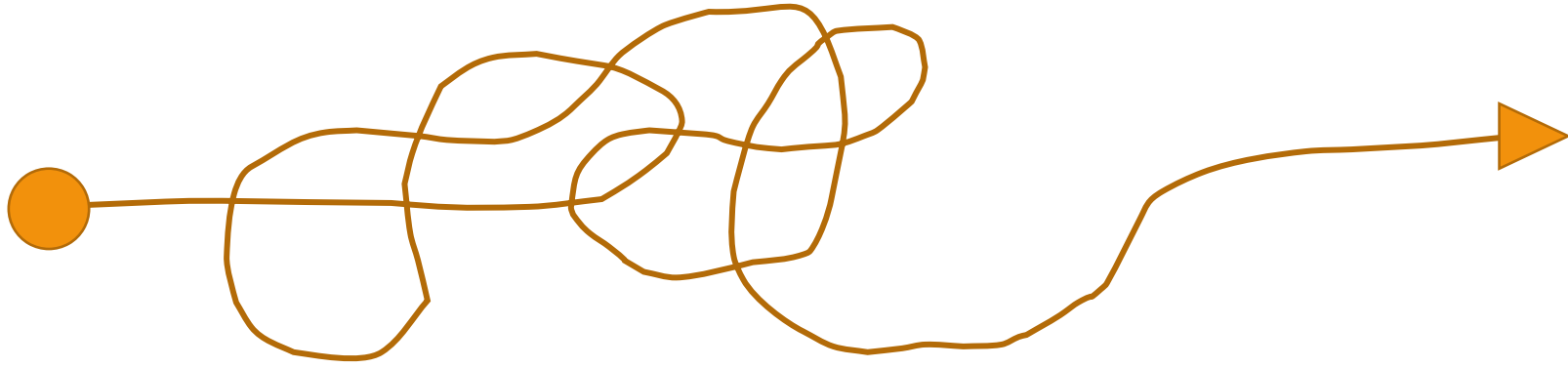


Emerging Threats – Turning from the hunter to the hunted





Effective and
Simple





Christoph Düggele

Security Analyst, baseVISION AG

MAS Information System Management

IPMA Level D

ITILv3



Contact Me

