Assume Breach

Achieve Resilience

Marko Haarala
Security Lead Finland & Baltic's

The “Assume Breach” problem

Maturity curve of Cyber Security Professional

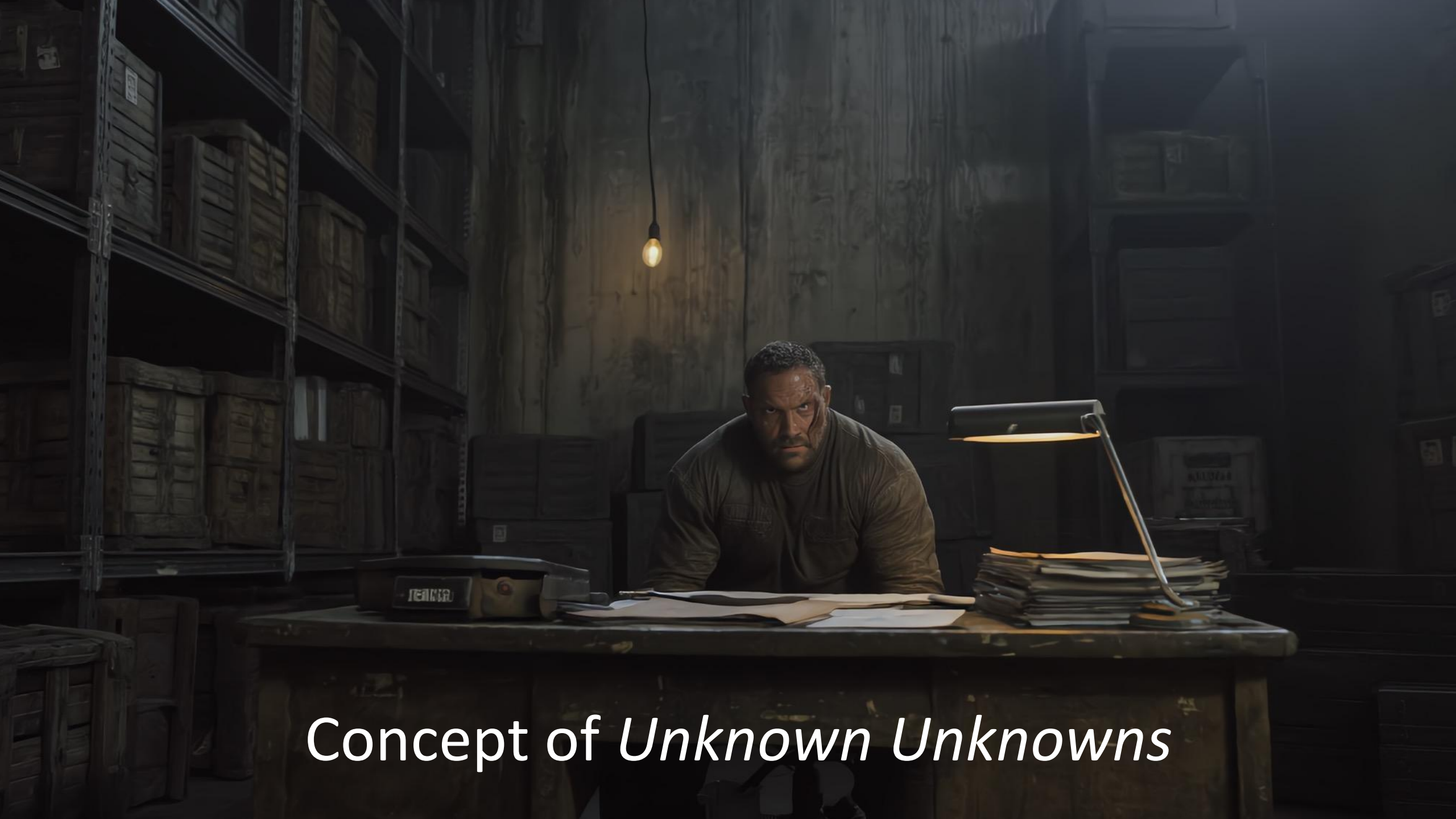
I can prevent the bad things

