Gib dem Dino Futter – adaptive Detektion von Bedrohungen in KRITIS-Netzwerken mittels Open-Source-Forensik

Michael Mundt, Harald Baier

31. DFN-Konferenz „Sicherheit in vernetzten Systemen“
30.-31. Januar 2024, Grand Elysée Hotel Hamburg

Agenda

- Motivation
- Systeme zur Angriffserkennung
- Threat Intelligence
- DFIR
- Konzept
- Evaluierung
- Zusammenfassung und Ausblick

Agenda

- Motivation
- Systeme zur Angriffserkennung
- Threat Intelligence
- DFIR
- Konzept
- Evaluierung
- Zusammenfassung und Ausblick

Angriffsvektoren im Cyberraum
2023

28.07.2023

Aufregung um gestohlenen Microsoft Masterkey: Was ist los? Wie sollte Ihr Unternehmen reagieren?

Quelle: Internet
https://www.matrix.ag/die-matrix/news/gestohlener-microsoft-masterkey-was-tun,
aufgerufen am 25.01.2024

GESCHICHTE EINES RANSOMWARE-ANGRIFFS

"Landkreis Anhalt-Bitterfeld, you are fucked"

Zwei Jahre nach dem Security-Vorfall in Anhalt-Bitterfeld sind die Folgen noch immer zu spüren. Sabine Griebsch war als CDO mittendrin, als der Hackerangriff zum Katastrophenfall wurde.

Ein Bericht von Daniel Ziegener

21. Juli 2023, 9:49 Uhr

Quelle: Internet
https://www.golem.de/news/geschichte-eines-ransomware-angriffs-landkreis-anhalt-bitterfeld-you-are-fucked-2307-175123.html
aufgerufen am 25.01.2024

Agenda

- Motivation
- Systeme zur Angriffserkennung
- Threat Intelligence
- DFIR
- Konzept
- Evaluierung
- Zusammenfassung und Ausblick

