Sh!t we got compromised.

A session on monitoring and remediation using Microsoft 365 Defender and Microsoft Sentinel.

Louis Mastelinck

Thijs Lecomte

Experts Live Netherlands

Louis Mastelinck

Incident Responder & Security Consultant

Lousec

Louismastelinck

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

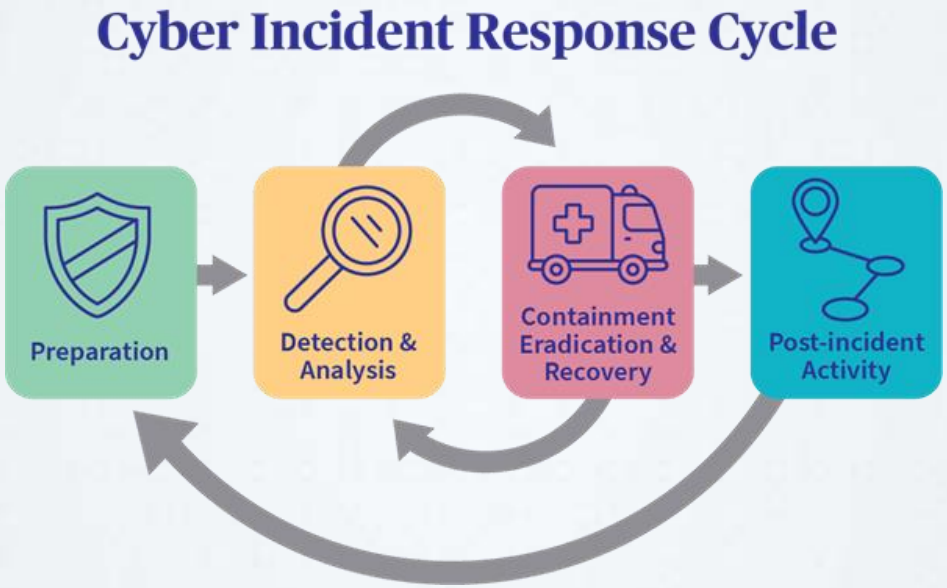
Thijs Lecomte

SOC Lead @ The Collective

Security MVP

https://m365securitybook.com

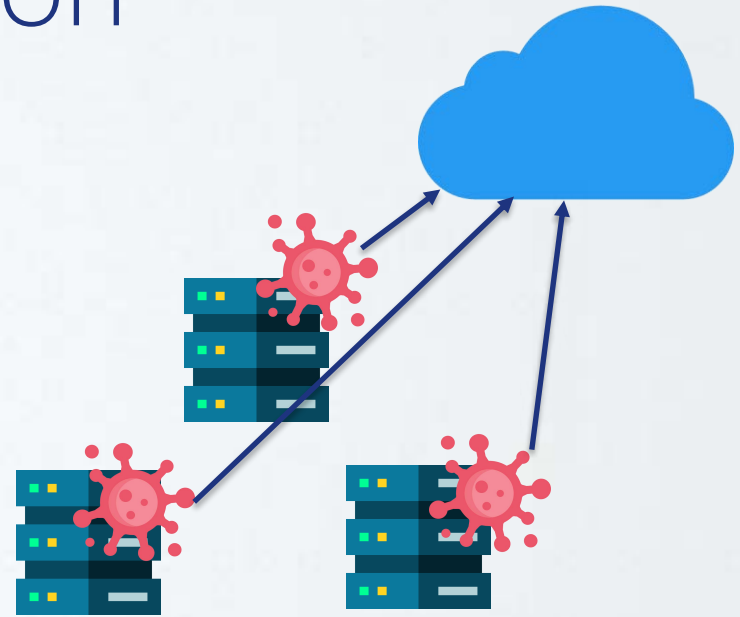