Maturity curve of Cyber Security Professional

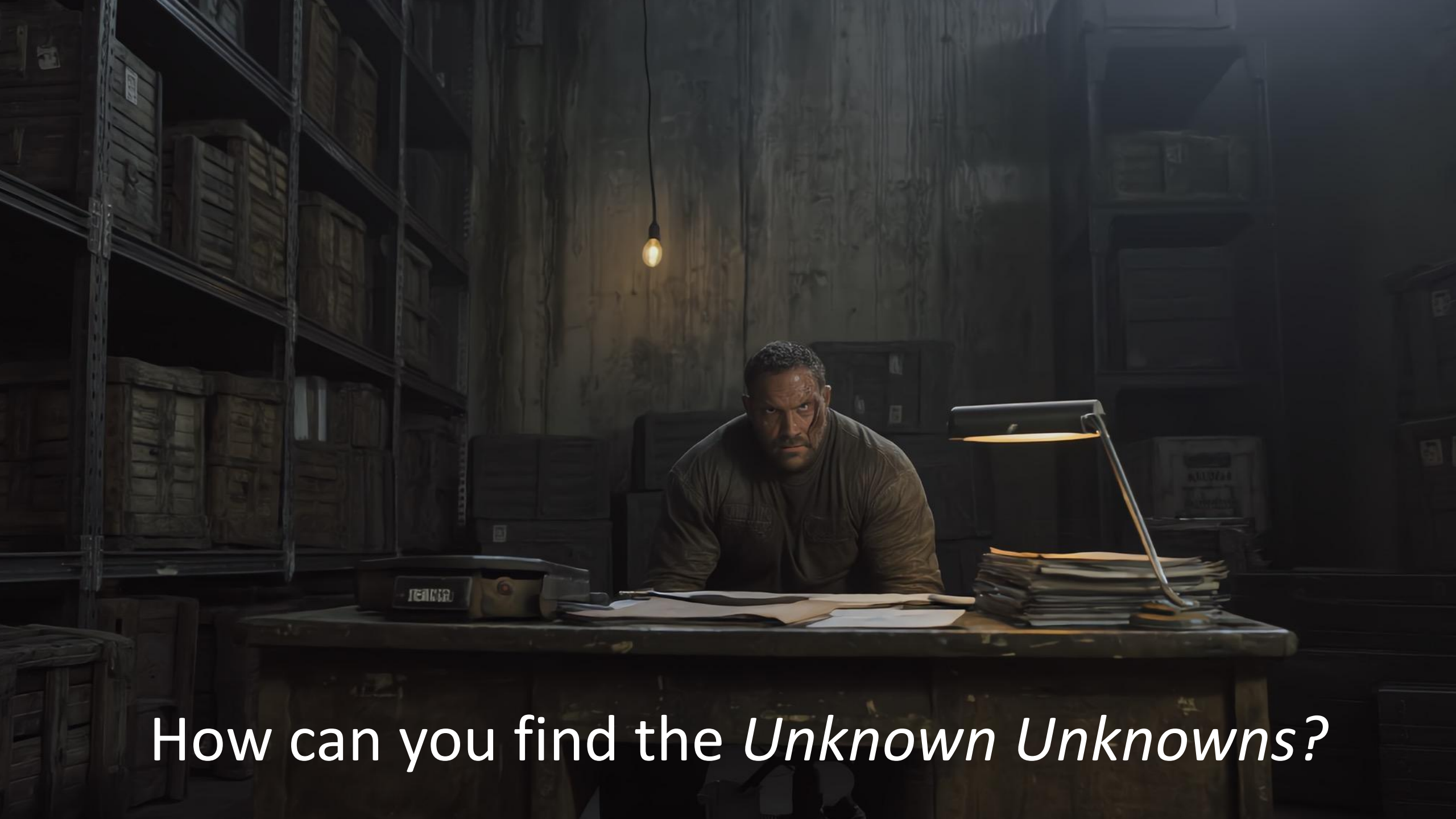
I can detect the bad things

Maturity curve of Cyber Security Professional

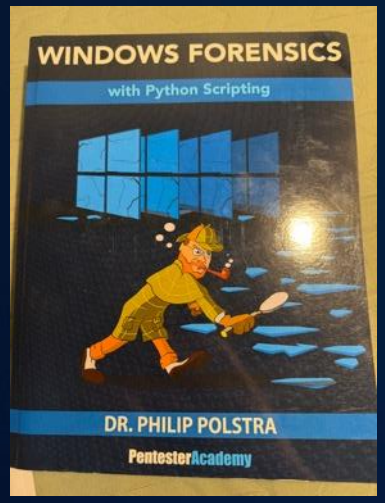
I cannot even see or understand the bad things

