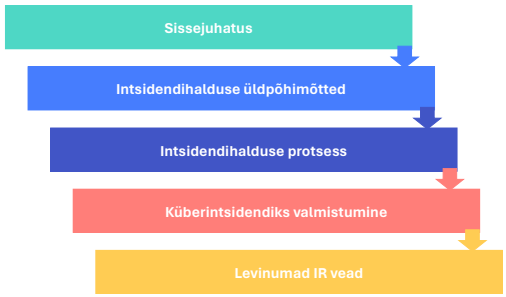
OIXIO Cyber

Küberintsidentideks valmistumine

Livio Nimmer | livio.nimmer@oixio.eu
CHFI | CEH | CND | CSA | ECIH | RESILIA | CCSK | ITIL
09.01.2026



Andmete omadused

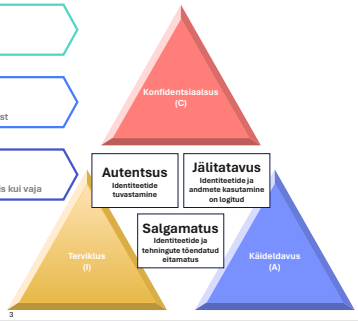
C Konfidentsiaalsus
Andmed on hoitud privaatsena ja kaitstuna

I Terviklus
Andmed on kaitstud volitamata muutmise eest

A Käideldavus
Andmed on kättesaadavad neile kel vaja ja siis kui vaja

Andmete äriline väärtus

- Isikuandmed
- Intellektuaalomand
- Ärisaladus



Intsidendi mõiste

- **Intsident – tõeline või arvatav, soovimatu või ootamatu, loomult kuritegelik või mitte, infoturvarike või sündmus või nende sari, mis võib kahjustada äritegevust või ähvardada teabe turvalisust. Intsident on näiteks:**
  - Süsteemi või süsteemide nakatumine luna- või pahavaraga
  - Süsteemi volitamata kasutamine
  - Teenusetõkestusrünnak
  - Veebilehe näostamine
  - Andmete vargus

Intsidendi mõiste

- **Ohumärgid – viitavad, et intsident võib toimuda tulevikus**
  - Süsteemide skaneerimisele viitavad logikanded
  - Vestlused tumeveebi foorumites
  - Uute turvanõrkuste avalikuks saamine

Intsidendi mõiste

- **Indikaatorid – viitavad, et intsident on toimumas või toimunud**
  - Kasutajate pöördumised
  - Süsteemide ebatavaline käitumine (suurenenud ressursikasutus, ebastabiilsus)
  - Suurenenud võrguliikluse mahud
  - Kahtlased võrguühendused
  - Tulemüüri sessioonitabeli täitumine
  - jne

Intsidendi mõiste

- **Indikaatorid – viitavad, et intsident on toimumas või toimunud**
  - Kasutajate pöördumised
  - Süsteemide ebatavaline käitumine (suurenenud ressursikasutus, ebastabiilsus)
  - Suurenenud võrguliikluse mahud
  - Kahtlased võrguühendused
  - Tulemüüri sessioonitabeli täitumine
  - jne

Rünne

Rünne = motivatsioon (eesmärk) + meetod + nõrkus

Ründed haridusasutuste vastu

- **Globaalne trend – rünnakute hulk suureneb**
  - Kolmas enim rünnatud valdkond 2024 aastal
- **Ajastatud ründed**
  - Kooli algus ja lõpp
  - Vaheajad
- **Õngitsusründed, lunavara, teenusetõkestusründed**

Oht ja ohusubjekt (Threat Actor)

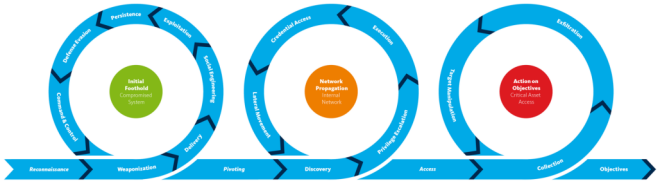
Oht	Ohusubjekt (Threat Actor)
Soovimatu sündmuse võimalik esinemine, mis võib kahjustada organisatsiooni tegevust	● Skriptinagad (script kiddies) ● Kinnisründeoht (APT - Advanced Persistent Threat) ● Häktivism ● Siseringioht (insider threat)