Phases of incident response



cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Detection & Analysis

Alert Information

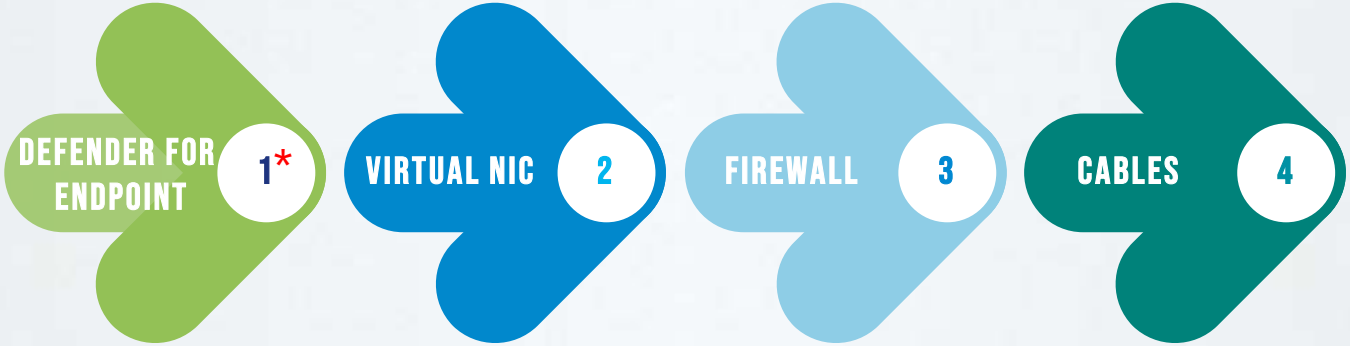


cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Containment

What not to do?

Isolating devices



REQUIRES ONBOARDING
REQUIRES SUPPORTED OS

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Difficult decisions

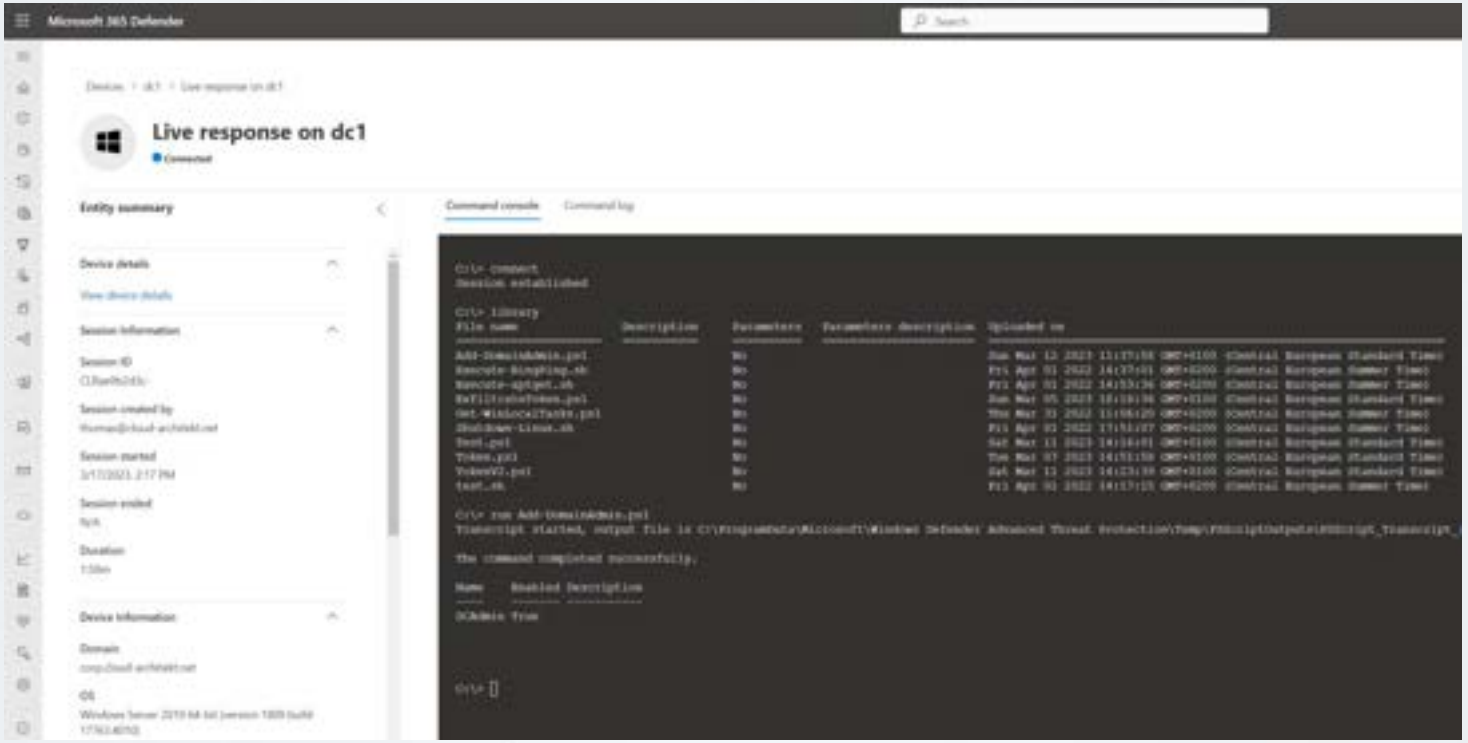
Defensie slachtoffer van zware cyberaanval, deel netwerk al dagen plat