Mail: christoph.dueggeli@basevision.ch

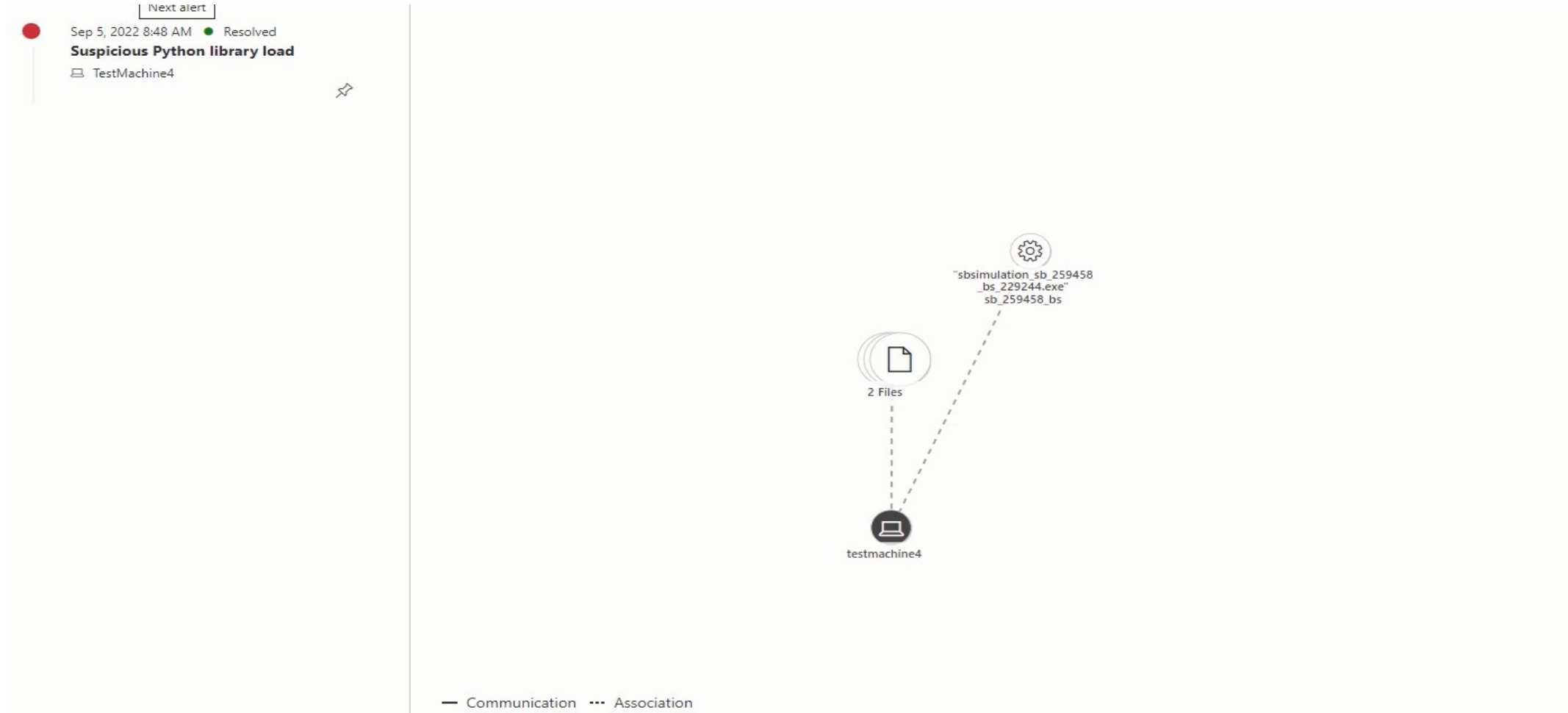
Phone: +41 622 91 30 00



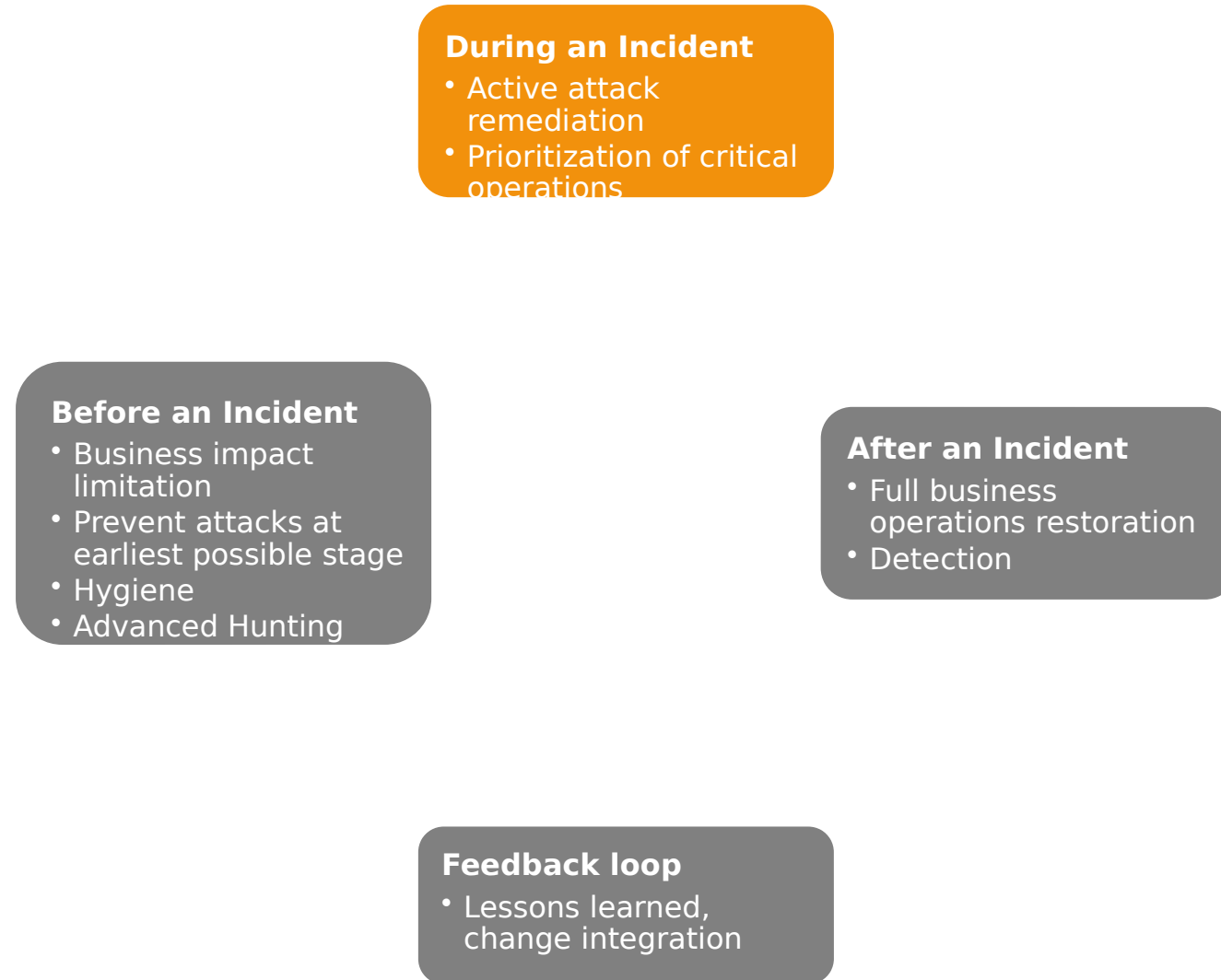
- Leftovers – when it's too late
- Is it over already?
- Table's turning – from the hunted to the hunter