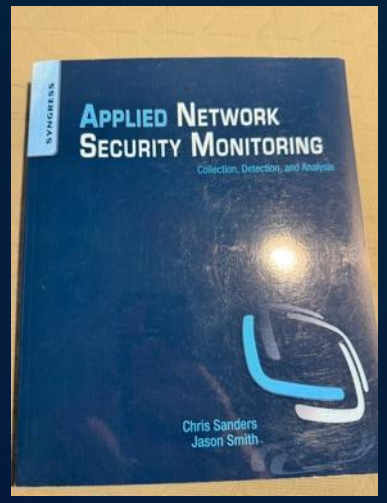


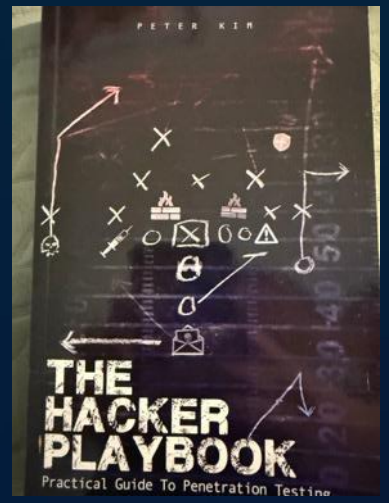
Concept of *Unknown Unknowns*

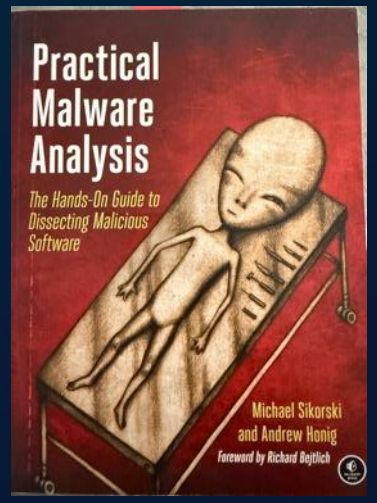

How can you find the *Unknown Unknowns?*

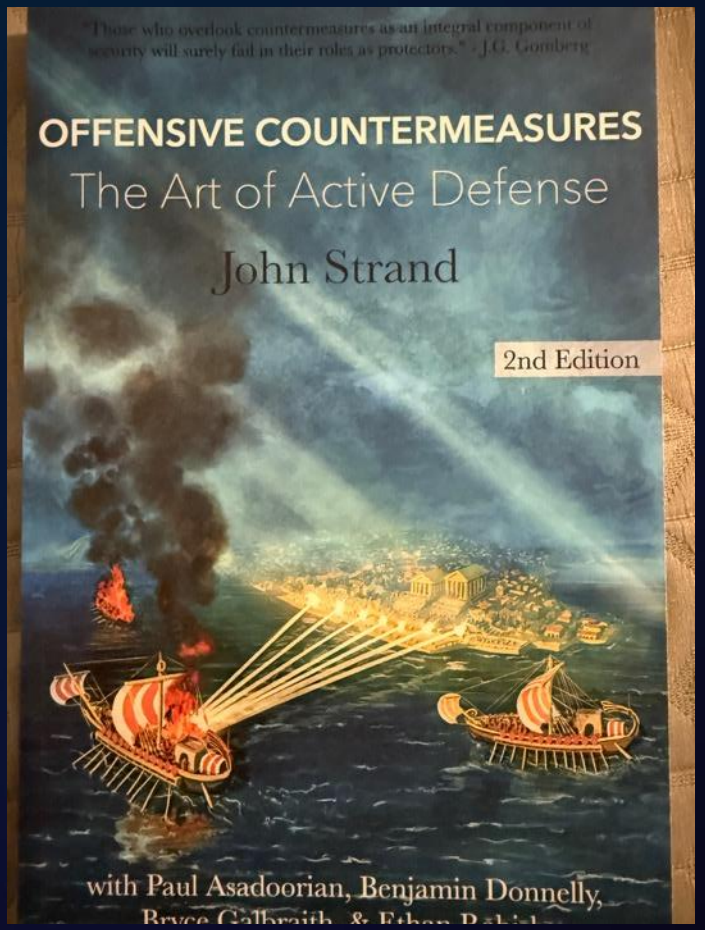
Education is free and you'll need it!