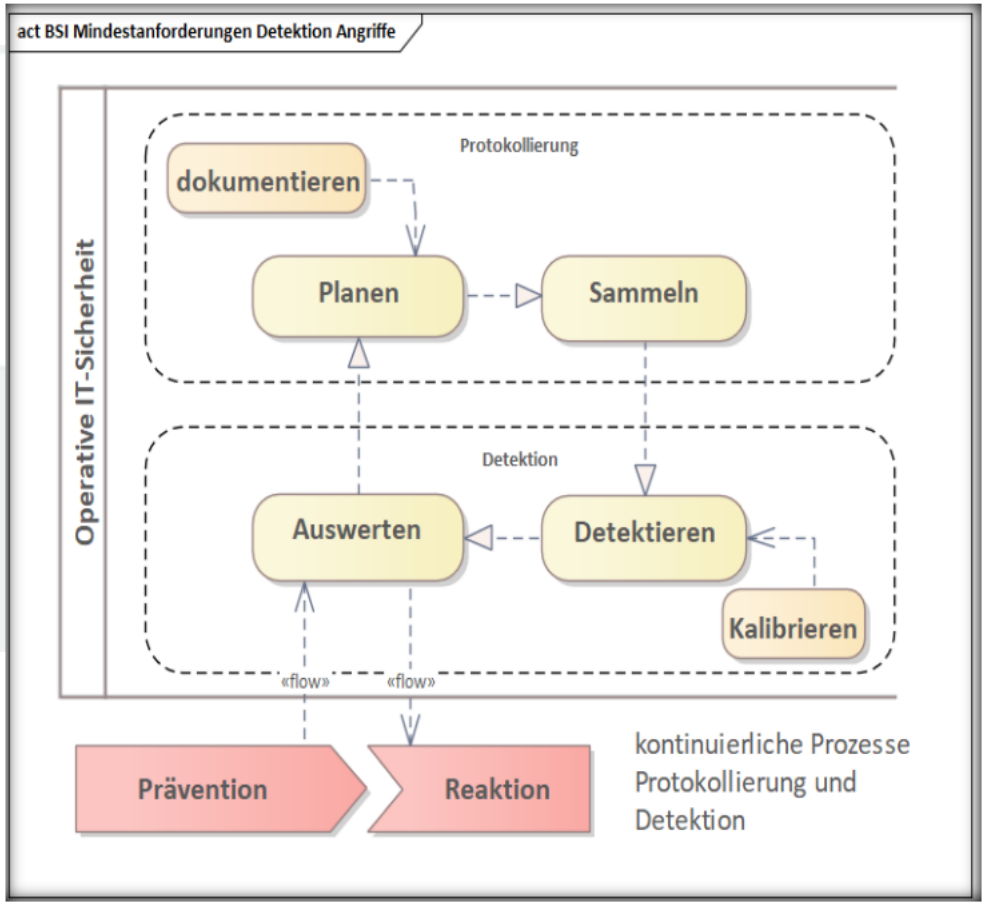
System zur Angriffserkennung

Orientierungshilfe

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung



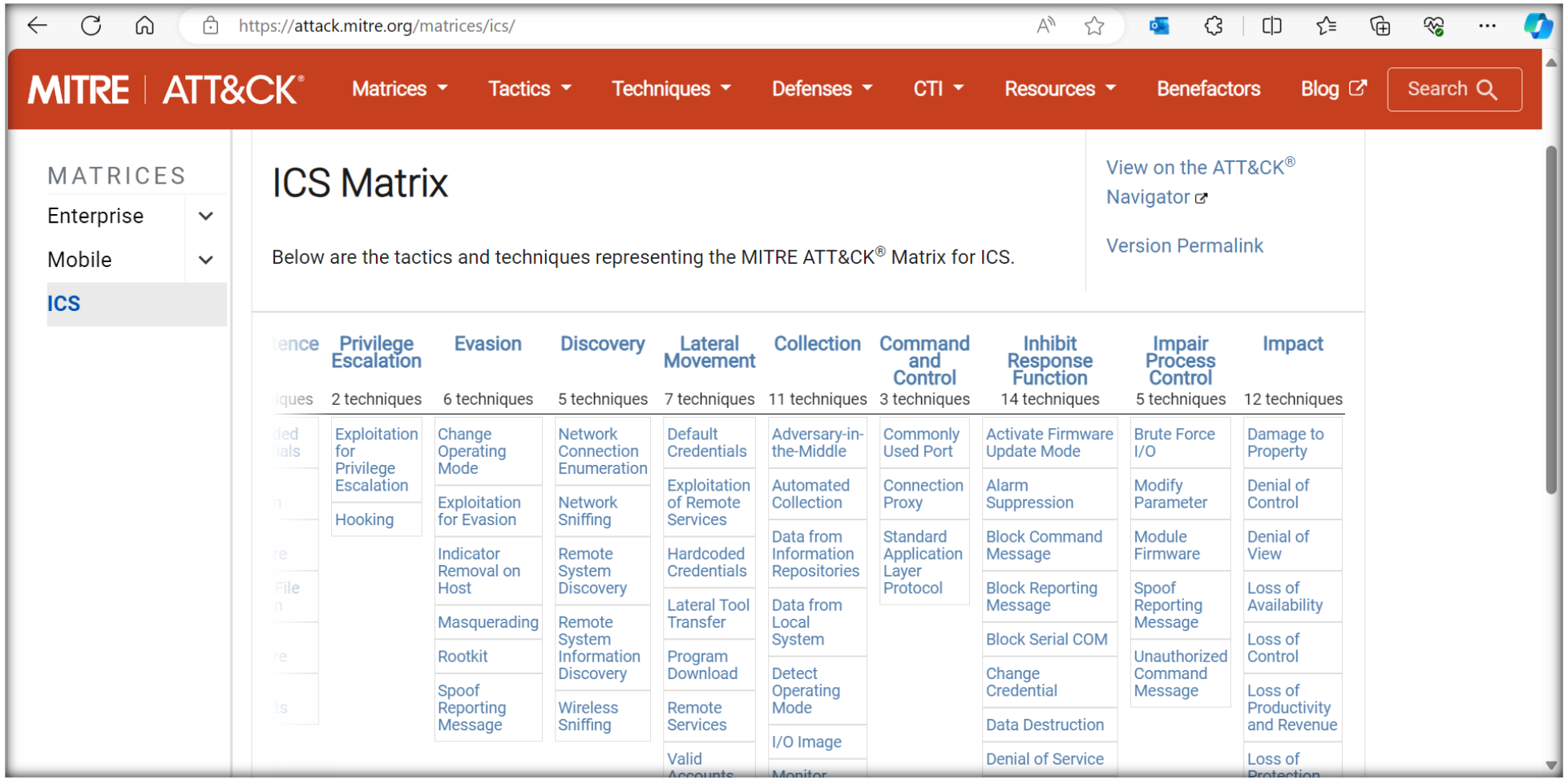
Quelle: Internet
Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung (bund.de),
aufgerufen am 25.01.2024

Agenda

- Motivation
- Systeme zur Angriffserkennung
- Threat Intelligence
- DFIR
- Konzept
- Evaluierung
- Zusammenfassung und Ausblick

Threat Intelligence

MITRE ATT&CK Framework



Quelle: Internet
Matrix | MITRE ATT&CK®.de),
aufgerufen am 25.01.2024

Threat Intelligence

Zusammenhänge im Datenmodell der Wissensdatenbasis

Quelle: Internet
https://attack.mitre.org/tactics/TA0104/
aufgerufen am 25.01.2024

MITRE | ATT&CK®

TACTICS

- ICS
  - Initial Access
  - **Execution**
  - Persistence
  - Privilege Escalation
  - Evasion
  - Discovery
  - Lateral Movement
  - Collection
  - Command and Control

Home > Tactics > ICS > Execution

Execution

The adversary is trying to run code or manipulate system functions, parameters, and data in an unauthorized way.

