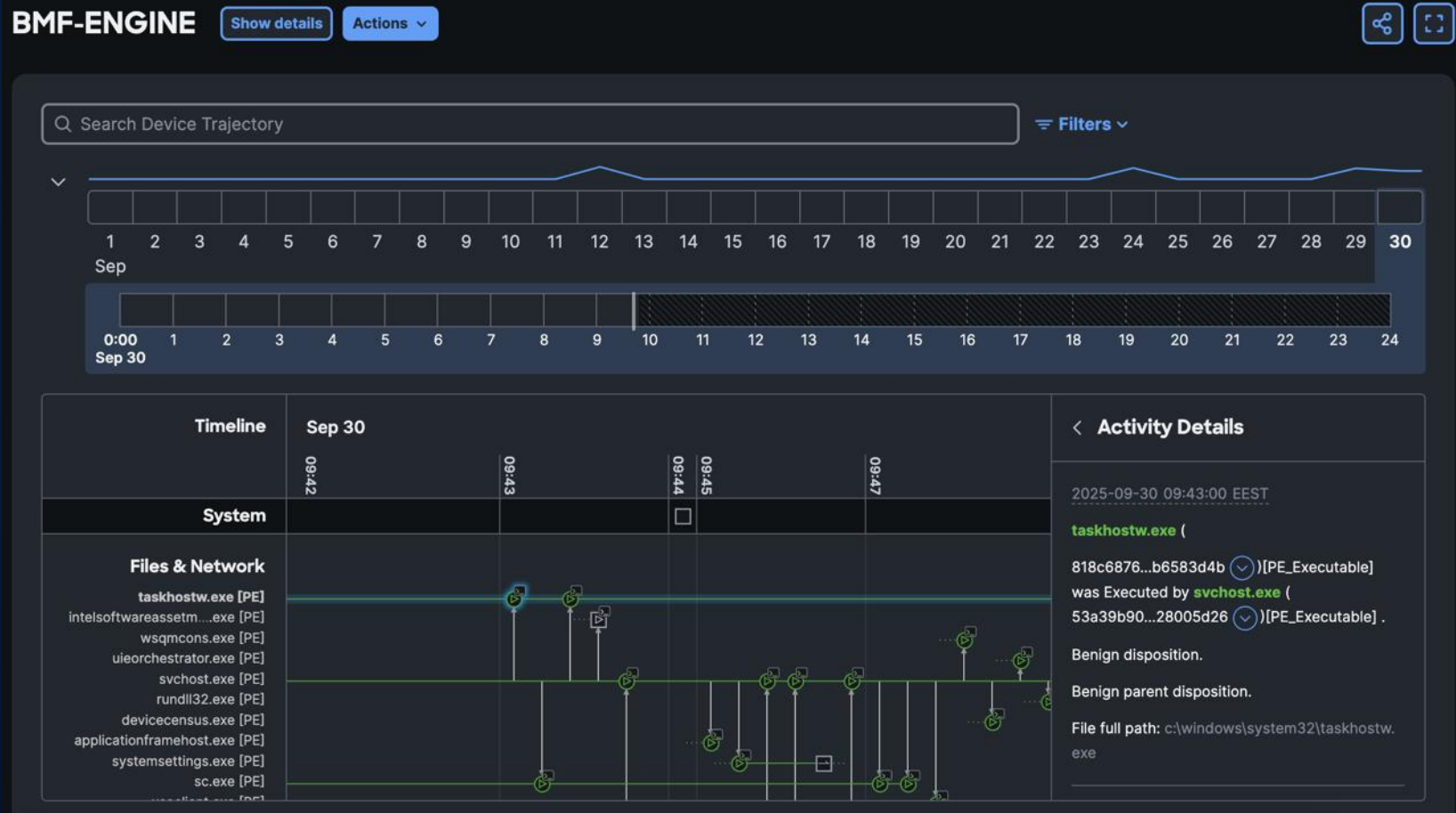
NAME	PATH	SOURCE	SHA256
Local Print Queue		drivers	
Generic software device		drivers	
Microsoft IPP Class Driver		drivers	
WSD Print Device	C:\WINDOWS\system32\driverstore\filerepository\wsdprint.inf_amd64_1f9e32519098c0b6\wsdprint.sys	drivers	92d9de16...aef84c5d
Computer Device		drivers	
Audio Endpoint		drivers	
VSX Systemwide	C:\WINDOWS\system32\driverstore\filerepository\vsx.inf_amd64_42061a793289195f\vsx.sys	drivers	53267d92...d3670070
teVirtualMIDI - Virtual MIDI Driver x64	C:\WINDOWS\system32\drivers\tevirtualmidi64.sys	drivers	9d8b3193...901c7063
Remote Desktop Device Redirection Port	C:\WINDOWS\system32\drivers\rdpdr.sys	drivers	d75c46a8...0366694e