Kahjud

Intsidendi kulu koosneb otsestest ja kaudsetest kahjudest

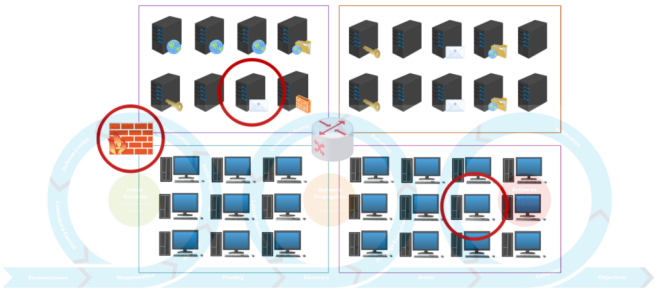
Otsesed	Kaudsed
● Tegevusseisak ● Rahaline kahju (näiteks lunaraha maksmine) ● Juriidilised ja seadusandlikud probleemid (NIS2, GDPR trahvid) ● Intsidendi menetluse kulud	● Andmete konfidentsiaalsuse, tervikluse ja käideldavuse kadu ● Mainekahju ● Klientide usalduse kadu

Tapuahel (Kill Chain)



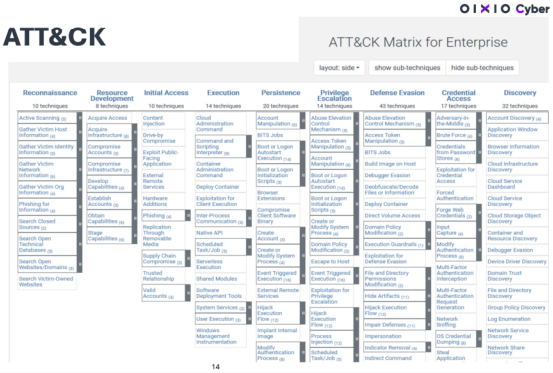
https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf

Tapuahel (Kill Chain)



13

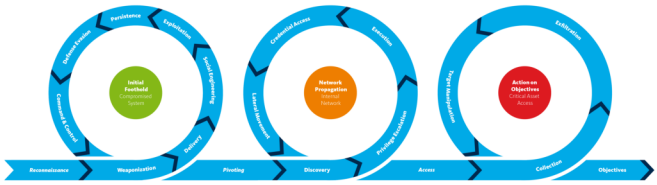
Mitre ATT&CK



https://attack.mitre.org/

14

15



ÕNGITSEMINE | KONTOD | TURVANÕRKUSED

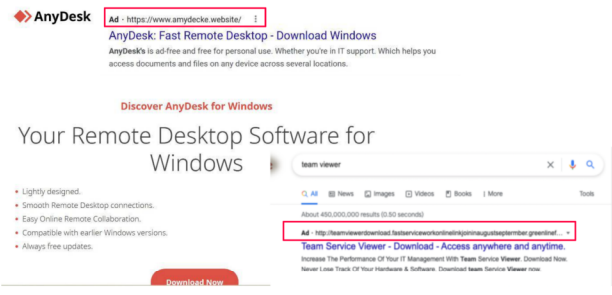
TARNEAHELARÜNDED + AI

16

Tehnikad: AI

17

Tehnikad: SEO mürgitamine ja malvertising

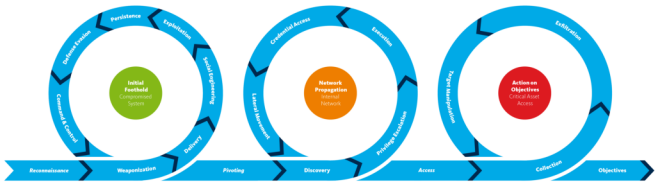


18

Tehnikad: LOTS

Living off Trusted Sites
https://lots-project.com

Legitiimsed	Kahtlased
Github / Bitbucket jne Onedrive / Google Drive / Dropbox jne Telegram / Discord / Twitter / Instagram / Facebook jne	pastebin.com anonfiles.com send.exploit.in ufile.io sendspace.com anonymfiles.com file.io



POWERSHELL | CMD | WMI | CLR

Powershell

- Logimine pole vaikimisi aktiivne
  - Powershell Core – eraldi logimine
- Funktsionaalsus:
  - Käivitada käsuridasid
  - Vältida avastamist (AMSI bypass jne)
  - Peita pahatahtliku tegevust
  - Käivitada teisi protsesse
  - Tirida teistest süsteemidest faile ning neid käivitada
  - Koguda süsteemiinfot
  - Muuta süsteemi konfiguratsiooni