Het leger kampt al sinds vorige donderdag met de gevolgen van een zware cyberaanval. Een deel van het computernetwerk kan voorlopig niet gebruikt worden, zegt de woordvoerder. Zo ligt het mailsysteem al enkele dagen plat. De computeraanval kwam er na een veiligheidslek in de software dat pas vorige week ontdekt werd. Het is niet duidelijk wie achter de computeraanval op Defensie zit.

Jens Franssen
ma 20 dec 2021 08:20

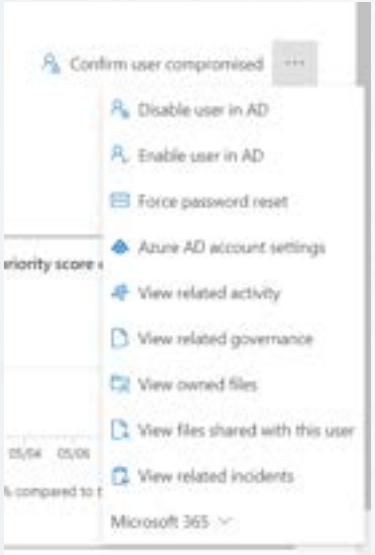
cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

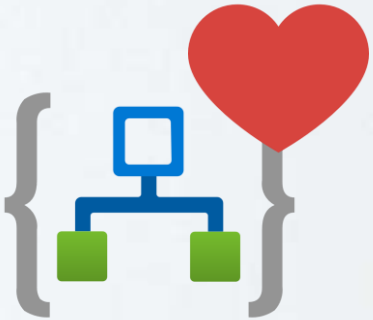
User Accounts



cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Revoking user accounts





Detection & Analysis

Protect

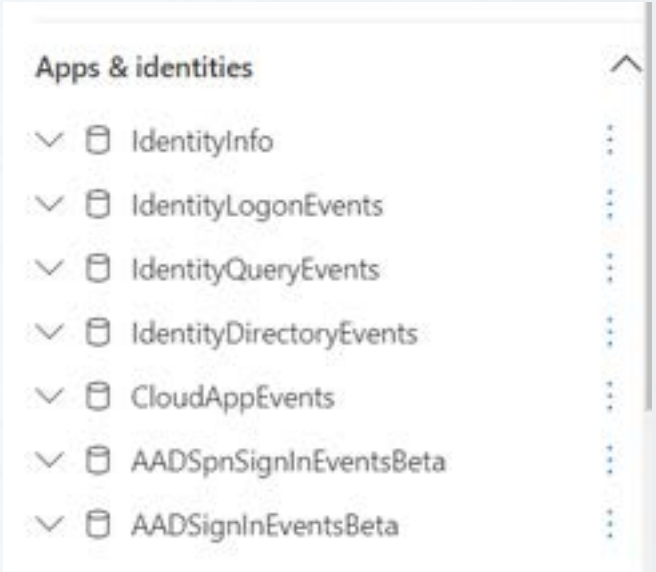
Infected machines

Symptoms = IOC's