T0807	Command-Line Interface	Adversaries may utilize command-line interfaces (CLIs) to interact with systems and execute commands. CLIs provide a means of interacting with computer systems and are a common feature across many types of platforms and devices within control systems environments. Adversaries may also use CLIs to install and run new software, including malicious tools that may be installed over the course of an operation.

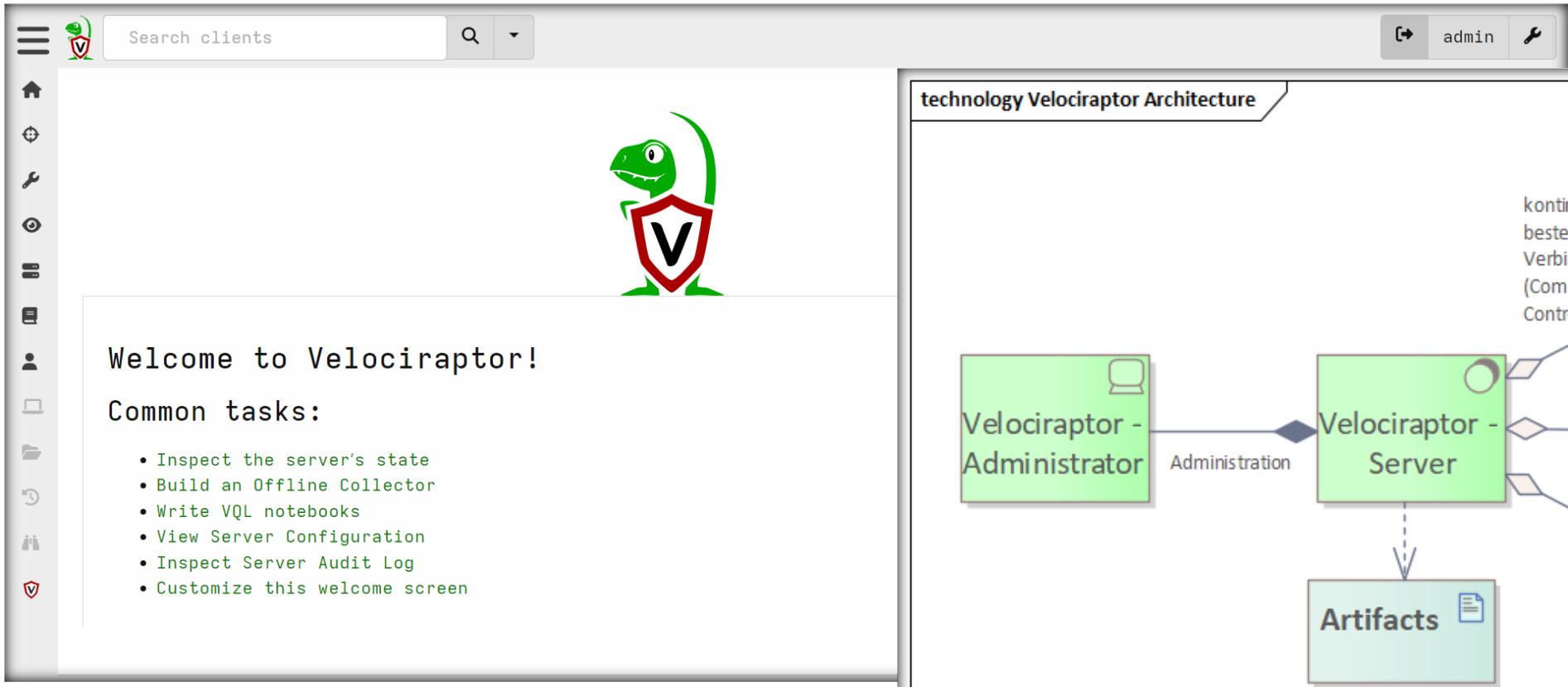
DS0017	Command	Command Execution	On Windows and Unix systems monitor executed commands and arguments that may use shell commands for execution. Shells may be common on administrator, developer, or power user systems depending on job function.

Agenda

- Motivation
- Systeme zur Angriffserkennung
- Threat Intelligence
- DFIR
- Konzept
- Evaluierung
- Zusammenfassung und Ausblick