SILENTTRINITY
COVENANT
PoshC2
https://howto.thec2matrix.com/
COBALTSTRIKE

Powershell

- Laialdaselt kasutusel legitiimsetes rakendustes (süstemihaldus, seire, turvanõrkuste haldus)
- Laialdaselt kasutusel administratiivsetes tegevustes
- Powershell without powershell ründed
  - Powershell ≠ powershell.exe
    - PS Core – pswh.exe
  - System.Management.Automation.dll
  - NoPowershell: Rundll32 C:\Users\Public\NoPowerShell.dll,main

Command Interpreter (cmd.exe)

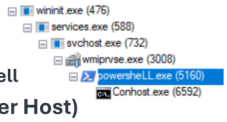
- Peita pahatahtliku tegevust
- Koguda süsteemi infot
- Muuta süsteemide parameetreid
- Kävitada rakendusi
- Minna mööda turvapoliitikatest
- Võimalik käivitada läbi teenuse, ajastatud tegumi, Startup kausta, WMI, Powershelli, IIS-i jne

Command Interpreter (cmd.exe)

cmd /c powershell.exe -exec bypass -file 1.ps1
cmd.exe /c C: & cd\ & cd "" & net use \\<ip> /u:<domain>\<username> <password>
cmd.exe /c C: & cd\ & cd "" & wmic /node:<ip> /user:<domain>\<username> /password:<password> process call create "<command>"
$system32\cmd.exe /C tasklist /svc | findstr lsass
cmd.exe /C systeminfo
cmd.exe /C net view \\HOST X
cmd /c sc.exe create "server power" binpath= "C:\Windows\system32\cmd.exe /c start C:\Windows\Help\help\MEUpdate.exe" & sc.exe start "server power"
cmd.exe /c for /F \"tokens=*\" %1 in ('wevtutil.exe el') DO wevtutil.exe cl \"%1\

Windows Management Instrumentation

- Klient-server lahendus
  - Klient: wmic.exe
    - Võib olla ka läbi DLL-i nagu Powershell
  - Server: wmiprvse.exe (WMI Provider Host)
    - Alam-protsess: cmd.exe, powershell.exe vms
- Väga palju süsteemihaldusrakendusi kasutab
- Administraatorid kasutavad
- Windows 11 järgmisest aastast vaikimisi keelatud



WMI

- Kontrollitakse, mis viirusetõrje masinas
- Lülitatakse tulemüür või viirusetõrje välja
- Süsteemi info kogumine, kasutajate ja gruppide kaardistamine
- Varukoopiate kustutamine
- Tegevused korraga paljude failidega
- Pahavara käivitamine süsteemides

IT kaughaldustööriistade kasutamine

- Anydesk
- Teamviewer
- Screenconnect
- Netsupport Manager
- Remcos
- Splashtop
- Atera
- UltraVNC / TightVNC

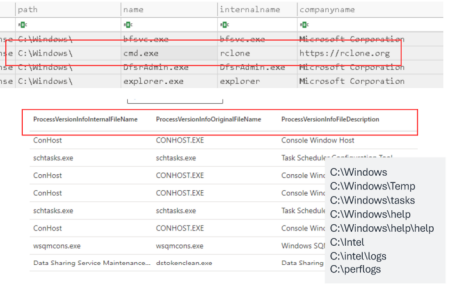
Tehnikad: LOLBins

Living Off the Land Binaries - https://lolbas-project.github.io

- arp.exe
- ping.exe
- netstat.exe
- reg.exe
- schtasks.exe
- sc.exe
- wmic.exe
- rundll32.exe
- msbuild.exe
- wscript.exe
- csrcipt.exe
- mshata.exe
- bitsadmin.exe
- utilman.exe
- regsvr32.exe
- msiexec.exe
- certutil.exe
- net.exe

Rakenduste ümbernimetamine

- Rundll32.exe
- Certutil.exe
- Msbuild.exe
- Psexec.exe
- Rclone.exe
- Winrar.exe
- 7zip.exe



Viirusetõrje vältimine

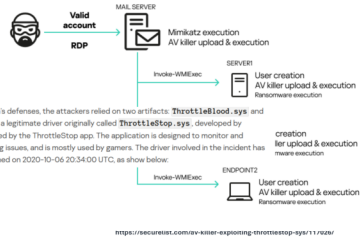
- Kliendispetsiifiline pahavara
- Signatuurid puuduvad
- Sogastamine
- Süstimis- ja õnnestusründed, kestakoodi laadimine
- Mäluresidentne pahavara
- Python, Rust, Go & .NET Framework JIT