Leftovers – when it's too late





Post Breach investigations – Thesis confirmation



The search for Patient Zero, IOCs and patterns

Suspicious Python library load

The MDE SIEM API deprecation that was announced earlier this year has been postponed for now, more details expected in Q3, 2022.
Part of incident: Multi-stage incident involving Initial access & Command and control including Ransomware on multiple endpoints [View incident](#)

TestMachine4 Risk level ■ ■ ■ High NT AUTHORITY\SYSTEM
Windows11 evaluation

ALERT STORY

9/3/2022 7:15:36 PM [3400] sbsimulator_service.exe

9/4/2022 3:59:05 PM [7068] sbsimulator.exe

- A suspicious file was observed

9/5/2022 8:48:58 AM [7968] sbsimulation_sb_259406_bs_229203.exe sb_259406_bs

- sbsimulation_sb_259406_bs_229203.exe loaded the file _psutil_windows.cp38
- Suspicious Python library load

8:49:00 AM [8156] cmd.exe /c "ver"

- Suspicious sequence of exploration activities

8:49:00 AM sbsimulation_sb_259406_bs_229203.exe process performed System Information Discovery by invoking cmd

- Suspicious sequence of exploration activities

8:49:06 AM Defender prevented execution of 'Trojan:Win32/MshtaLolBin.B' in command line 'C:\Windows\System32'

- An active 'MshtaLolBin' malware in a command line was prevented from executi...