DFIR

Velociraptor Framework

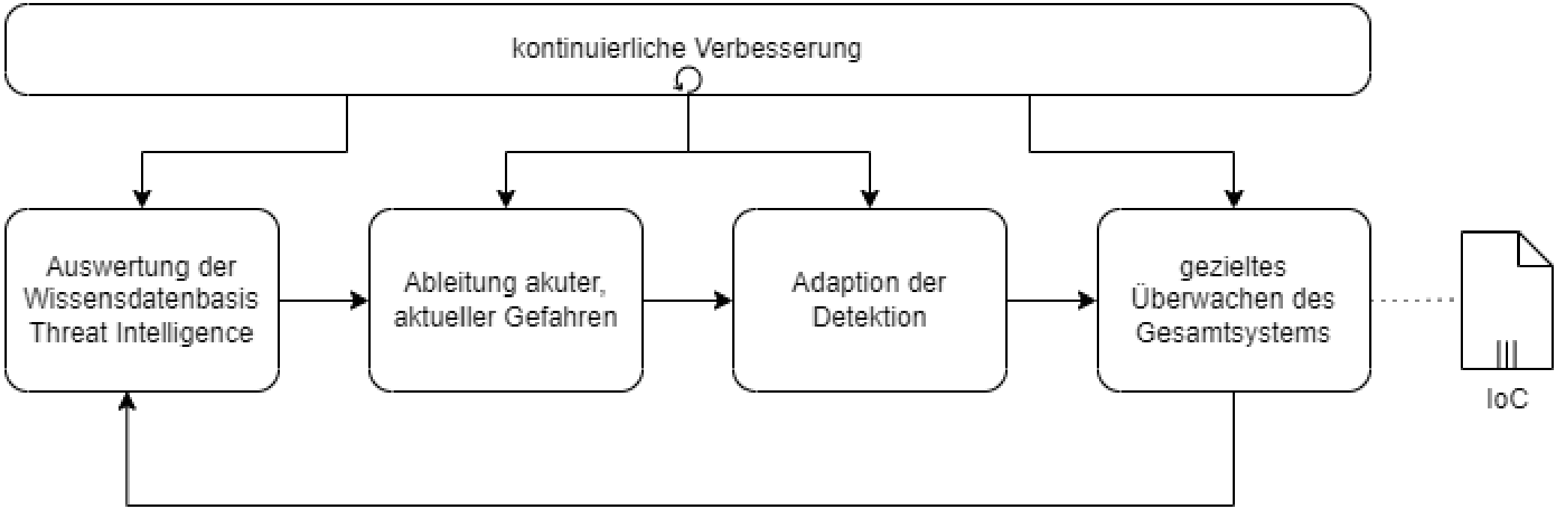


Agenda

- Motivation
- Systeme zur Angriffserkennung
- Threat Intelligence
- DFIR
- Konzept
- Evaluierung
- Zusammenfassung und Ausblick

