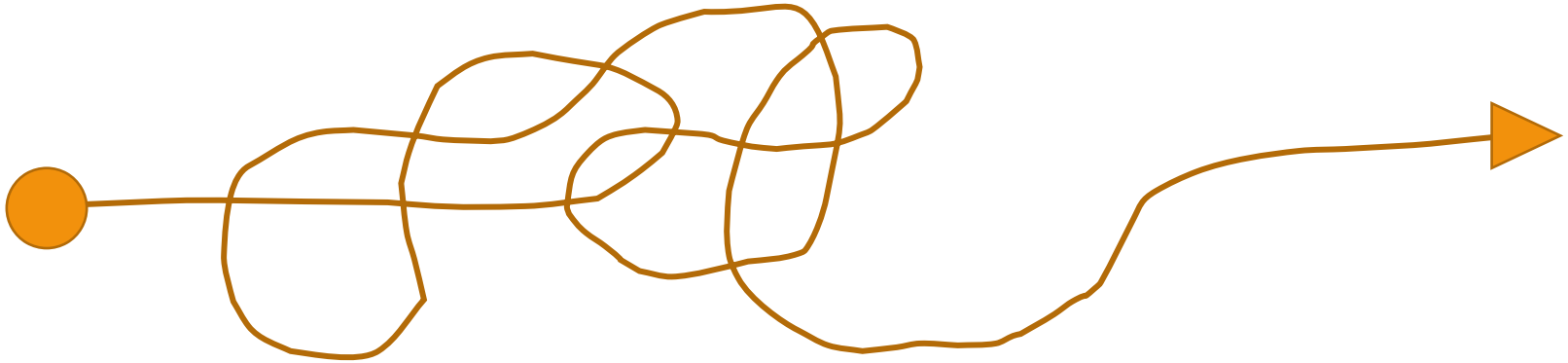
Emerging Threats – Turning from the hunter to the hunted

baseVISION
SECURE & MODERN ENDPOINT MANAGEMENT



Effective and Simple

About me...