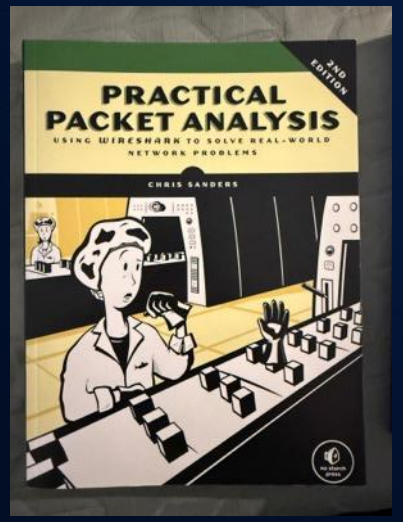


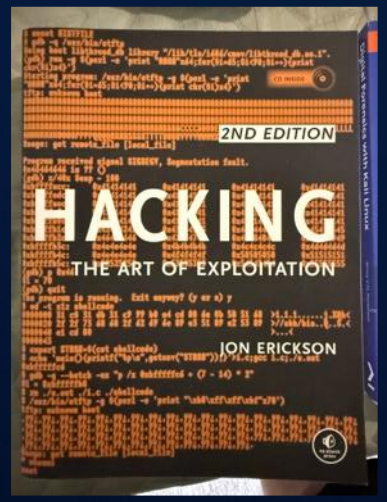


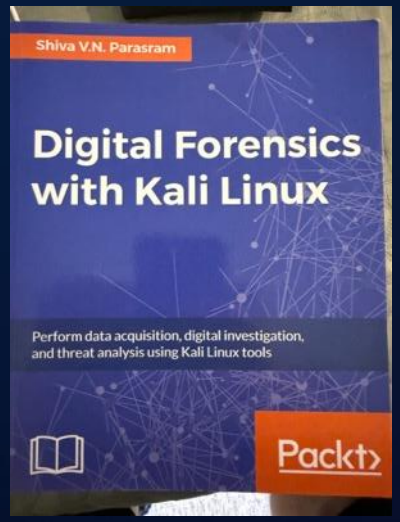


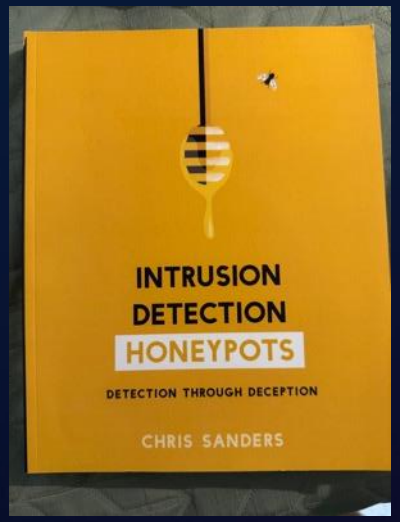












Steps towards continuous forensic OSQuery

Investigate

Query | Script

Devices

Filters

Catalog query

for

- (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

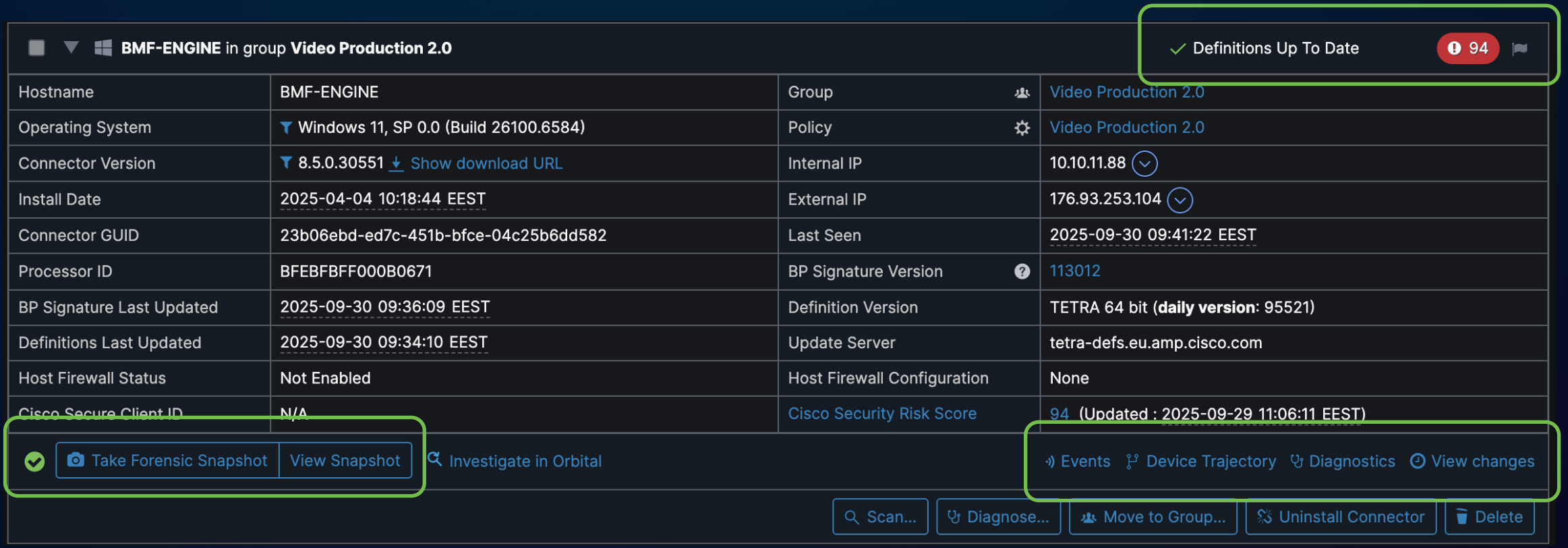
PowerShell History