[7252] sbsimulation_sb_259508_bs_229287.exe sb_259508_bs

- File create bdata.bin
- SolarWinds malicious binaries associated with a supply chain attack
- 'Solorigate' high-severity malware was detected

[5352] sctasks.exe sctasks /Create /SC DAILY /TN prqman /F /TR c:\windows\notepad.exe /RU SYSTEM

- Suspicious behavior by cmd.exe was observed
- sctasks.exe created a scheduled task 'prqman'
- Masqueraded task or service

[4696] sbsimulation_sb_259510_bs_229289.exe sb_259510_bs

- File create bdata.bin
- Suspicious behavior by
- Solorigate Cobalt Strike
- Possible ongoing hands
- A suspicious file was ob

bdata.bin

File path: c:\windows\temp\sb-sim-temp-jmil4h\sb_259510_bs_v6j6tqp3\bdata.bin

Object details

File size	321.02 KB	Signer	Unsigned file
			▲ This file's signer is unknown
SHA1	9185029c2630b220a74620c8f3d04886a457e1cf	SHA256	1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c
MDS	35abfb98dac5bf48f7ac0e67afc9bdb7		

PE metadata

Original name	NETSETUPPSVC.DLL	Company	NULL
Product	Microsoft® Windows® Operating System	Description	Network Setup Service

sbsimulation_sb_259406_bs_229203.exe

Instance details

Created	Sep 5, 2022 8:48:58 AM	Device	TestMachine4
---------	------------------------	--------	--------------

File path: C:\Program Files\SafeBreach\SafeBreach Endpoint Simulator\app\22.1.6\simulation\sbsimulation_sb_259406_bs_229203.exe

Object details

File size	16.62 MB	Signer	Unsigned file
			▲ This file's signer is unknown
SHA1	8d5743c5067db0c67d219294f05c78daa153498d	SHA256	5f3da383d4916d7e5c66552af8354fd6dae9429047e23a86ef56b54e450946ed
MDS	2822a834c32a3a06fee57b4da5d840ec		

The search for Patient Zero, IOCs and patterns

The screenshot displays a SIEM alert story for 'Suspicious Python library load'. The main alert is for ID [7068] on 9/4/2022 at 3:59:05 PM, with a risk level of High. The host is TestMachine4 (Windows11, evaluation) and the user is NT AUTHORITY\SYSTEM. The alert details include:

- File create bdata.bin
- SolarWinds malicious binaries associated with a supply chain attack (High, Detected, Resolved)
- 'Solorigate' high-severity malware was detected (High, Detected, Resolved)
- schtasks.exe created a scheduled task 'prqman' (Low, Detected, Resolved)
- Masqueraded task or service
- A suspicious file was observed
- A suspicious file was observed

The alert story shows a sequence of events:

- 9/3/2022 7:15:36 PM: [3400] sbsimulator_serv...
- 9/4/2022 3:59:05 PM: [7068] sbsimulator... (Main alert)
- 9/5/2022 8:48:58 AM: [7968] sbsimul...
- 8:48:58 AM: sbsimulation_sb_259406_bs_229203.exe loaded the file _psutil_windows.cp38
- 8:49:00 AM: [8156] cmd.exe /c "ver"
- 8:49:00 AM: sbsimulation_sb_259406_bs_229203.exe process performed System Information Discovery by invoking cm...
- 8:49:06 AM: Defender prevented execution of 'Trojan:Win32/MshtaLolBin.B' in command line 'C:\Windows\System32'
- An active 'MshtaLolBin' malware in a command line was prevented from executi...

Analysis panels for the main alert include:

- Object details: File path (c:\windows\temp\sb-sim-temp-jmlk4h\sb_259510_bs_v6j6tqp3\bdata.bin), File size (321.02 KB), SHA1 (9185029c2630b220a74620c8f3d04886a457e1cf), MD5 (35abfb98dac5bf48f7ac0e67afc9bdb7), PE metadata (Original name: NETSETUPSPVC.DLL, Product: Microsoft® Windows® Operating System).
- Instance details: Created (Sep 5, 2022 8:48:58 AM), Device (TestMachine4), File path (C:\Program Files\SafeBreach\SafeBreach Endpoint Simulator\app\22.1.6\simulation\sbsimulation_sb_259406_bs_229203.exe).
- Object details: File size (16.62 MB), SHA1 (8d5743c5067db0c67d219294f05c78daa153498d), MD5 (2822a834c32a3a06fee57b4da5d840ec).