Konzept

Adaptive Detektion von CTI-bekannten Bedrohungen

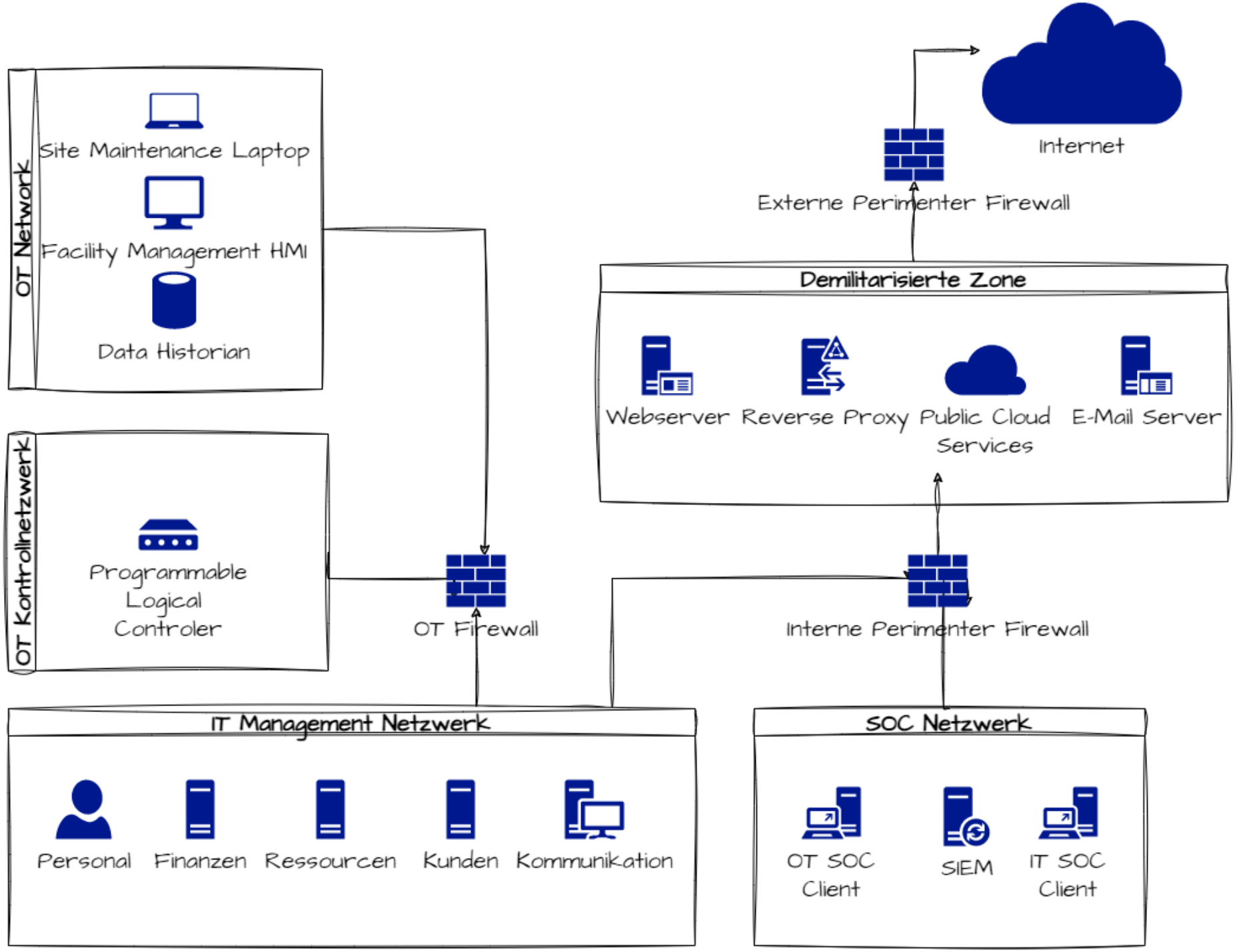


Agenda

- Motivation
- Systeme zur Angriffserkennung
- Threat Intelligence
- DFIR
- Konzept
- Evaluierung
- Zusammenfassung und Ausblick

Evaluierung

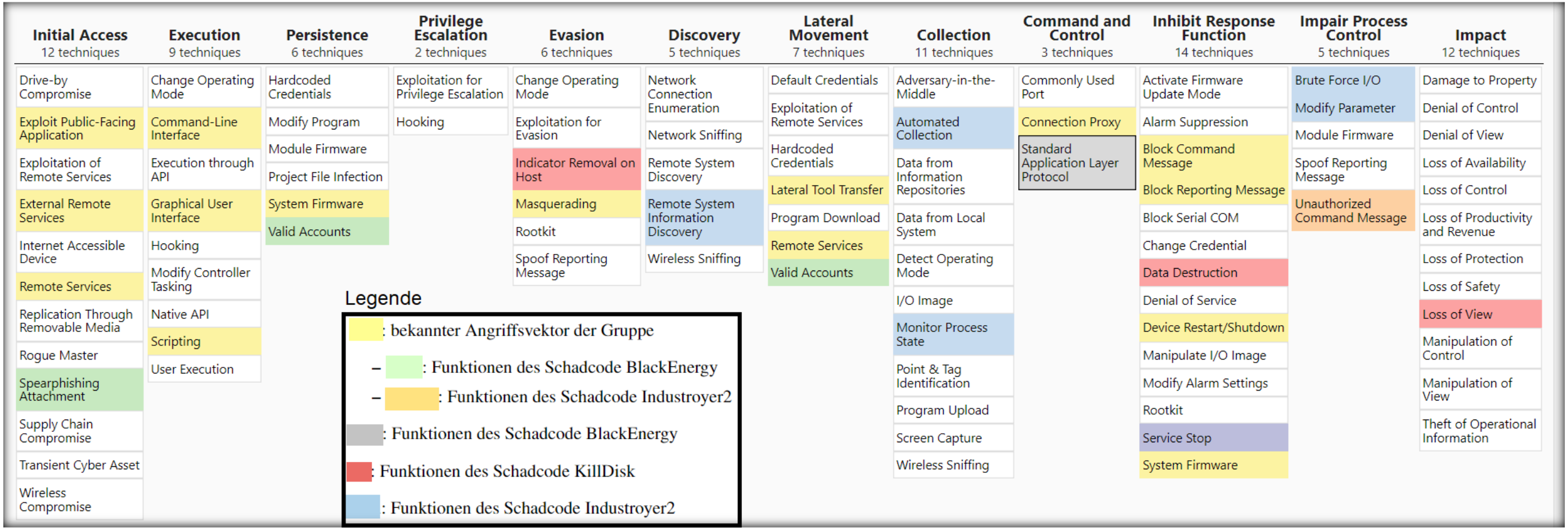
Scope der Testumgebung



Quelle:
Einer AIT – Präsentation nachempfunden

Evaluierung

Auswahl des Angriffsvektors



Initial Access (12 techniques)	Execution (9 techniques)	Persistence (6 techniques)	Privilege Escalation (2 techniques)	Evasion (6 techniques)	Discovery (5 techniques)	Lateral Movement (7 techniques)	Collection (11 techniques)	Command and Control (3 techniques)	Inhibit Response Function (14 techniques)	Impair Process Control (5 techniques)	Impact (12 techniques)
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Scripting						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	User Execution						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise							Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

Legende

: bekannter Angriffsvektor der Gruppe

- : Funktionen des Schadcode BlackEnergy
- : Funktionen des Schadcode Industroyer2