Listening Ports

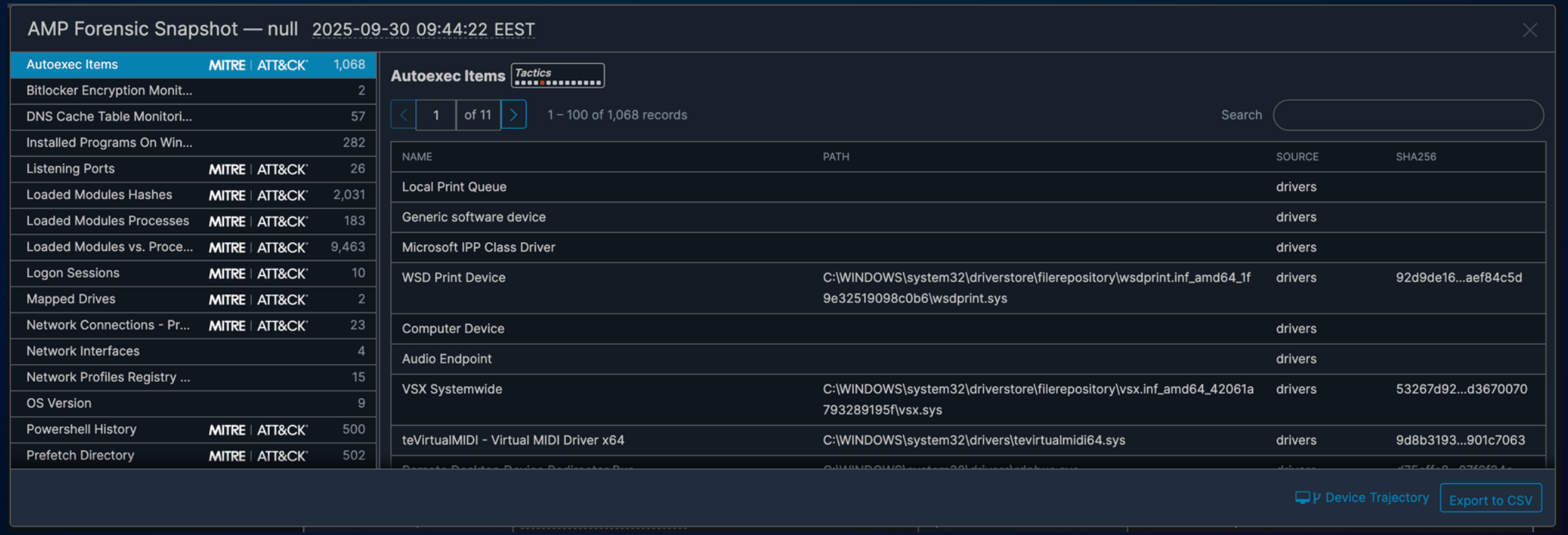
Processes

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

In practice – get the tools you need



What the box is running



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

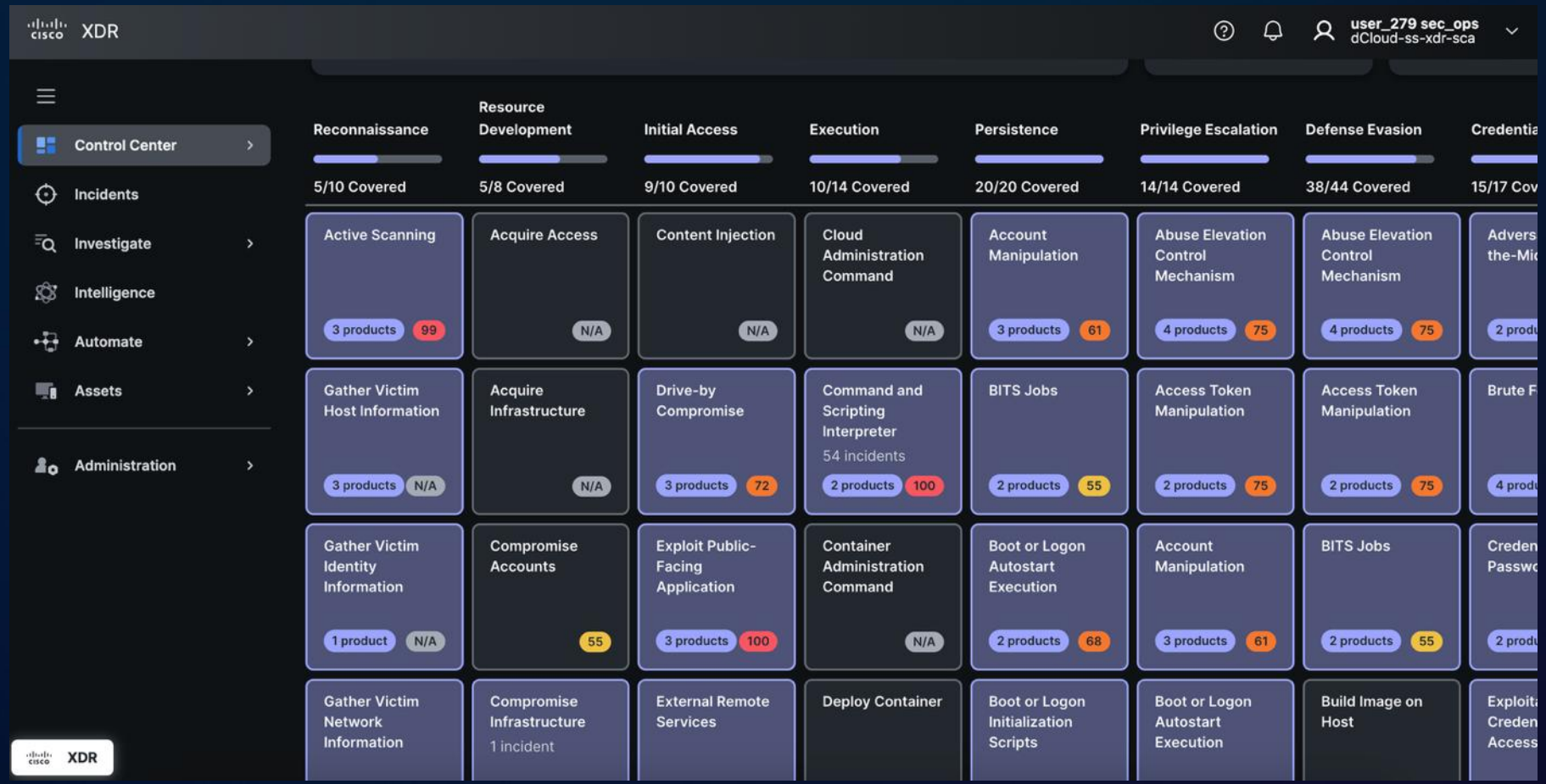
Tightly integrated and open defense layer
Cisco Managed 24/7 Threat Hunting
Cisco 24/7 Incident Response