baseVISION
SECURE & MODERN ENDPOINT MANAGEMENT

EC-Council CEH CERTIFIED

Microsoft 365 CERTIFIED SECURITY ADMINISTRATOR ASSOCIATE

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

Microsoft CERTIFIED IDENTITY AND ACCESS ADMINISTRATOR ASSOCIATE

Microsoft CERTIFIED SECURITY OPERATIONS ANALYST ASSOCIATE

Christoph Düggeli

Security Analyst, baseVISION AG

MAS Information System Management

IPMA Level D

ITILv3

Contact Me

Mail: christoph.dueggeli@basevision.ch

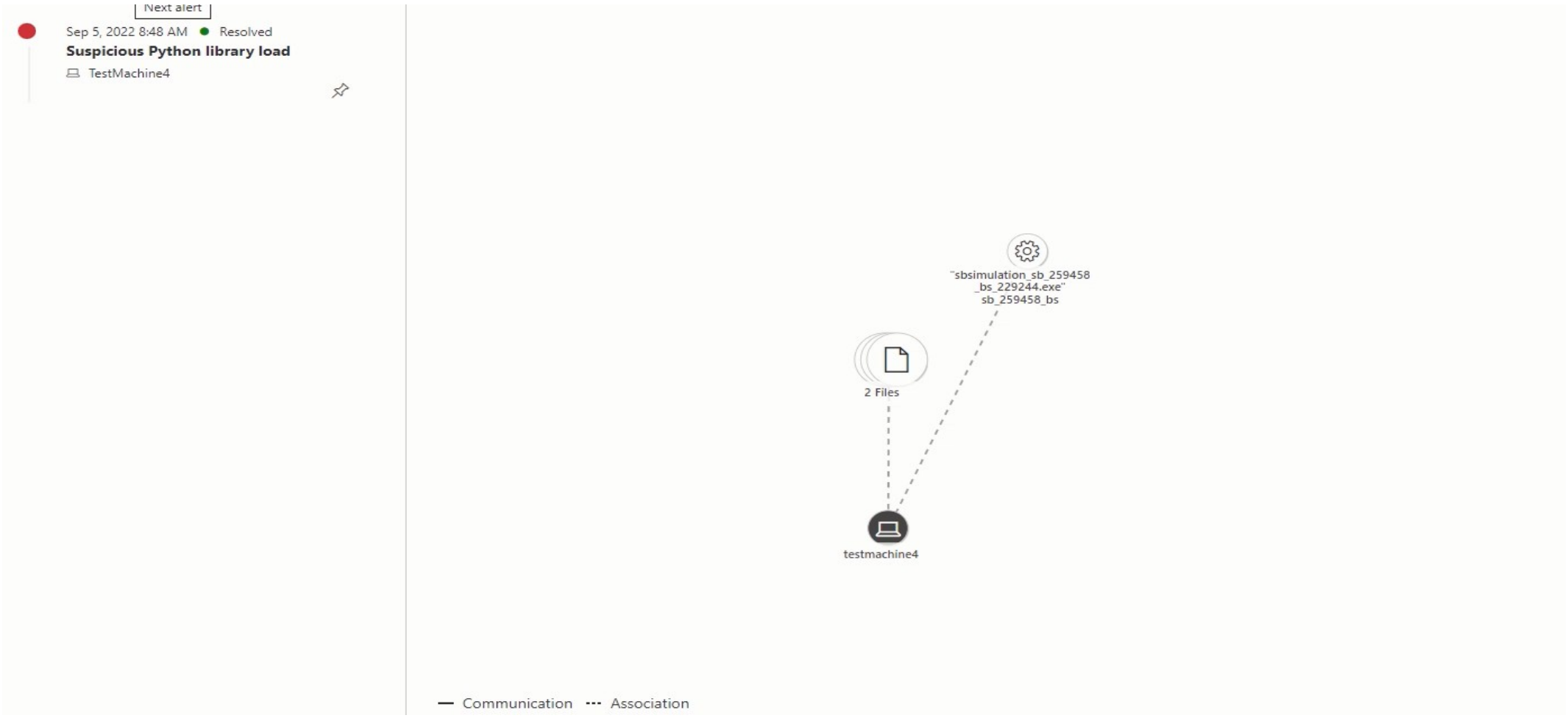
Phone: +41 622 91 30 00

Content

- Leftovers – when it’s too late
- Is it over already?
- Table’s turning – from the hunted to the hunter

Leftovers – when it’s too late

Crime scene


Next alert
Sep 5, 2022 8:48 AM
Resolved
Suspicious Python library load
TestMachine4
"sbsimulation_sb_259458
_bs_229244.exe"
sb_259458_bs
2 Files
testmachine4
Communication
Association

Post Breach investigations – Thesis confirmation

During an Incident
- Active attack remediation
- Prioritization of critical operations

Before an Incident
- Business impact limitation
- Prevent attacks at earliest possible stage
- Hygiene
- Advanced Hunting