: Funktionen des Schadcode BlackEnergy

: Funktionen des Schadcode KillDisk

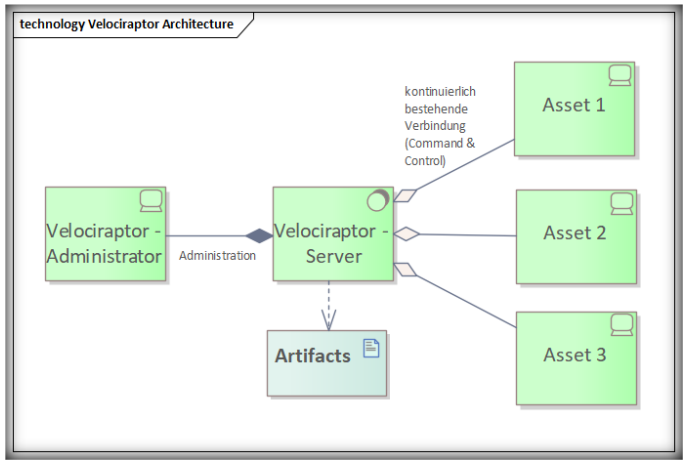
: Funktionen des Schadcode Industroyer2

Quelle: Internet
https://mitre-attack.github.io/attack-navigator/
aufgerufen am 25.01.2024

Evaluierung

Ansätze zur kontinuierlichen Überwachung IT/OT

Detektion des Droppers von Black Energy



ICS	T0865	Spearphishing Attachment

BlackEnergy targeted energy sector organizations in a wide reaching email spearphishing campaign. Adversaries utilized malicious Microsoft Word documents attachments. [6]

Quelle: Internet
https://attack.mitre.org/techniques/T0865/
aufgerufen am 25.01.2024

```
rule BlackEnergy
{
    meta:
        description = "Detects VBS Agent from BlackEnergy Report - file Dropbearrun.vbs"
        author = "Florian Roth"
        reference = "http://feedproxy.google.com/~r/eset/blog/~3/BXJbnGSvEFc/"
        date = "2016-01-03"
        hash = "b90f268b5e7f70af1687d9825c09df15908ad3a6978b328dc88f96143a64af0f"

    strings:
        $s0 = "WshShell.Run \"dropbear.exe -r rsa -d dss -a -p 6789\", 0, false" fullword ascii
        $s1 = "WshShell.CurrentDirectory = \"C:\\WINDOWS\\TEMP\\Dropbear\\\"" fullword ascii
        $s2 = "Set WshShell = CreateObject(\"WScript.Shell\")" fullword ascii /* Goodware String -
      occured 1 times */

    condition:
        filesize < 1KB and 2 of them
}
```

Listing 1: Yara-Regel zur Detektion der Dropper-Datei

```
LET Yararule = '''rule Name {...}'''
---------------------- File Detektion ---------------
LET Globs = 'C:/Users/**'

SELECT * FROM foreach(row={
   SELECT FullPath FROM glob(globs=Globs)
}, query={
   SELECT str(str=String.Data) As Hit,
   String.Offset As Offset,
   Filename FROM yara(accessor="file", files=FullPath, rules=Yararule)
})
LIMIT 50
```

Listing 2: VQL-Skript zur Ausführung der Yara-Regel

Evaluierung

Ansätze zur kontinuierlichen Überwachung IT/OT

Powershell-Kommandos

Home > Techniques > ICS > Scripting

Scripting

ID: T0853

Sub-techniques: No sub-techniques

ⓘ Tactic: Execution

ⓘ Platforms: None

Version: 1.0

Created: 21 May 2020

Last Modified: 13 October 2023

Quelle: Internet
https://attack.mitre.org/techniques/T0853/
aufgerufen am 25.01.2024

Detection

ID	Data Source	Data Component	Detects
DS0017	Command	Command Execution	Monitor command-line arguments for script execution and subsequent behavior. Actions may be related to network and system information Discovery, Collection, or other scriptable post-compromise behaviors and could be used as indicators of detection leading back to the source script. Scripts are likely to perform actions with various effects on a system that may generate events, depending on the types of monitoring used.

```
1 --Sichern der Powershell History
2 LET GLOBS='C:/Users/*/AppData/Roaming/Microsoft/Windows/PowerShell
      /PSReadLine'
3 SELECT * FROM foreach(
4     row={SELECT * FROM glob(globs=GLOBS)},
5     query={SELECT read_file(filename=FullPath+format(format="%v",
      args="/ConsoleHost_history.txt"), accessor="file") FROM scope
      ()}
6     )
7 ------ alternativ (mit Artefakt):
8 SELECT Stat.Atime AS Time, LineNum, Line, Username, Fqdn
9 FROM source(artifact="Windows.System.Powershell.PSReadLine")
```

Listing 8: Auslesen der Powershell History

Evaluierung

Ansätze zur kontinuierlichen Überwachung IT/OT

Überwachen der Remote Services

Home > Techniques > ICS > Remote Services

Remote Services

Adversaries may leverage remote services to move between assets and network segments. These services are often used to allow operators to interact with systems remotely within the network, some examples are RDP, SMB, SSH, and other similar mechanisms. [1] [2] [3]

Quelle: Internet
https://attack.mitre.org/techniques/T0886/
aufgerufen am 25.01.2024

```
1 SELECT *
2 FROM source(artifact="Linux.Syslog.SSHLogin")
3 WHERE Method =~ "pass"
4 AND result =~ "Accept"
```