Thesis

Thesis confirmation

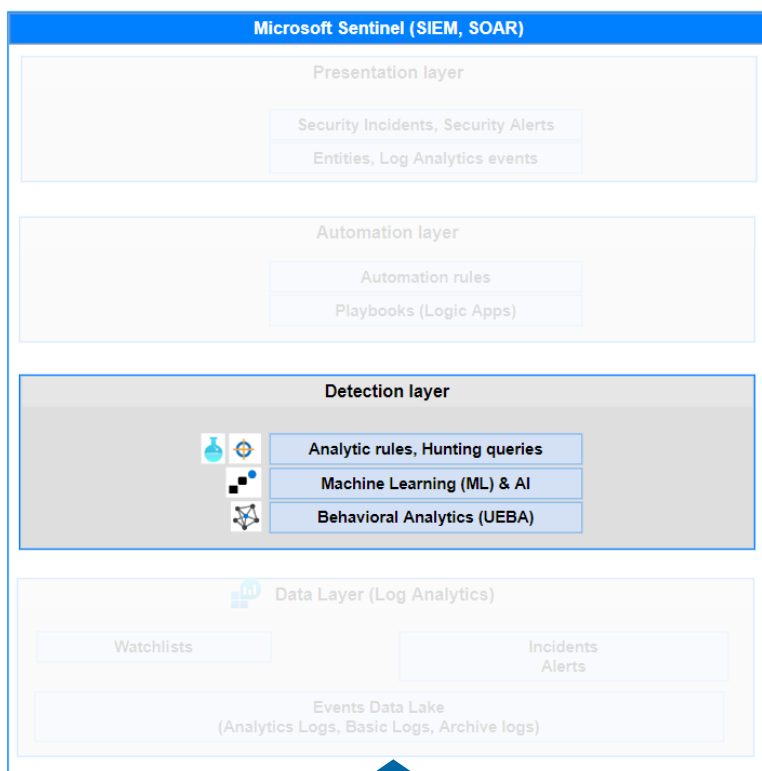
Communication

Is it over already?





Break the chain – Detections



Analytic rules

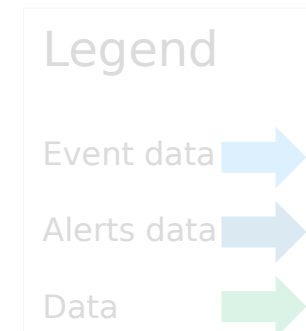
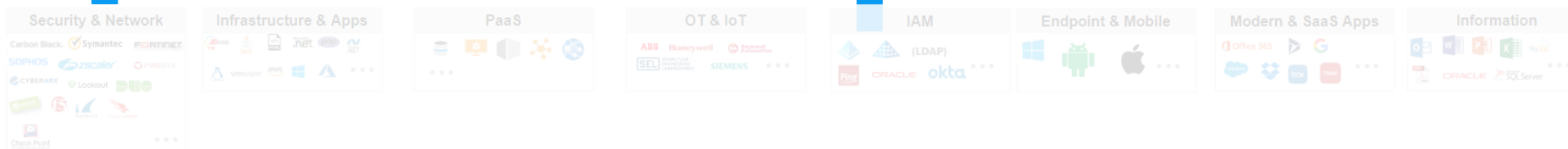
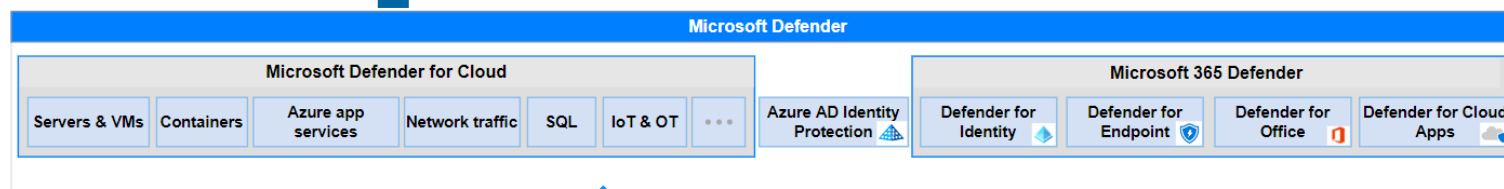
- Detection logic correlates data from Log Analytics tables (**KQL**)
- Trigger for Automation (Automation rules/Playbooks)
- Query schedule: 1 minute - 14 days
- Can include external IOC data during runtime
- Detection results (entities) summarized in security incidents
- Community contributions