+

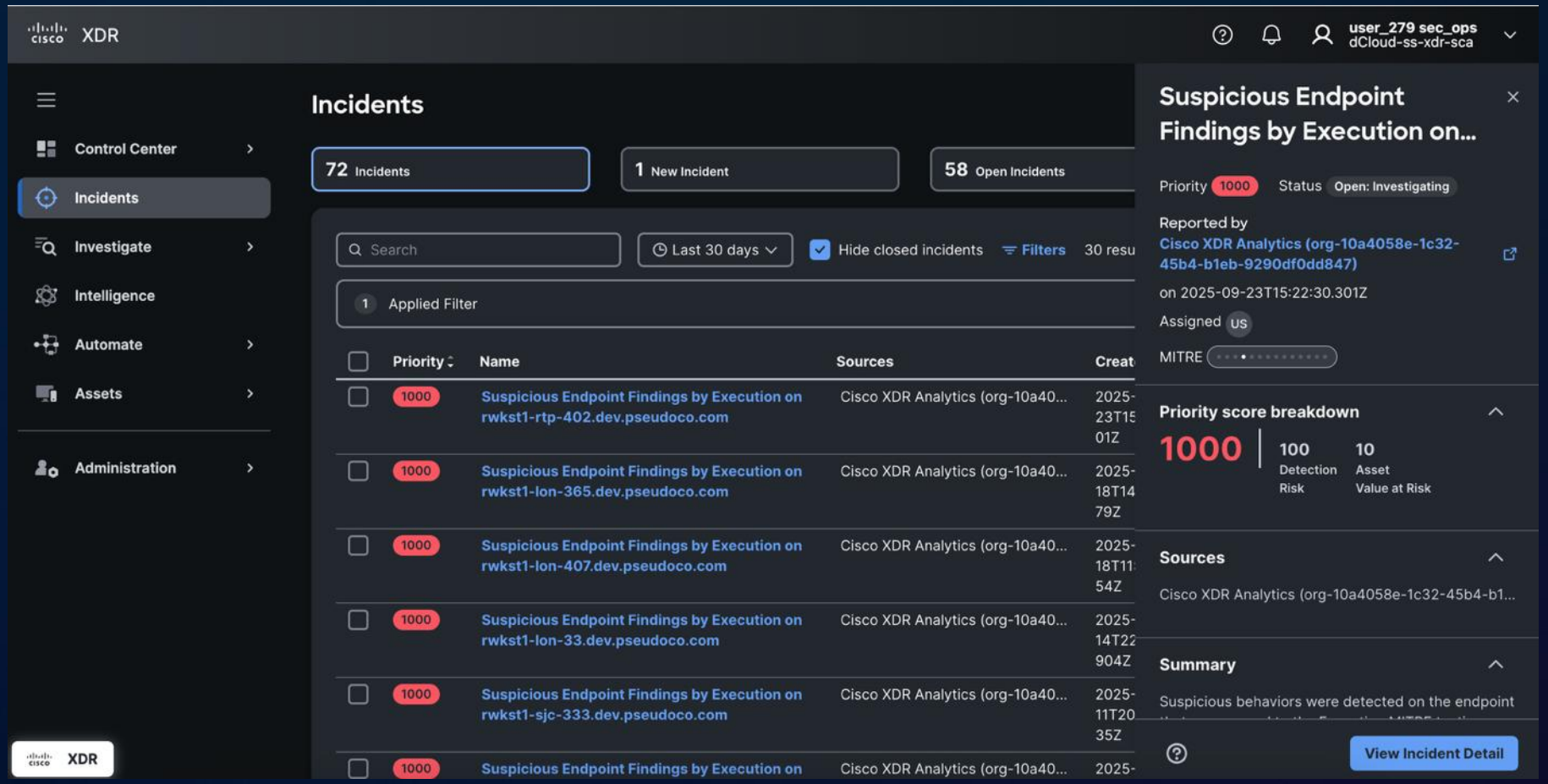
Resilience platform

3rd party raw data
3rd party alerts
Application logs etc.