Listing 10: Herausfilterung aller SSH Logins mit Passwort

Evaluierung

Simulation eines Programmable Logical Controlers

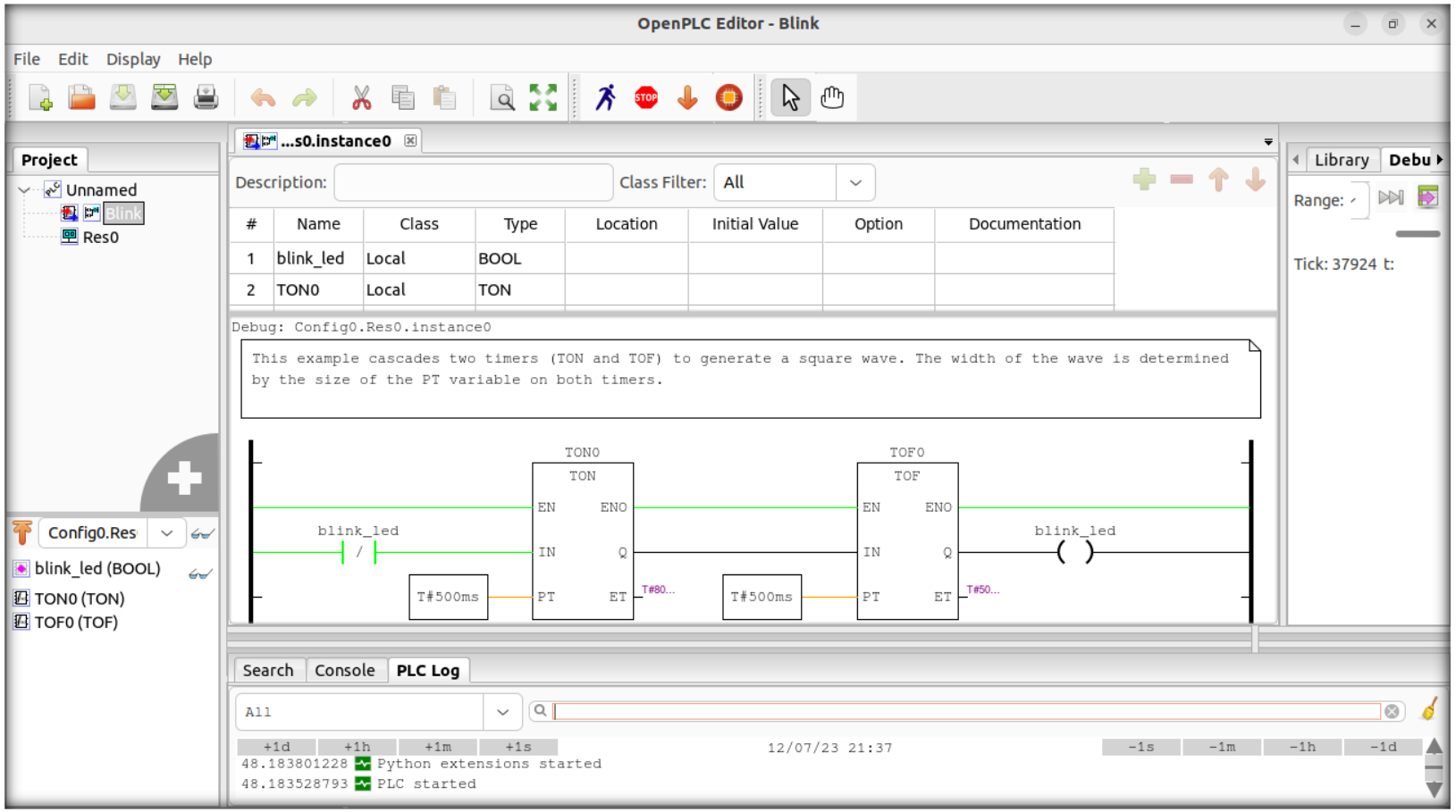
OPENPLC

TO A MORE
OPEN FUTURE

EDITOR RUNTIME

Quelle: Internet
https://autonomylogic.com/
aufgerufen am 25.01.2024

```
22 PROGRAM program0
23   VAR
24     In1 : BOOL := FALSE;
25     Out1 : BOOL := FALSE;
26   END_VAR
```