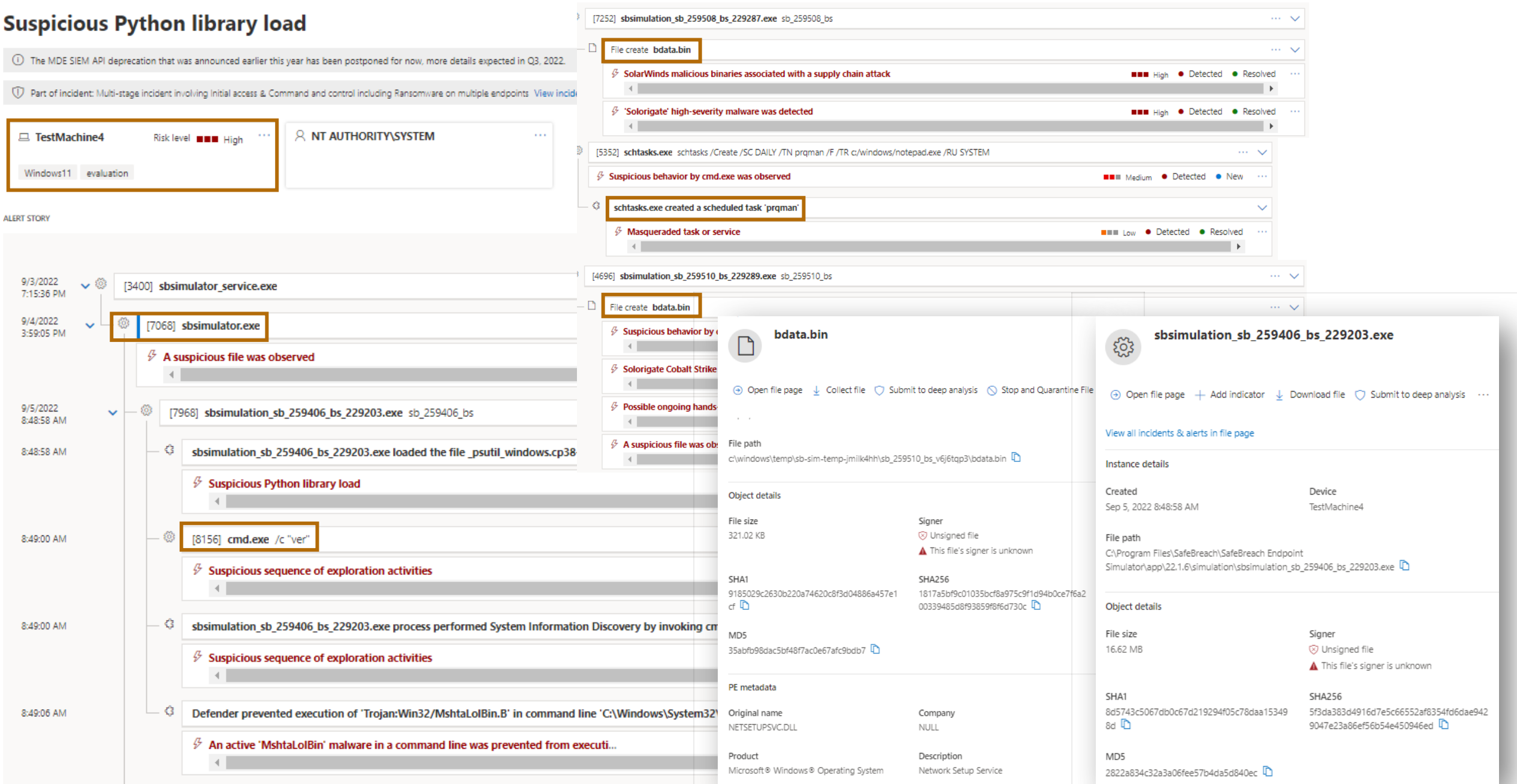
After an Incident
- Full business operations restoration
- Detection

Feedback loop
- Lessons learned, change integration

Visualization based on:
Design security for a resiliency strategy - Training | Microsoft Learn