OIXIO Cyber

Viirusetõrje neutraliseerimine

Living Off The Land Drivers - https://www.loldrivers.io

- EDRKiller
- Avkiller
- Backstab
- Aukill
- Terminator

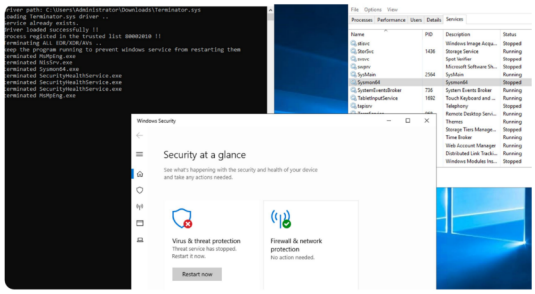


Logpoint - EDR Killers - After All EDRs Are Not Invincible.pdf

https://securelist.com/av-killer-exploiting-throttlestop-sys/111026/

OIXIO Cyber

Viirusetõrje neutraliseerimine



Logpoint - EDR Killers - After All EDRs Are Not Invincible.pdf

OIXIO Cyber

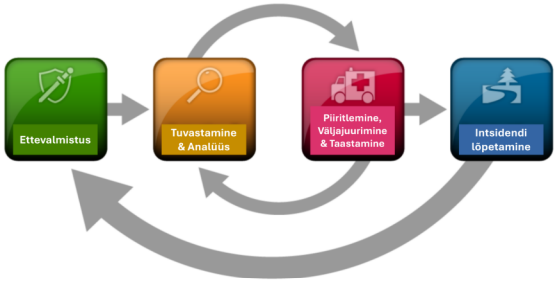
Intsidendihaldus

Intsidendihaldus on selgelt defineeritud protseduuride kogum intsidentide käsitlemiseks arvuti- ja võrgusüsteemides.

- Aidata organisatsioonil kiirelt ja efektiivselt ning minimaalsete kahjudega taastada süsteemide talituspidevus
- Minimeerida võimalikud kahjud, mis võivad tekkida andmete vargusest või kaost ning kriitiliste süsteemide talituspidevuse katkemisest
- Viia ellu süstemaatiline vastutegevus järgides valdkonna parimaid praktikaid
- Vältida sarnaste intsidentide kordumist tulevikus
- Aidata organisatsioonil tasakaalustada turbenõudeid finantskulutustega
- Täita regulatiivseid nõudeid (NIS2, EITS, GDPR, ISO vms)

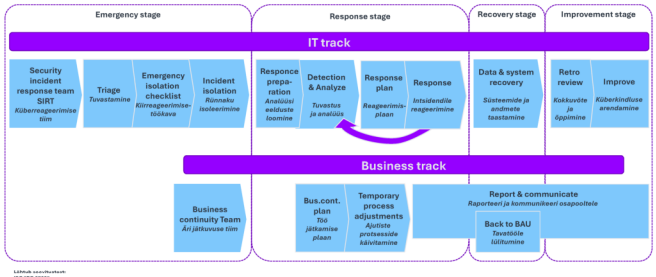
OIXIO Cyber

Intsidentide käsitlemise protsess



OIXIO Cyber

Intsidendi lahendamise protsess - PICERL



OIXIO Cyber

Regulatsioonid ja standardid

NIST

NIST SP800-61R3

Incident Response Recommendations and Considerations for Cybersecurity Risk Management

E-ITS

E-ITS - DER. Avastamine ja reageerimine

ISO

ISO 27035

Information Security Incident Management

DER. Avastamine ja reageerimine

- DER.1: Turvaintsidentide avastamine
- DER.2: Turvaintsidentide haldus
- DER.2.1: Turvaintsidentide käsitlus
- DER.2.2: IT-kriminalistika võimaldamine
- DER.2.3: Ulatuslike turvaintsidentide lahendamine