Device Trajectory

Export to CSV



# Know your systems!



# Tear it apart





# Foundation for the search of the Unknown Unknowns

## Layered structure for efficiency and cost saving

### XDR

Tightly integrated and open defense layer  
Cisco Managed 24/7 Threat Hunting  
Cisco 24/7 Incident Response



# Foundation for the search of the Unknown Unknowns

## Layered structure for efficiency and cost saving

### XDR

Tightly integrated and open defense layer  
Cisco Managed 24/7 Threat Hunting  
Cisco 24/7 Incident Response

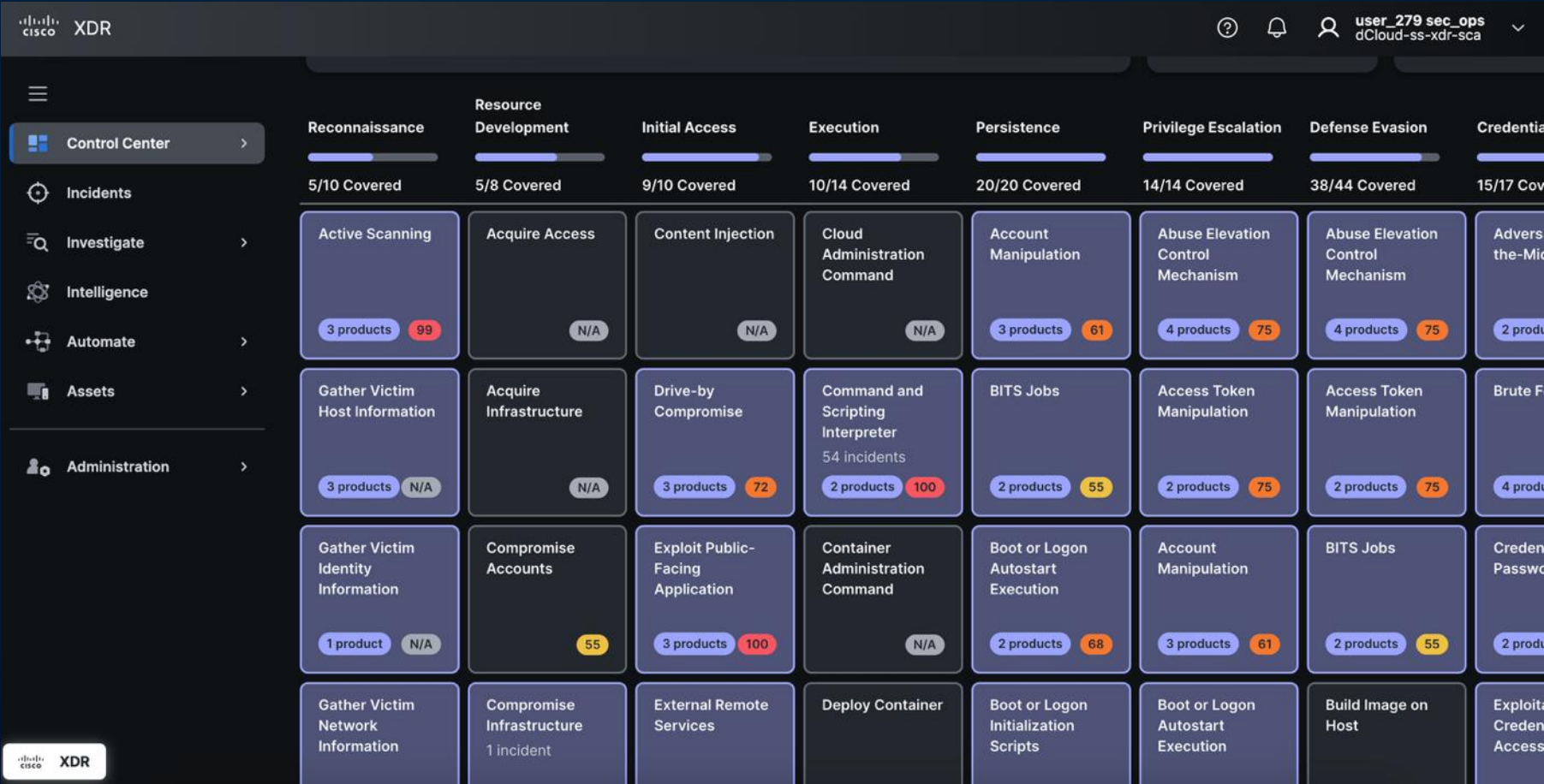


### Resilience platform

3<sup>rd</sup> party raw data  
3<sup>rd</sup> party alerts  
Application logs etc.