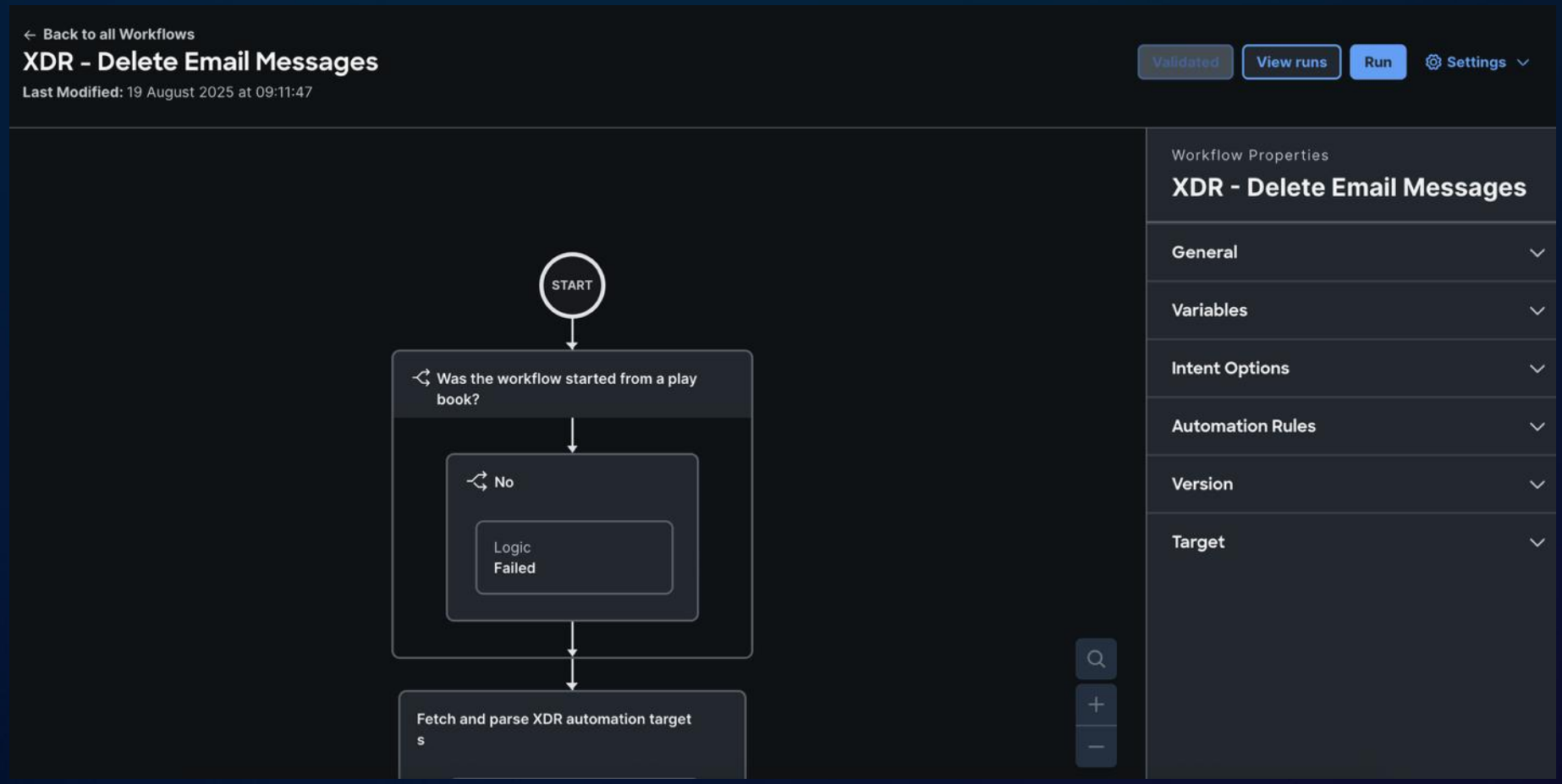
Look at the environment like bad guys are looking