Üldpõhimõtted I

- Intsidendi lahendamise käigus tuleb arvestada organisatsiooni väärtusahela kaitset. Intsidendi lahendamise eesmärgiks on esmajoones vältida ründe levimist ärikriitilistesse süsteemidesse või ärikriitiliste süsteemide talituspidevuse taastamine. Ärikriitiliste teenuste sulgemine tuleb viia läbi kaalutletult ning kooskõlastatult ettevõtte juhtkonnaga.
- Intsidendi kommunikatsioon väliste osapooltega peab olema kaalutletud ning kooskõlastatud organisatsiooni kommunikatsioonijuhiga.
- Lisaks intsidendi mõju kiirele piiritlemisele, on esmajärjekorras oluline teha kindlaks võimalik andmeleke ning selle ulatus, kuna andmete lekkimine võib põhjustada organisatsioonile märkimisväärseid kahjusid.
- Intsidendi lahendamise käigus tuleb selgitada välja intsidendi algpõhjus, et vältida edaspidiseid rünnakuid.

Üldpõhimõtted II

- Enne intsidendi lahendamise tegevustega alustamist lepitakse kokku muudatuste halduse viisis. Minimaalselt luuakse jagatud tabel, kuhu kõik märgivad iga tegevuse ja süsteemides tehtava muudatuse. Tabel peab sisaldama järgmist: kuupäev ja kellaaeg; süsteemi nimi ja IP, milles muudatus tehti, tegija nimi, muudatuse eesmärk.
- Kõik intsidendiga seotud kompromiteerimise indikaatorid dokumenteeritakse ühtsesse andmebaasi, milleks võib olla minimaalselt Exceli tabel (Table of Doom). TOD sisaldab intsidendi üldist ajajoont ning kõiki tuvastatud ründe indikaatoreid.
- Töökohaarvutite analüüsimisel tuleb jälgida andmekaitse põhimõtteid ning tagada kasutajate ootus privaatsusele. Uurimisel tuleb keskenduda meta-andmetele. Intsidendiga mitteseotud andmeid ja infot ei edastata tööandjale.
- Kui ründe ulatus pole teada, siis suhtlemiseks ei kasutata asutuse taristus olevaid süsteeme, kuna need võivad olla ründaja kontrolli all.

Protsess: Ettevalmistus

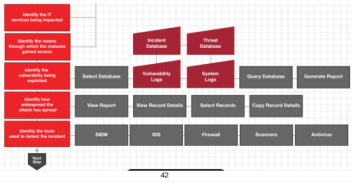
- **Intsidendi eduka lahendamise eelduseks on korralik ettevalmistus. Ettevalmistus hõlmab:**
  - Intsidendihalduse poliitika ja plaani väljatöötamist
  - Intsidendihalduse protseduuride väljatöötamist
  - Intsidendihalduse töövahendite ettevalmistust, testimist ning koolitusi
  - Ennetavate ja tuvastavate tehnoloogiate juurutamist.

Protsess: Ettevalmistus

https://github.com/swannman/ircapabilities/blob/master/README.md

Intsidentide käsitlemise plaan

- Joondatud asutuse infoturvapoliitikaga
- Testitud õppuste käigus
- Joondatud asutuse tegevuskeskkonna, riskide, kriisiplaanidega
- Sisaldab standardtegevusi ning mänguplaane (playbooks)



OIXIO Cyber

Esmaregeerija tööriistakomplekt

- Tarkvara asitõendite kogumiseks
- Kaablid ja tühjad andmekandjad
- Esmareageerija juhend
- Mänguplaanid (playbooks)

OIXIO Cyber

Tehnoloogiad ja dokumentatsioon

- Logiserver / SIEM koos analüütikareeglitega, et koguda ja edastada logisid
- IDS/IPS/NDR koos vajaliku riistvaraga
- Puhtad süsteemitõmmised (kuldpildid) ning tarkvara tõmmiste masspaigalduseks
- Lühiteatmelehed (spikrid) töövahendite kasutamiseks
- Kommunikatsiooniplaanid ja juhised intsidendi ajal suhtluse korraldamiseks
- Intsidendi dokumentatsiooni põhjad
- Juhtkonna aruande põhi
- Pressiteate põhi
- Arhitektuuri ja võrguskeemid