# Look at the environment like bad guys are looking





# 1. Let the technology handle the easy stuff

The screenshot displays the Cisco XDR Incidents dashboard. The left sidebar contains navigation links for Control Center, Incidents (selected), Investigate, Intelligence, Automate, Assets, and Administration. The main area shows a list of incidents with columns for Priority, Name, Sources, and Create time. A filter is applied, showing 30 results. The right sidebar provides details for the selected incident, including its priority (1000), status (Open: Investigating), reported by (Cisco XDR Analytics), and assigned user (us). It also includes a priority score breakdown and a summary of the incident.

**Incidents**

72 Incidents | 1 New Incident | 58 Open Incidents

Search: [ ] Last 30 days [v] Hide closed incidents [x] Filters 30 results

1 Applied Filter

Priority	Name	Sources	Create
1000	Suspicious Endpoint Findings by Execution on <a href="#">rwkst1-rtp-402.dev.pseudoco.com</a>	Cisco XDR Analytics (org-10a40...	2025-23T15:01Z
1000	Suspicious Endpoint Findings by Execution on <a href="#">rwkst1-lon-365.dev.pseudoco.com</a>	Cisco XDR Analytics (org-10a40...	2025-18T14:79Z
1000	Suspicious Endpoint Findings by Execution on <a href="#">rwkst1-lon-407.dev.pseudoco.com</a>	Cisco XDR Analytics (org-10a40...	2025-18T11:54Z
1000	Suspicious Endpoint Findings by Execution on <a href="#">rwkst1-lon-33.dev.pseudoco.com</a>	Cisco XDR Analytics (org-10a40...	2025-14T22:904Z
1000	Suspicious Endpoint Findings by Execution on <a href="#">rwkst1-sjc-333.dev.pseudoco.com</a>	Cisco XDR Analytics (org-10a40...	2025-11T20:35Z
1000	Suspicious Endpoint Findings by Execution on	Cisco XDR Analytics (org-10a40...	2025-

**Suspicious Endpoint Findings by Execution on...**

Priority: 1000 Status: Open: Investigating

Reported by: Cisco XDR Analytics (org-10a4058e-1c32-45b4-b1eb-9290df0dd847) on 2025-09-23T15:22:30.301Z

Assigned: us

MITRE: [ ]

**Priority score breakdown**

1000 | 100 Detection Risk | 10 Asset Value at Risk

**Sources**

Cisco XDR Analytics (org-10a4058e-1c32-45b4-b1...)

**Summary**

Suspicious behaviors were detected on the endpoint

View Incident Detail

# 2. Automate or let Cisco to do this for you

← Back to all Workflows

XDR - Delete Email Messages

Last Modified: 19 August 2025 at 09:11:47

Validated

View runs

Run

⚙ Settings ▾

START

Was the workflow started from a play book?