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

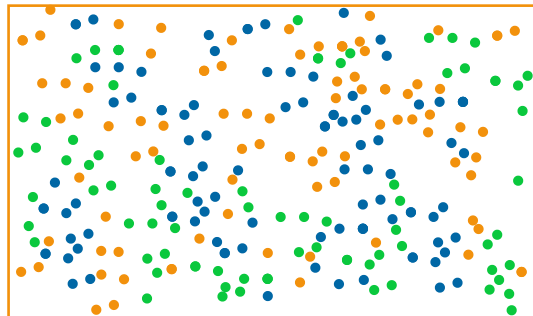
- AI, ML
- Correlation of events and entity behavior patterns
- Microsoft Detection logic
- Custom detection rules (running on **KQL**) in Microsoft 365 Defender



Detect future malicious patterns/IOC



Events



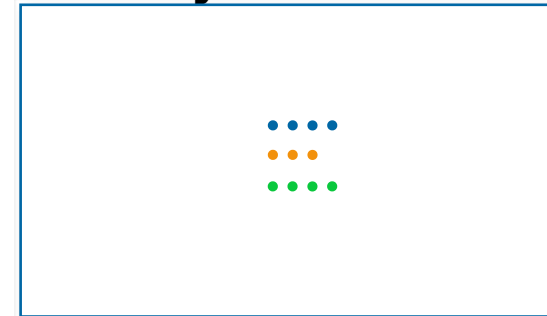
System/user-driven events stored in multiple tables