OIXIO Cyber

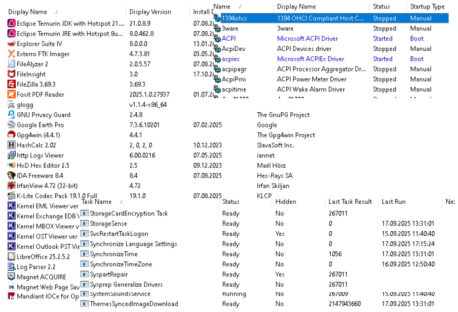
Varad

- Protsessid (ITIL)
  - Varade haldus
  - Konfiguratsioonihaldus
- Tehnoloogiad
  - Varade haldustarkvara
    - Aktiivne ja passivne tuvastamine
      - Kattuvus
    - Tarkvara inventuur
    - Konfide võrdlus
    - Üle süsteemide päringime
      - Või EDR/OsQuery?
    - Aruandlus ja andmete eksport

OIXIO Cyber

Kuldtõmmised

- Tarkvarad
- Protsessid
- Teenused
- Ajastatud tegumid
- Ohjurid



OIXIO Cyber

Tehnoloogiad

SIEM
Security Onion
Wazuh
ELK
QRadar
Graylog

NDR/IDS
Security Onion
Zeek
Suricata
ClearNDR

EDR
Sysmon
Security Onion
Wazuh
OpenEDR

+ TURVALISED BAASSÄTTED

OIXIO Cyber

Klientseadmete kaitse

OPS.1.1.4: Kaitse kahjurprogrammide eest

Põhifunktsionaalsus

- Ennetus- ja tuvastusvõimekus
- Platvormide tugi (Win, Linux, OSX, serverid, mobiilseadmed)
- Kasutajaliides ja administreerimise lihtsus
- Ressursikasutus
- Hind (omamise kogukulu)

Lisafunktsionaalsus

- Rakenduste käivituskontroll
- Turvanõrkuste haldus
- Turvapaikade haldus
- Mobiilseadmete haldus
- EDR
- Logihaldus

OIXIO Cyber

Sysmon

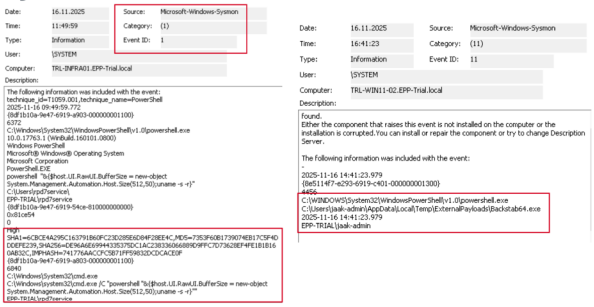
Tasuta lahendus klientseadmete telemeetria kogumiseks Windows platvormidel
Sysmon for Linux
https://github.com/microsoft/SysmonForLinux

Põhjalik telemeetria
Protsessilogid, ohjurite ja teekide laadimise logid, failide loomise ja kustutamise logid, võrguühenduste logid, registri logid

Vajab põhjalikku seadistamist
Sysmon Modular, Sysmon Configuration Builder jne
https://github.com/olafhartong/sysmon-modular
https://github.com/bananagobananza/SysmonConfigurationBuilder

OIXIO Cyber

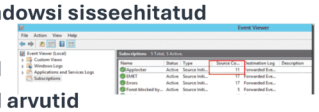
Sysmon

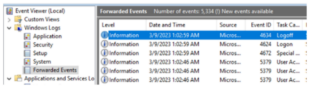


OIXIO Cyber

Windows Event Forwarding

- Logide keskne kogumine Windowsi sisseehitatud vahenditega
- Toetatud push/pull meetodid
- Domeenis ja domeenivälised arvutid
- Autentimine, krüpteeritud ühendused
- Logide filtreerimine
  - Supercharger
    - https://www.logbinder.com/windowseventcollector/
  - Palantir WEC Subscriptions
    - https://github.com/palantir/windows-event-forwarding





OIXIO Cyber

Security Onion

Võrguanalüüs

Signatuuri- ja anomaaliapõhine ründetuvastus (IDS)

Klientseadmete telemeetria (EDR)

Logihaldus

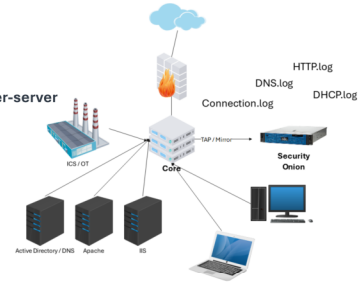
Juhtumihaldus

Pettus (deception honeypot)