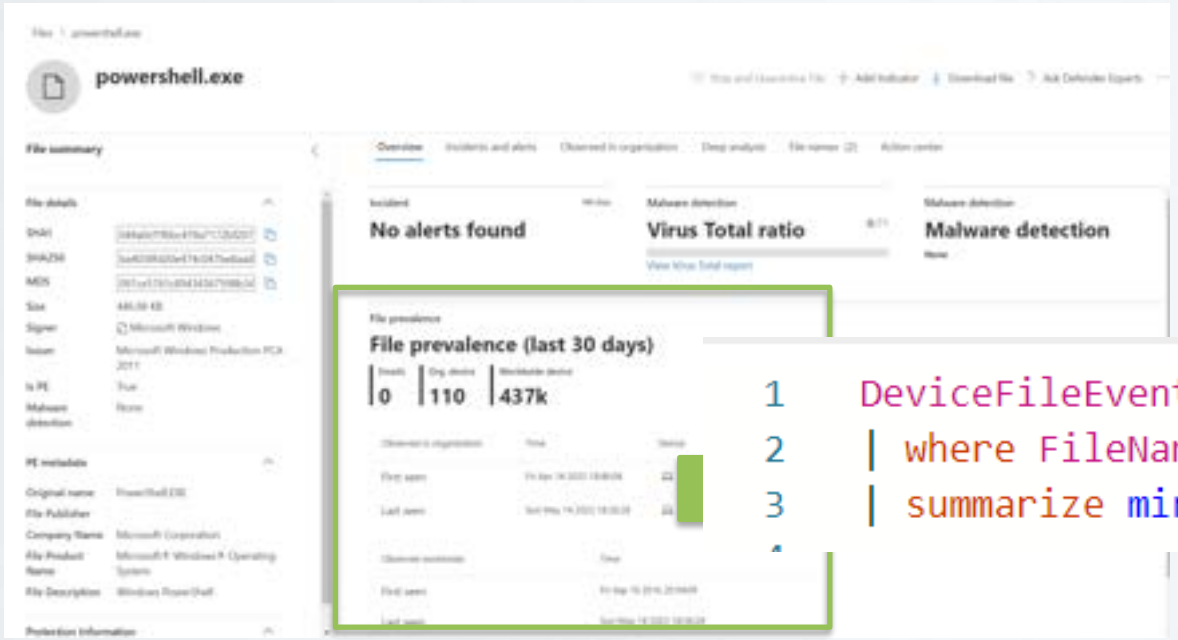
Using IOC's to dig deeper

Defender for Identity

AD Logs in Sentinel?



Using IOC's to dig deeper




```
1   DeviceFileEvents
2   | where FileName == "powershell.exe"
3   | summarize min(Timestamp) by DeviceName
```

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

There is more than Defender

Hunting across sources

- Non-onboarded devices
- Double checking

Important logs

- Proxy
- Network
- Applications

Network Logs

Adding logs in SIEM

Cost exercise

01 IPS/IDS

02 Allow traffic

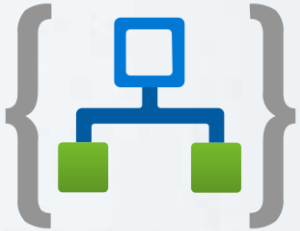
03 Deny traffic

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

SOC Independence

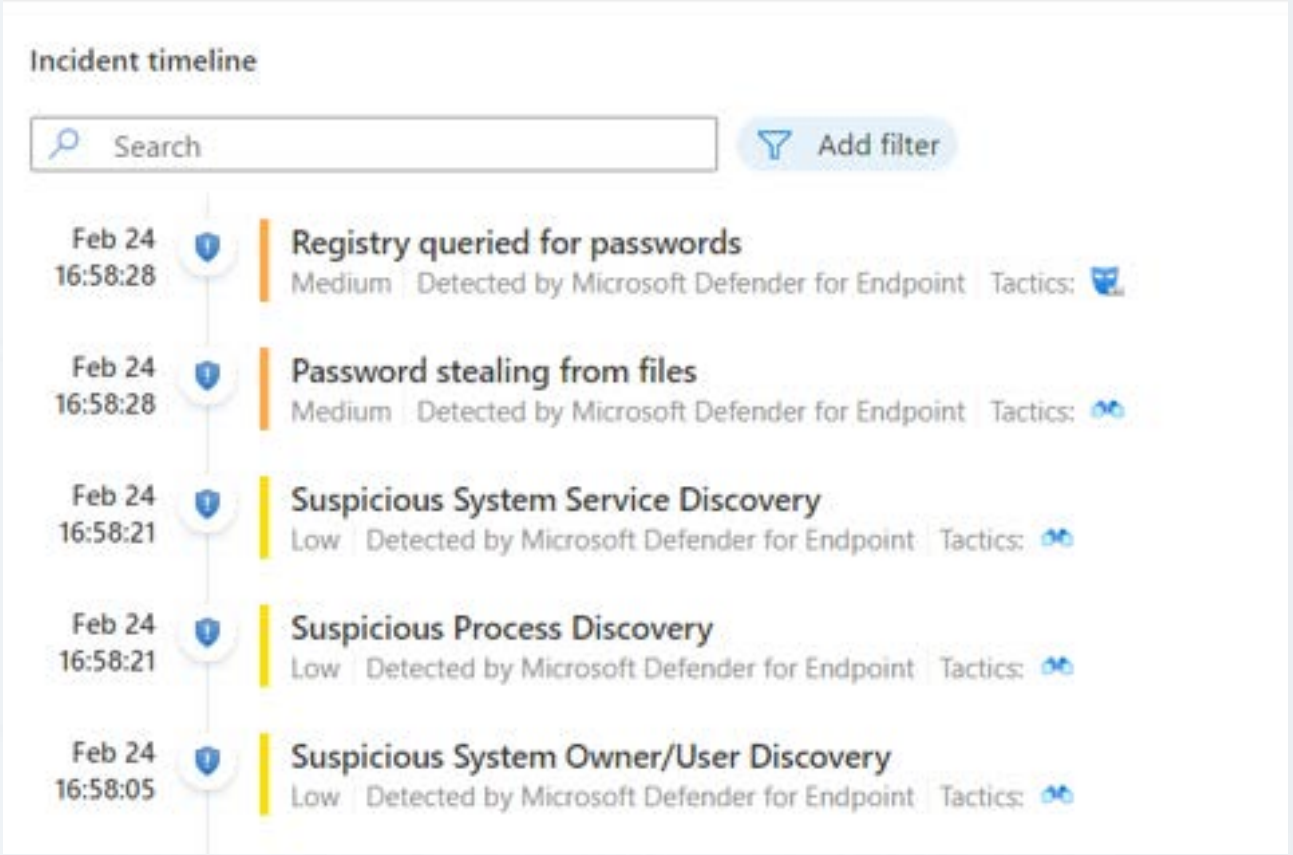
Allows for quicker actions when sh!t hits the fan