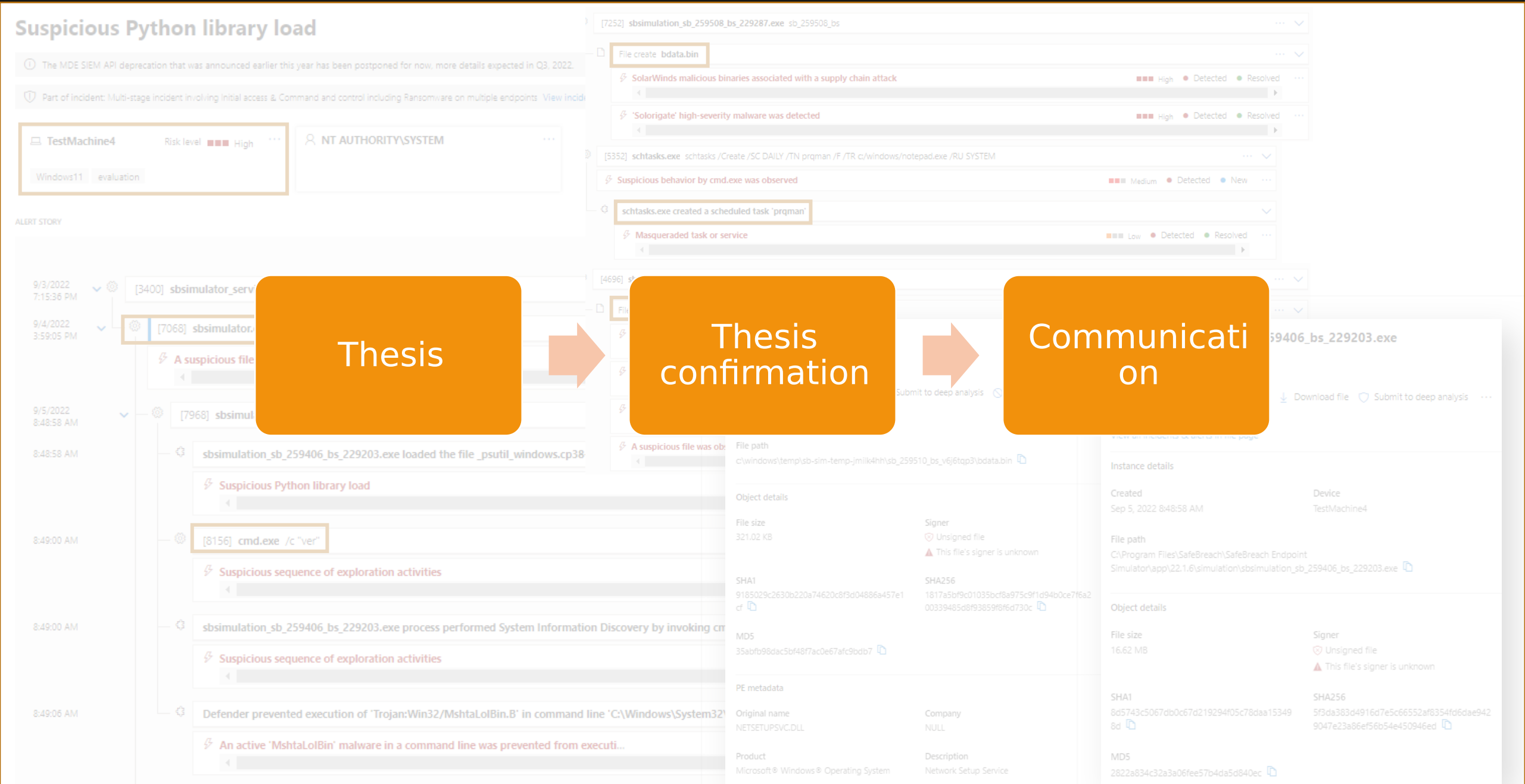
The search for Patient Zero, IOCs and patterns

baseVISION



The search for Patient Zero, IOCs and patterns

baseVISION



Is it over already?

Is it over already? Detections

During an Incident
- Active attack remediation
- Prioritization o f critical operations

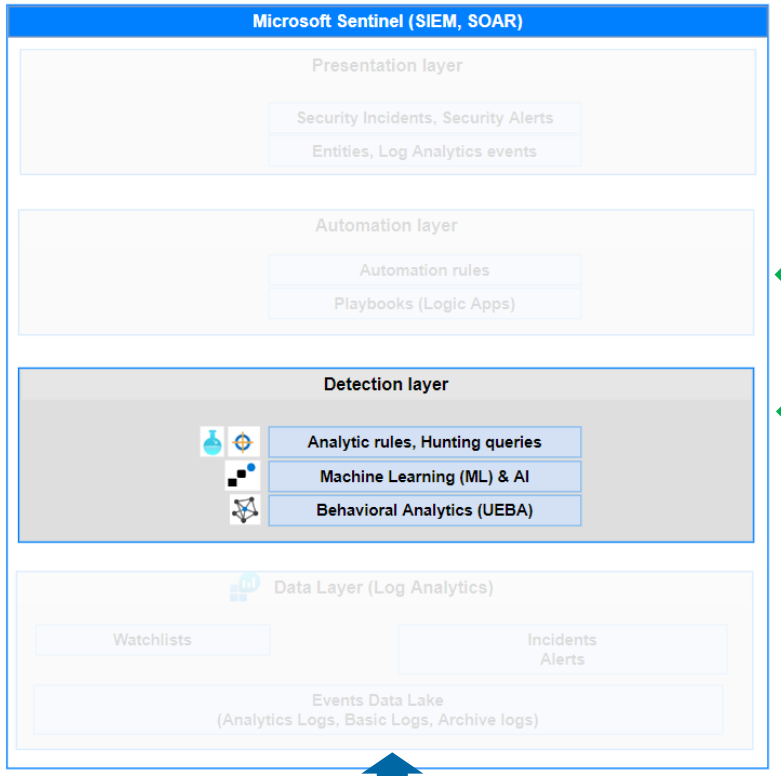
Before an Incident
- Business impact limitation
- Prevent attacks at earliest possible stage
- Hygiene
- Advanced Hunting