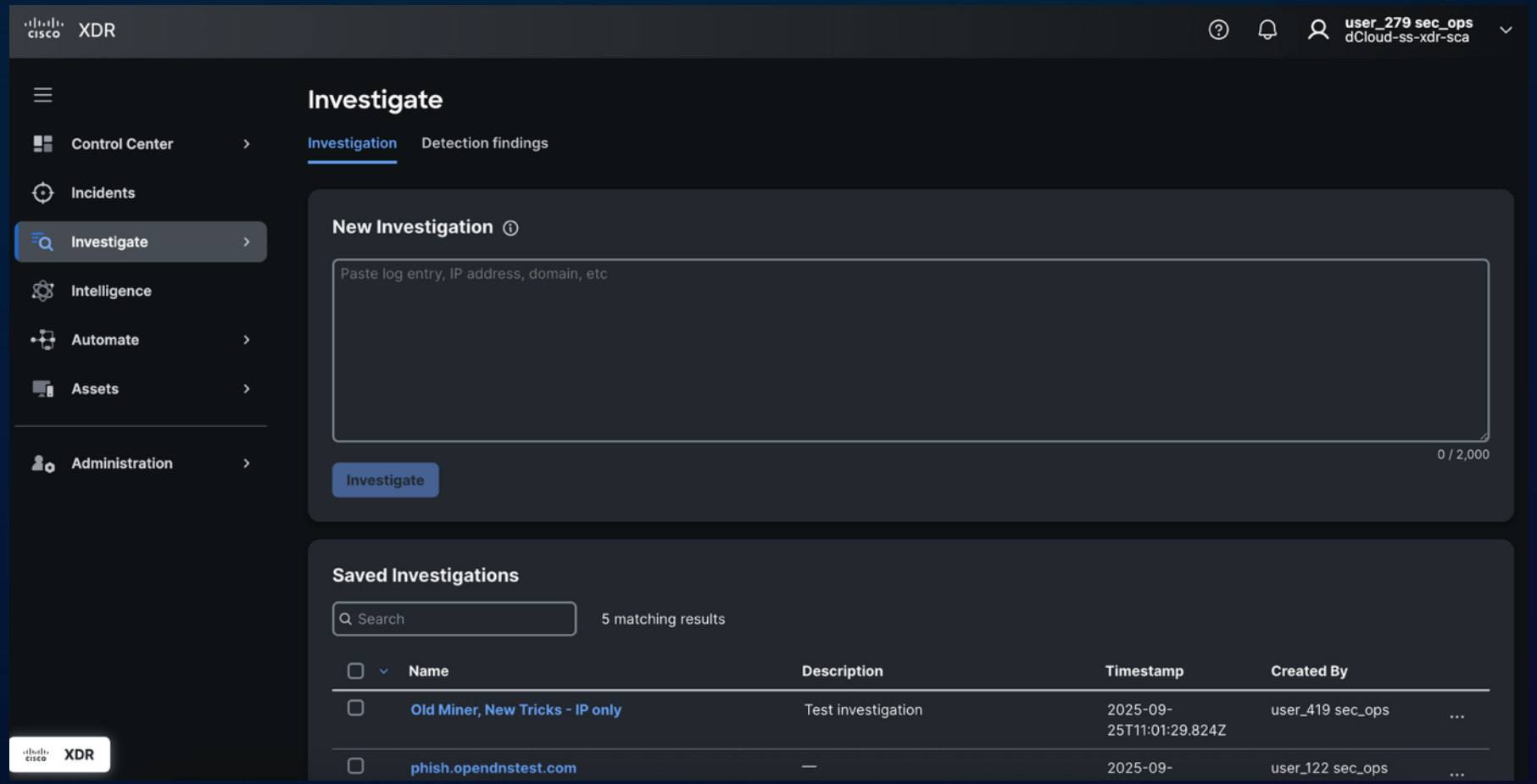
1. Let the technology handle the easy stuff



2. Automate or let Cisco to do this for you



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_grps 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 ▼1	Last Active Time ▲2	Server Port ▼3	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	34[illegible].84M	4.82%	29 minutes 29s
SSL_CN: lcbase-01.	13	917	11	[illegible]7.86k	4.77%	< 1s
SSL_CN: lcbase-01.	13	917	11	[illegible]7.86k	4.77%	< 1s
SSL_CN: lcbase-01.	18,520	1.24M	15,438	2[illegible].72M	4.79%	3 minutes 6s

Breach Protection Suite enhances resiliency

- AI Driven
- Telemetry Rich
- Platform Powered

Cisco Breach Protection Suite Composition

Essentials

- Cisco XDR Essentials
- Secure Email Threat Defense
- Secure Endpoint Advantage
- Software Support Enhanced

Advantage

Everything in Essentials **Plus**

- Cisco XDR Advantage
- Secure Endpoint Premier
- Secure Network Analytics
- Cisco Telemetry Broker

Premier

Everything in Advantage Plus

- Cisco XDR Premier (Managed XDR)
- Cisco Talos Incident Response
- Cisco Technical Security Assessments

Platform

Cisco 24/7 Threat Hunting

Full 24/7 MXDR & IR

DIY ⟷ Hybrid ⟷ Outsource


CISCO