Central Logs



Remediation actions

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC



Context is everything

SOC needs to connect with business

Add context during IR

Detection & Analysis
Using the tools

Finding indicators

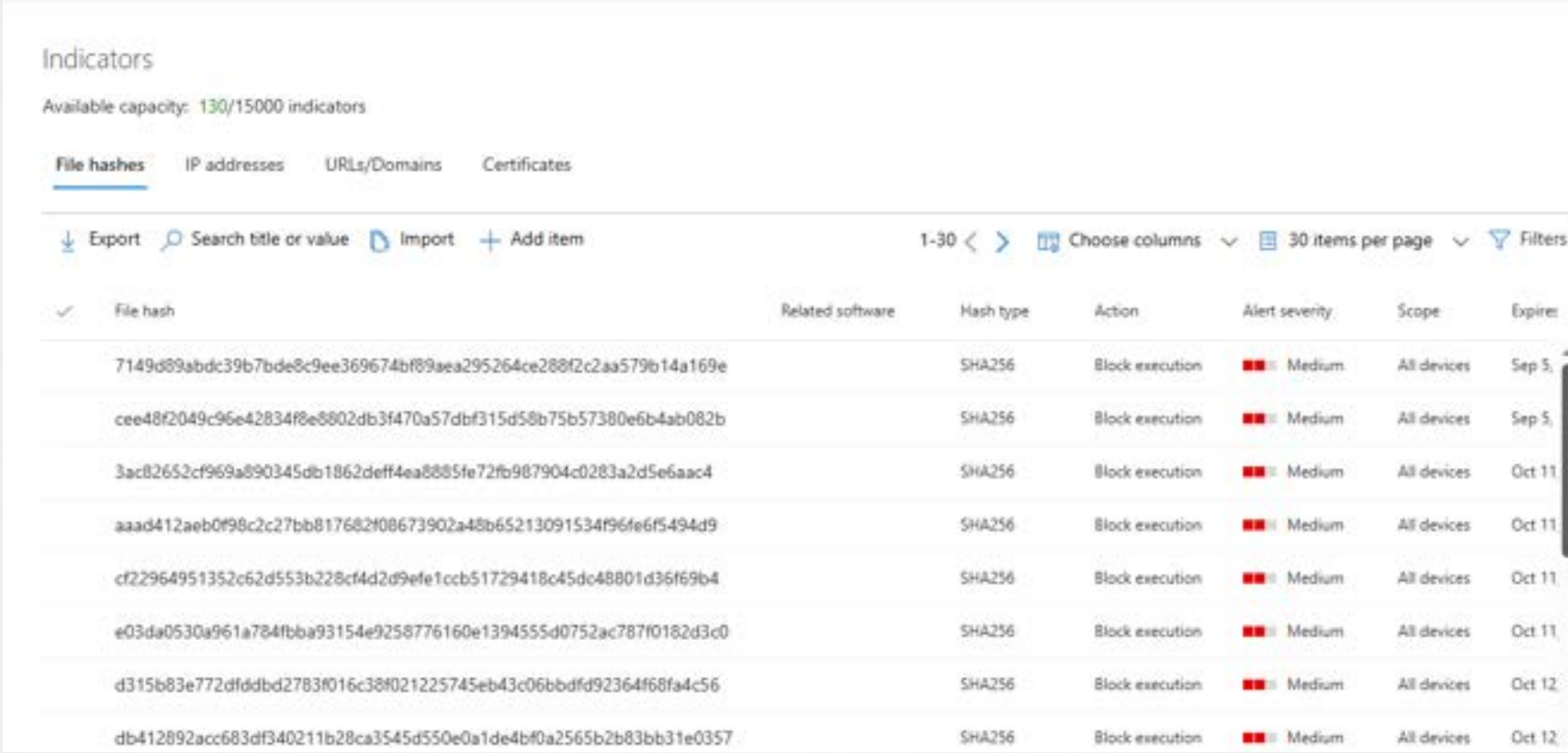
MDE alerting/logs

Sandbox analysis

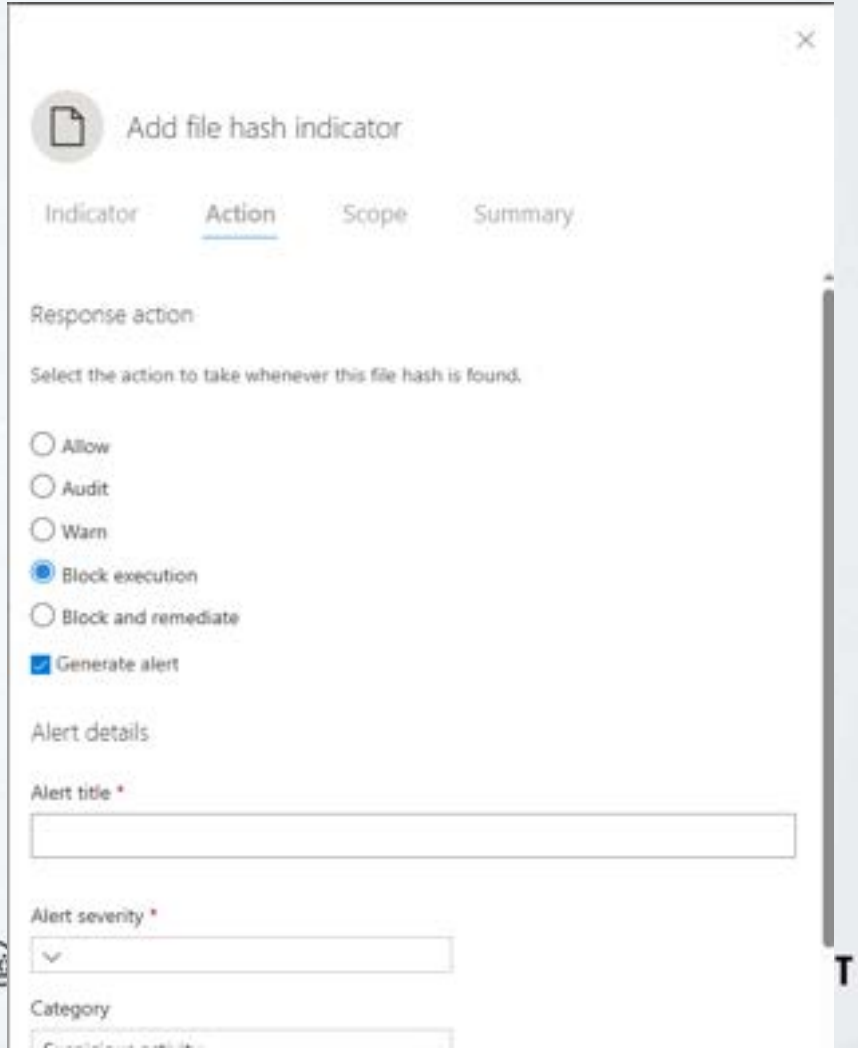
Public resources

Reverse engineering

Protect


Indicators
Available capacity: 130/15000 indicators
File hashes
IP addresses
URLs/Domains
Certificates
Export
Search title or value
Import
Add item
1-30