After an Incident
- Full business operations restoration
- Detection

Feedback loop
- Lessons learned, change integration

Visualization based on:
Design security for a resiliency strategy - Training | Microsoft Learn

Break the chain – Detections



Analytic rules

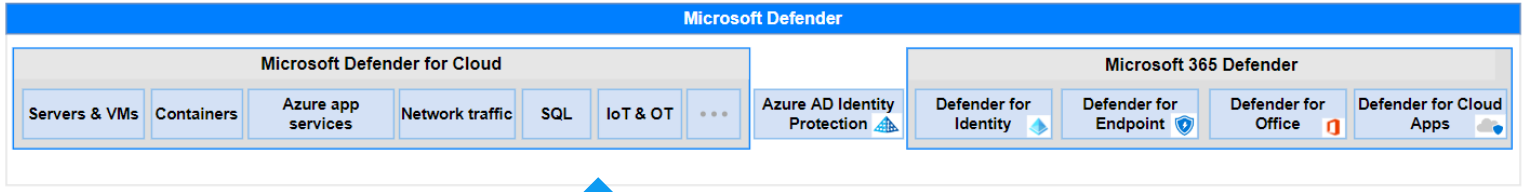
- Detection logic correlates data from Log Analytics tables (**KQL**)
- Trigger for Automation (Automation rules/Playbooks
- Query schedule: 1 minute – 14 days
- Can include external IOC data during runtime
- Detection results (entities) summarized in security incidents
- Community contributions

Hunting queries

- Proactive Hunting for specific use cases/patterns (MITRE ATT&CK) Techniques)
- Manual Bulk-run
- Hunting query logic (**KQL**) can be migrated to an Analytic rule
- Livestream
- Community contributions

Microsoft Detection

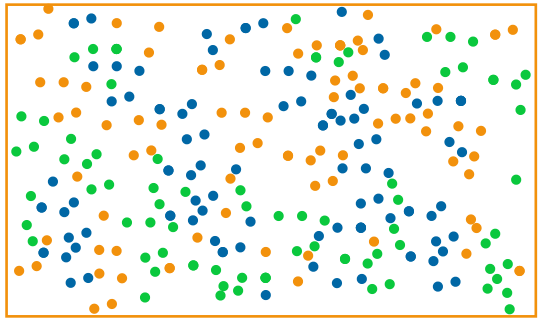
- AI, ML
- Correlation of events and entity behavior patterns
- Microsoft Detection logic
- Custom detection rules (running on **KQL**) in Microsoft 365 Defender



Break the chain – Detections

Detect future malicious patterns/IOC

Events

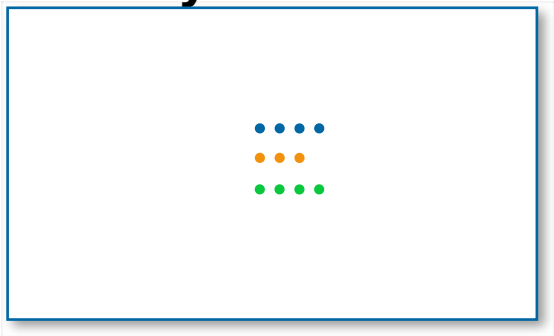


System/user-driven events stored in multiple tables

Detection

Custom queries searching for **identified malicious patterns/IOC** in Sentinel Tables