Detection



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

Security Incidents

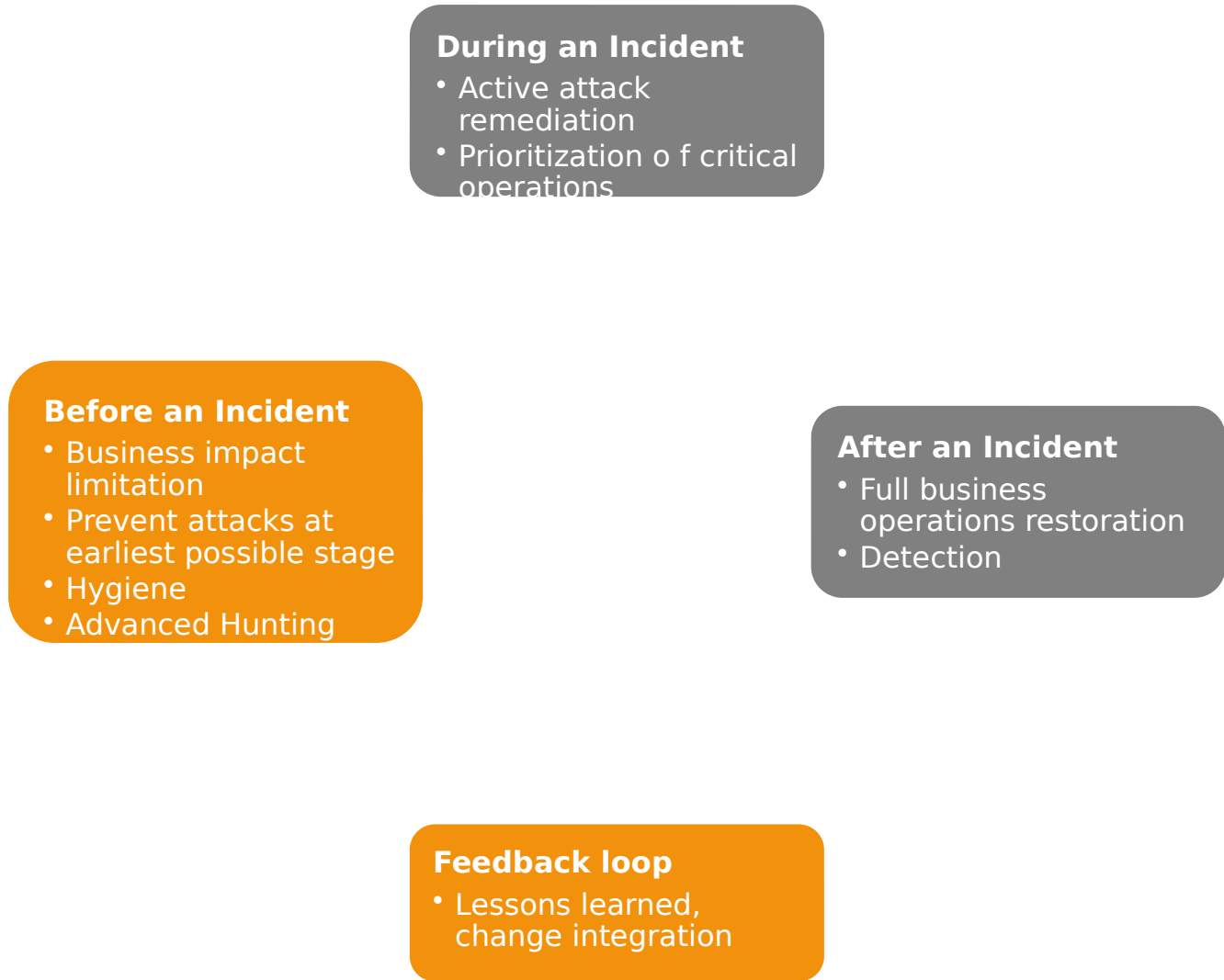


Security incidents with aggregated detection results visible to the customer / SOC

Table's turning - from the hunted to the hunter



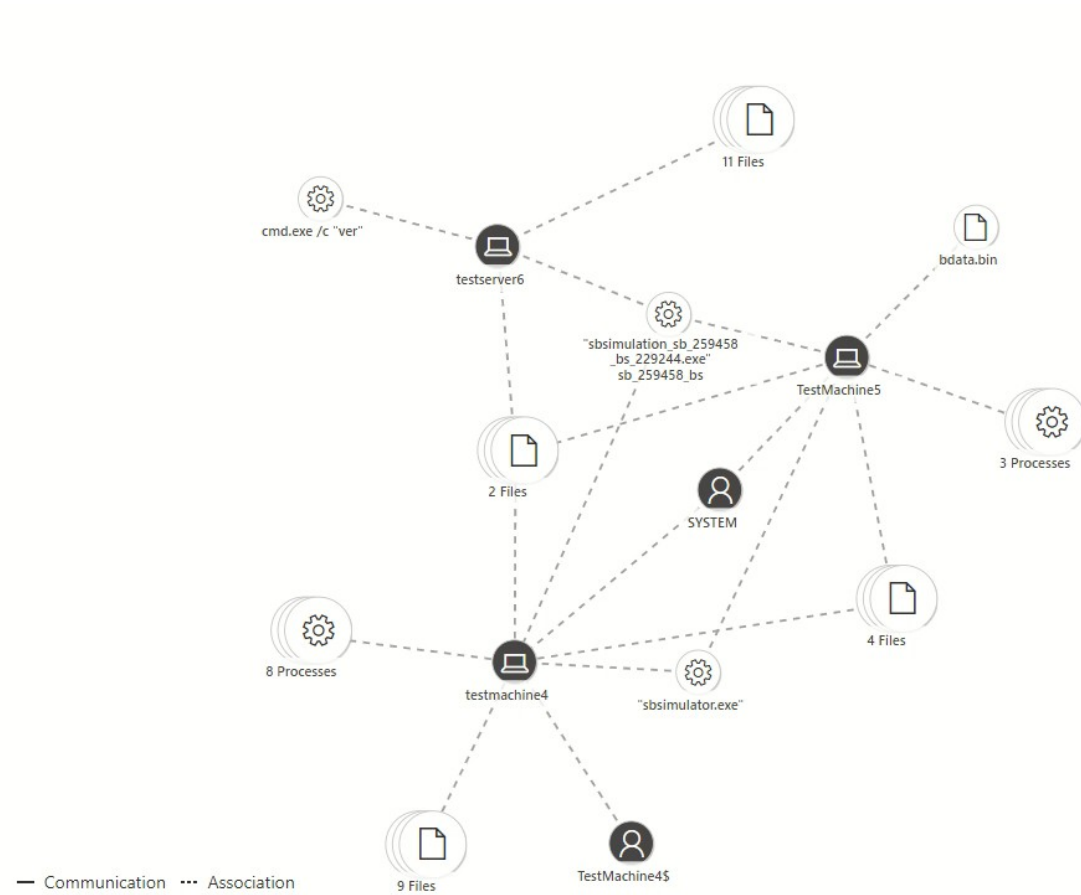
Table's turning – from the hunted to the hunter