Choose columns
30 items per page
Filters
File hash
Related software
Hash type
Action
Alert severity
Scope
Expires
7149d89abdc39b7bde8c9ee369674bf89aea295264ce288f2c2aa579b14a169e
SHA256
Block execution
Medium
All devices
Sep 5,
cee48f2049c96e42834f8e8802db3f470a57dbf315d58b75b57380e6b4ab082b
SHA256
Block execution
Medium
All devices
Sep 5,
3ac82652cf969a890345db1862deff4ea8885fe72fb987904c0283a2d5e6aac4
SHA256
Block execution
Medium
All devices
Oct 11
aaad412aeb0f98c2c27bb81768f08673902a48b65213091534f96fe6f5494d9
SHA256
Block execution
Medium
All devices
Oct 11
cf22964951352c62d553b228cf4d2d9efe1ccb51729418c45dc48801d36f69b4
SHA256
Block execution
Medium
All devices
Oct 11
e03da0530a961a784fbba93154e9258776160e1394555d0752ac787f0182d3c0
SHA256
Block execution
Medium
All devices
Oct 11
d315b83e772dfddbd2783f016c38f021225745eb43c06bbdfd92364f68fa4c56
SHA256
Block execution
Medium
All devices
Oct 12
db412892acc683df340211b28ca3545d550e0a1de4bf0a2565b2b83bb31e0357
SHA256
Block execution
Medium
All devices
Oct 12

Protect



cegeka INSPARK TIC

Pushing indicators

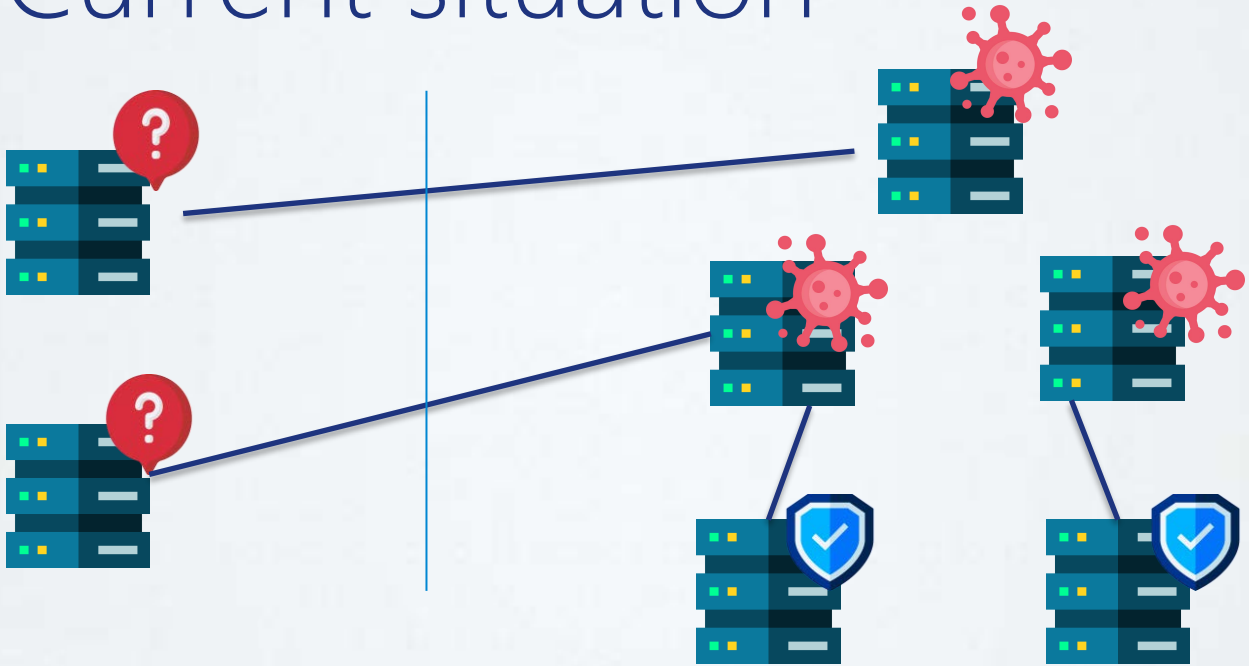
Where?