Security Incidents



Security incidents with aggregated detection results visible to the customer / SOC

Table’s turning – from the hunted to the hunter

Table’s turning – from the hunted to the hunter

During an Incident
- Active attack remediation
- Prioritization o f critical operations

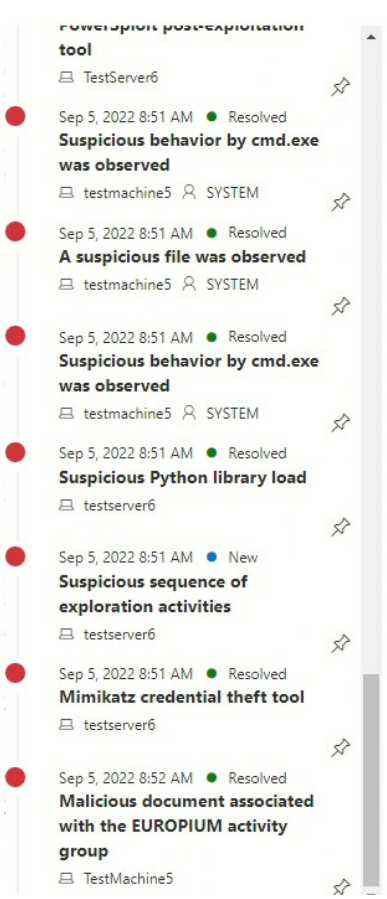
Before an Incident
- Business impact limitation
- Prevent attacks at earliest possible stage
- Hygiene
- Advanced Hunting

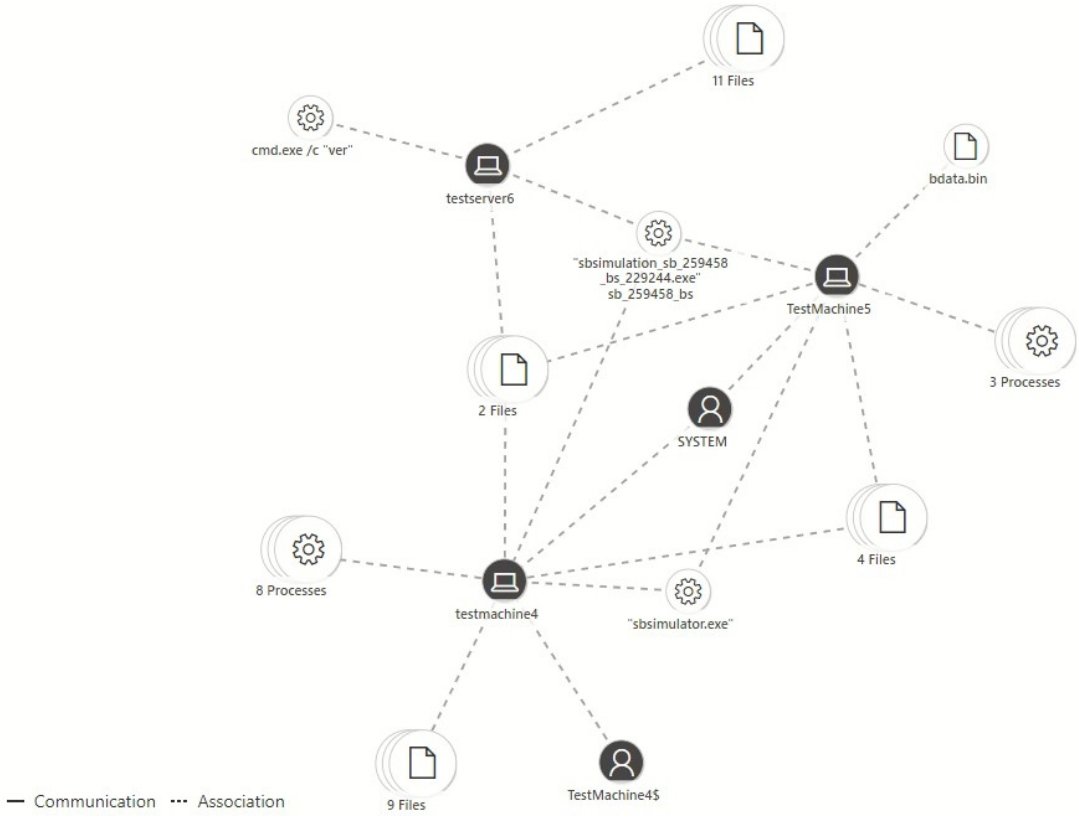
After an Incident
- Full business operations restoration
- Detection