Table's turning – Proactive Threat Hunting



- Powercat post-exploitation tool**
 - TestServer6
 - Sep 5, 2022 8:51 AM Resolved
Suspicious behavior by cmd.exe was observed
 - testmachine5 SYSTEM
 - Sep 5, 2022 8:51 AM Resolved
A suspicious file was observed
 - testmachine5 SYSTEM
 - Sep 5, 2022 8:51 AM Resolved
Suspicious behavior by cmd.exe was observed
 - testmachine5 SYSTEM
 - Sep 5, 2022 8:51 AM Resolved
Suspicious Python library load
 - testserver6
 - Sep 5, 2022 8:51 AM New
Suspicious sequence of exploration activities
 - testserver6
 - Sep 5, 2022 8:51 AM Resolved
Mimikatz credential theft tool
 - testserver6
 - Sep 5, 2022 8:52 AM Resolved
Malicious document associated with the EUROPIUM activity group
 - TestMachine5

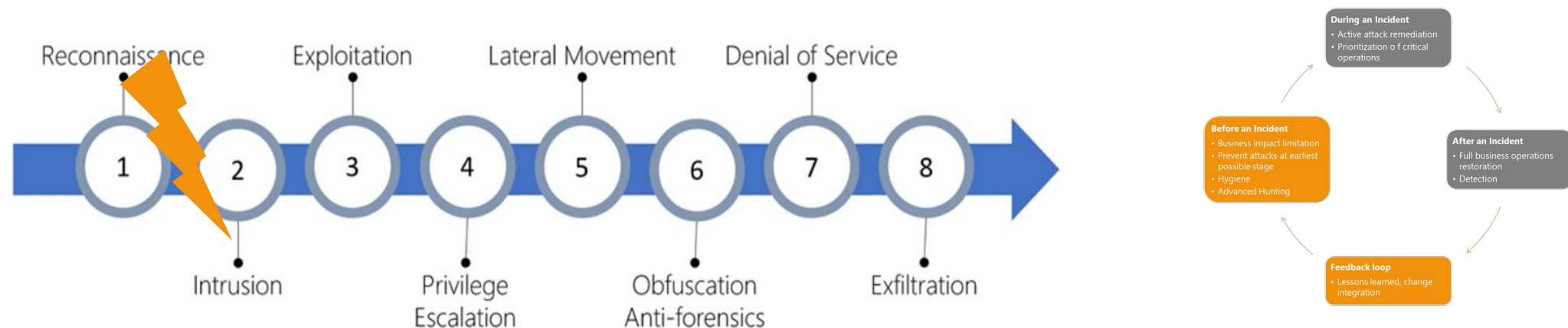


Table's turning – Proactive actions

- 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



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

Thank you!

baseVISION
SECURE & MODERN ENDPOINT MANAGEMENT