- Defender
- Sentinel

Automation

- MSSP
- Multiple environments

Current situation



Onboarded

Not onboarded

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Auditing & Monitoring

Dear customer

thijs.lecomte.admin@thecollective.eu has Update conditional access policy called CAPOL - BLOCK - OFFICE DESKTOP ACCESS - COMPLIANCY. The following changes were done: Users CAPolicy : CAPOL-BLOCK-OFFICEDESKTOPACCESS-COMPLIANCY

Please find the JIRA incident: View Issue
To provide feedback: Please reopen the incident through our JIRA portal and provide feedback in the comments

If you have any questions or remarks, please don't hesitate to reach out to our SOC team.
Kind regards
Cloud Control - The Collective

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Detection & Analysis

Enlarging the scope

Detect

Custom detections

Onboard the not onboarded

Importance of visiblity

Monitoring

Detection

Remedation

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

A story of not onboarded devices

Usage of personal devices

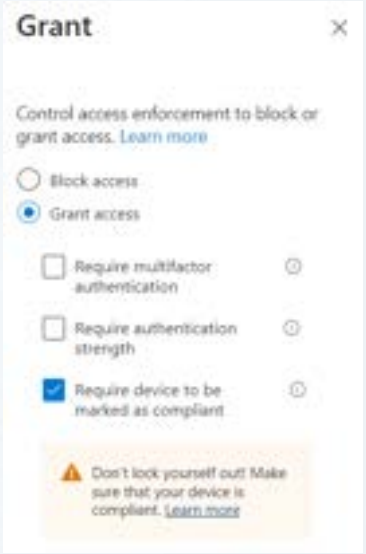
Malware from phishing email

Access to Password Manager (Developer)

Difficulties

- Identification
- Remedation

A story of not onboarded devices



cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Onboarding requires logging in

But…

They will steal your account…?

Sacrifice an account

They already had domain admin

Make new one

Use it and burn it

Monitor it

Recovery

Recover

- Restore a backup
  - Quicker
  - Integrity?
- Clean install
  - More effort
  - Do things the right way

But how did we find the source?

THOR APT Scanner (Nextron)

Advanced YARA rule scanner

Exploit method

Vulnerability

This is not a sponsorship
It just worked for us!

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

THOR

REASON_1: YARA rule SUSP_ServU_SSH_Error_Pattern_Jul21_1 / Detects suspicious SSH component exceptions that could be an indicator of exploitation attempts as described in advisory addressing CVE-2021-35211 in ServU services
SUBSCORE_1: 60
REF_1: https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35211#FAQ
SIGTYPE_1: internal
MATCHED_1:
- ***Removed due to Trial License Restriction*** at *0x0*

RULEDATE_1: 2021-07-12
TAGS_1: CVE_2021_35211, EXPLOIT, EXTVAR, SUSP, T1021
RULENAME_1: SUSP_ServU_SSH_Error_Pattern_Jul21_1
AUTHOR_1: Florian Roth

Alerts

Alert 1

Jan 22 11:13:13 [redacted] *10.12.51.79*

MODULE: ProcessCheck
MESSAGE: YARA rule match on process memory
RULE: EXT_HKTL_Meterpreter_inMemory
TAGS: HKTL, METASPLOIT, VENDOR
DESC: Detects Meterpreter in-memory
SCORE: 85
REFERENCE: https://www.reddit.com/r/purpleteamsec/comments/hjux11/meterpreter_memory_indicators_detection_tooling/
RULEDATE: 2020-06-29
AUTHOR: netbiosX, Florian Roth
SIGTYPE: internal
PID: 736
NAME: svchost.exe
CMD: C:\Windows\system32\svchost.exe -k DcomLaunch -p -s PlugPlay
USER: NT AUTHORITY\SYSTEM
PATH: C:\Windows\System32\svchost.exe
CREATED: Sun Dec 25 13:20:36 2022
MATCHED_STRINGS:
- ***Removed due to Trial License Restriction*** at *0x0*

MODULES: (not in module)

Closing off

Scope

Full scope takes time, but is essential

01

02

Independence

At time of crisis, the SOC needs to be able to respond swiftly.

Auditing

Trust, but verify

04

03

Vulnerability Management

It's a never-ending cycle.

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Rate our session on Yellenge

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

14h00 – 14h50

Ease your workload by implementing Configuration-as-Code for Microsoft 365

Experts Live Netherlands