No

Logic Failed

Fetch and parse XDR automation targets

Q

+

-

Workflow Properties

XDR - Delete Email Messages

General ▾

Variables ▾

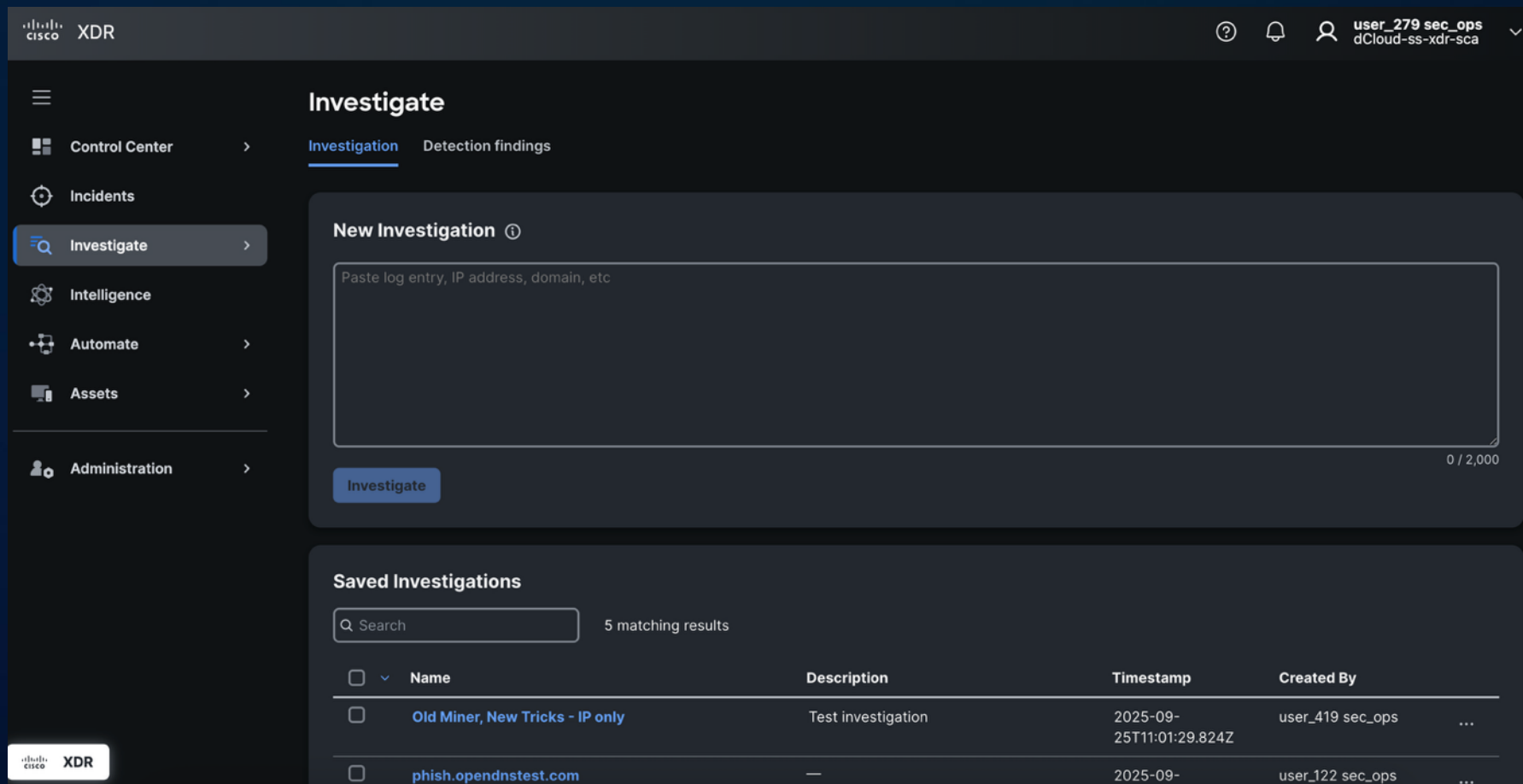
Intent Options ▾

Automation Rules ▾

Version ▾

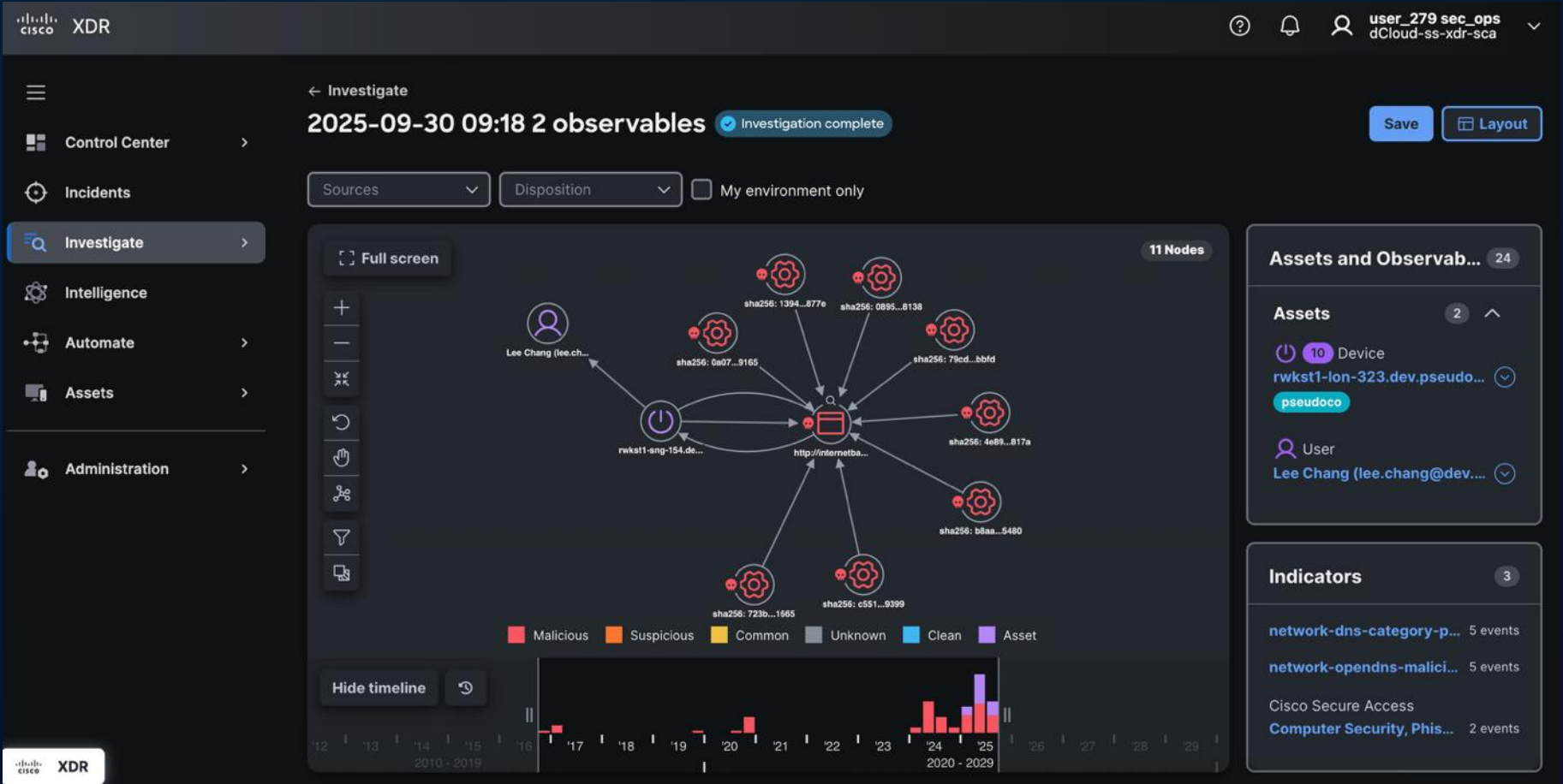
Target ▾

## F3. Hunt or let Cisco to do this for you





# 4. Focus on Unknown Unknowns



# Back to the darkroom – Back to the raw data





# Back to the darkroom – Back to the raw data

Filter Domain : Test\_Intfc\_grp Time : Last 6 hours 5 minutes  
Client or Server Host : 172.16.2.205

Table Short List

Flow Table - 4 records

Client Host	Start Active Time	Last Active Time	Server Port	Server Host	Server A
172.16.2.64	Apr 10, 2014 2:08:42 PM (2 hours 57 minutes 58s ago)	Apr 10, 2014 2:38:11 PM (2 hours 28 minutes 29s ago)	443	172.16.2.205	SSL_CN:
172.16.2.64	Apr 10, 2014 1:44:15 PM (3 hours 22 minutes 25s ago)	Apr 10, 2014 1:44:15 PM (3 hours 22 minutes 25s ago)	443	172.16.2.205	SSL_CN:
172.16.2.64	Apr 10, 2014 1:26:32 PM (3 hours 40 minutes 8s ago)	Apr 10, 2014 1:26:32 PM (3 hours 40 minutes 8s ago)	443	172.16.2.205	SSL_CN:
172.16.2.64	Apr 10, 2014 12:35:18 PM (4 hours 31 minutes 22s ago)	Apr 10, 2014 12:38:24 PM (4 hours 28 minutes 16s ago)	443	172.16.2.205	SSL_CN:

Server Application Details	Client Packets	Client Bytes	Server Packets	Server Bytes	Client Ratio (%)	Duration
SSL_CN: lcbase-01.	263,424	17.66M	220,026	343.84M	4.82% <input type="text"/>	29 minutes 29s
SSL_CN: lcbase-01.	13	917	11	7.86k	4.77% <input type="text"/>	< 1s
SSL_CN: lcbase-01.	13	917	11	7.86k	4.77% <input type="text"/>	< 1s
SSL_CN: lcbase-01.	18,520	1.24M	15,438	24.72M	4.79% <input type="text"/>	3 minutes 6s

# Breach Protection Suite enhances resiliency

AI Driven

Telemetry Rich

Platform Powered



Cisco XDR



Secure Network  
Analytics



Talos Incident  
Response



Secure Email  
Threat Defense



Secure Endpoint



Cisco Managed  
Services



# Cisco Breach Protection Suite Composition