Feedback loop
- Lessons learned, change integration

Visualization based on:
Design security for a resiliency strategy - Training | Microsoft Learn

Table's turning – Proactive Threat Hunting



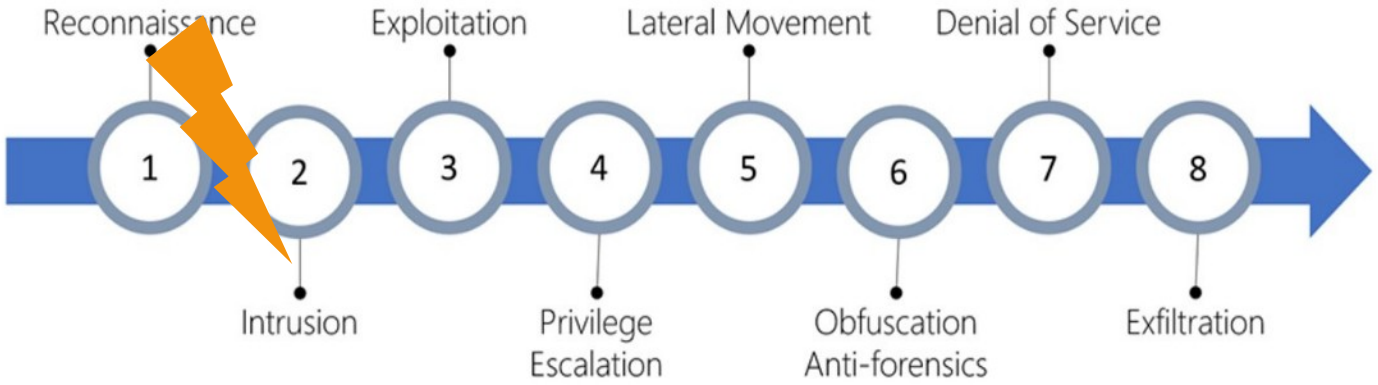


Table’s turning – Proactive actions

- Proactively and continuously searching for malicious patterns and IOCs to **prevent** adversary activities
- **Proactive Threat hunting** based on hypothesis, threat intelligence data
- Searching for gaps (configuration, hygiene, vulnerabilities, identity behavior, …)

Goals:

- Detection of anomalies, attacks and attack vectors at the earliest possible stage
- Disruption of human-operated/sophisticated attacks exploiting vulnerabilities



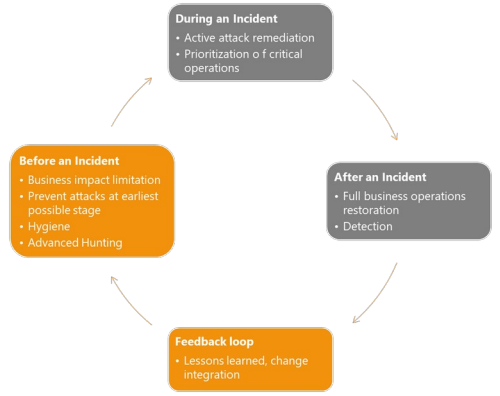


Image source: Understand security operations frameworks, processes, and procedures - Training | Microsoft Learn
Image based on MITRE ATT&CK ™ framework

Effective and Simple Security

- Coverage
- Integration
- Microsoft as Security and Threat Experts
- Efficient Operation

Thank you!

baseVISION
SECURE & MODERN ENDPOINT MANAGEMENT