Evaluierung

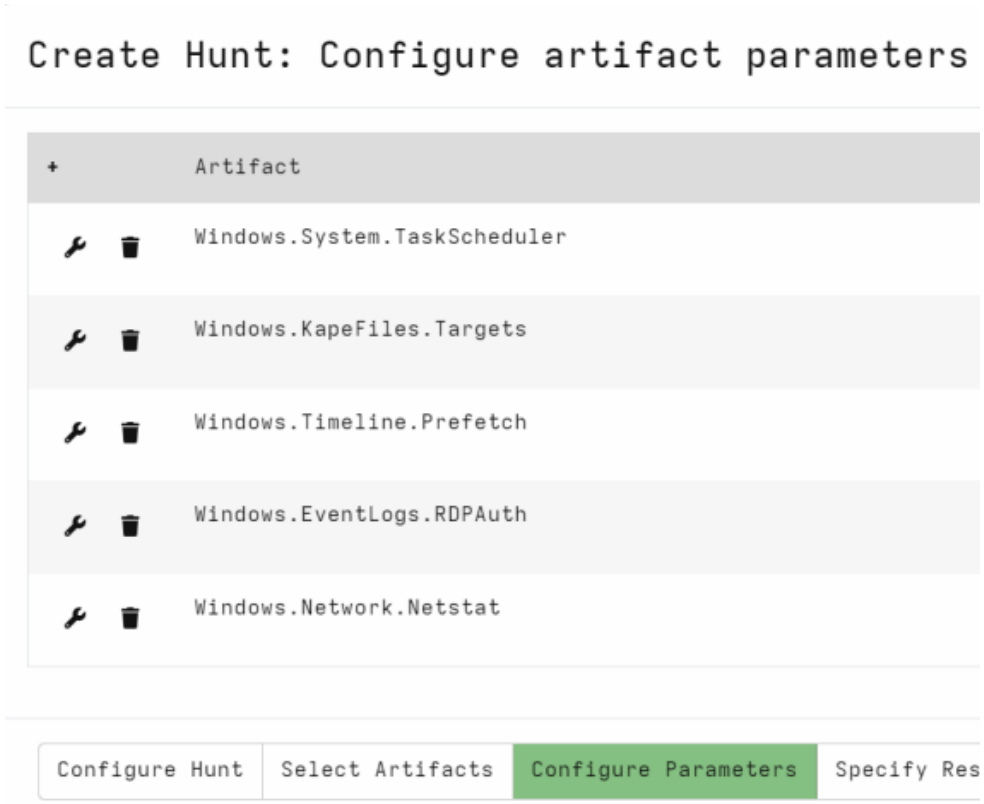
Agriffstechniken des Sandworm-Teams gegen PLC

Tabelle 1: Angriffe gegen die konkrete PLC-Implementierung

Id	Technique	Angriffspunkte	Detektion
T0803	Block Command Message	Eingangssignal an In1	Überwachen des Logfiles auf Stillstand im Betrieb, Monitoring des Netzwerks auf Fehlermeldungen bei der Zustellung von Daten an den PLC
T0804	Block Report Message	Ausgangssignal an Out1	Vergleichen der Logfile Einträge mit gemessenen Ausgangsdaten
T0816	Device Restart/ Shutdown	Laufzeitumgebung (runtime) des PLC	Überwachen des Logfiles auf Beenden und Neustart der PLC-Instanz
T0857	System Firmware	Codebasis der PLC Instanz	Überprüfen der Integrität der Bestandteile der Codebasis

Evaluierung

Adaption der Angriffstechniken gegen PLC




```
--Erzeugen und Vergleichen des Hashwertes des ST-
/* - festlegen der Datei mit ST Quellcode */
LET Datei = '/**/PLC/plc.st'
/* - einlesen des originalen Hashwerts H1 */
LET H1 = '440e20fe034d799af09e029fdab27858'
/* - berechnen Hashwerts H2 und davon MD5-Hash H3 */
LET H2 = SELECT hash(path=FullPath).MD5 AS Hash
FROM glob(globs=Datei)
LET H3 = H2[0].Hash
/* - vergleichen der Hashwerte und loggen des Ergebnis */
SELECT * FROM if(condition=(H1=H3),
  then={
    SELECT H1,H3 FROM scope()
    WHERE log(message='OK: %v sind gleich %v', args=[H1,H3])
  },
  else={
    SELECT H1,H3 FROM scope()
    WHERE log(message='Fehler: %v weichen ab %v', args=[H1,H3])
  })
```

Listing 5: VQL-Skript zur Überprüfung der Integrität der Codebasis

T0857	System Firmware	Codebasis der PLC Instanz	Überprüfen der Integrität der Bestandteile der Codebasis

Agenda

- Motivation
- Systeme zur Angriffserkennung
- Threat Intelligence
- DFIR
- Konzept
- Evaluierung
- Zusammenfassung und Ausblick

Zusammenfassung und Ausblick

Adaptive Detektion von CTI-bekannten Bedrohungen

Zusammenfassung:

- Einbeziehung der Cyber Threat Intelligence
- Deutliche Flexibilisierung gegenüber aktuellen Cyber-Bedrohungen
- Verschiebung des Fokus in der Cyber-Defense
- Adaption des Verfahrens für die operative IT-Sicherheit

Ausblick:

- Weitere Angriffsvektoren
- Automatisierung

Vielen Dank für Ihre Aufmerksamkeit

Fragen?

Glossar

- ATT&CK Adversarial Tactics, Techniques and Common Knowledge
- CTI Cyber Threat Intelligence
- DFIR Digital Forensics and Incident Response
- DMZ Demilitarisierte Zone
- ICS Industry Control Systems