OIXIO Cyber

Kasutusjuhud: võrguseire

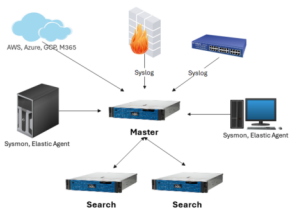
- Keskne võrgulogi
  - HTTP, DNS, DHCP, SMB, RDP jne
  - Zeek Connection.log
    - Flow-laadne aga detailsem
  - Klient-klient, klient-server, server-server liiklus
- PCAP analüüs
- Signatuuripõhine IDS
- SSL/TLS profileerimine
- ICS protokollide tugi
  - DNP3, P7, BACNet, Modbus jne
- CommunityID



OIXIO Cyber

Kasutusjuhud: logihaldus

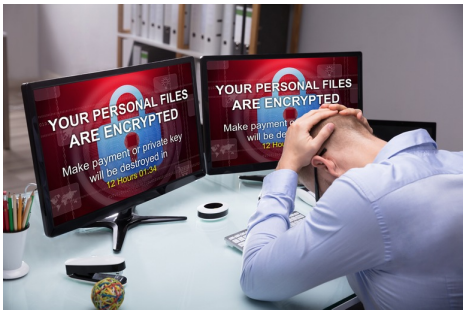
- Tsentraliseeritud logimine
- Windows, Linux, OSX
  - Sysmon, Elastic Agent
- Võrguseadmed
  - Syslog
  - Fortigate, Checkpoint, Cisco jne
- Pilveteenused
  - Azure, AWS, GCP, M365 jne
- Valmis 200+ integratsiooni



Paigaldus

- Paindlik
  - Virtuaalmasinad, enda riistvara, SOS riistvara
  - Andmekeskus ja pilv
- Skaleeruv
  - Üksikust serverist kuni jaotatud arhitektuurini, mis on võimeline toetama 100k+ klientseadmega võrke
- TAP / Mirror

Protsess: Tuvastamine



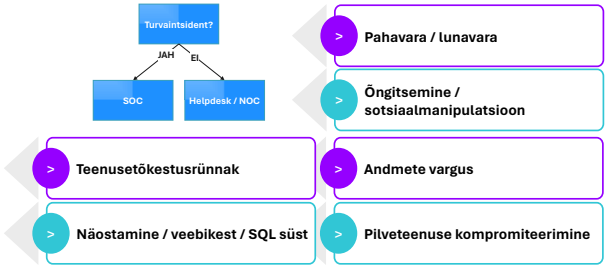
Protsess: Tuvastamine

- Tuvastamise faasis saab organisatsioon teadlikuks sündmustest, mis viitavad intsidendile. Tuvastamise faasis on oluline saada võimalikult palju infot selle kohta, mis juhtus. Teostatakse esmane triaaž ja intsidendi klassifitseerimine.

Protsess: Tuvastamine

- Sündmused, mis osutavad võimalikule intsidendile:
  - SIEM või logisüsteemi teavitus;
  - Viirusetõrje teavitus kahtlasest failist;
  - Lõppkasutaja pöördumine;
  - Välise osapoole (CERT Eesti või interneti teenusepakkuja) pöördumine;
  - Lunaraha nõue arvutis või arvutites;
  - Jne.
- Kas tegemist on intsidendiga või mitte pole alati koheselt selge

Protsess: Tuvastamine



Protsess: Tuvastamine

- Kui palju süsteeme mõjutatud?
- Kas kriitilised süsteemid mõjutatud?
- Kas kriitilised andmed on mõjutatud?
- Kas on mõju organisatsiooni talituspidevusele?
- Kas kaasneb SLA-de või seaduse rikkumine?
- Mis tüüpi ründega on tegu?

- Üks kriitiline süsteem > mitu ebaolulist.

Meeskond

Intsidendi juht – igale intsidendile määratakse intsidendi juht tagamaks intsidendi organiseeritud ja koordineeritud lahendamine.

Tehniline

- Turvaanalüütikud
- Süsteemiadministraatorid
- IT tugipersonal
- Turbeinsenerid
- Küberkriminalistika ekspert

Äri

- Juhtkonna esindaja
- Infoturbejuht
- Jurist
- Kommunikatsioonijuht
- Personalijuht

Protsess: Analüüs

- Analüüsi faasis kogutakse vajalikud asitõendid intsidendi edasiseks lahendamiseks. Eesmärgiks on tuvastada intsidendi võimalik ulatus ja mõju ning leida intsidendi toimumise juurpõhjus
- Analüüsi faas peab olema teostatud piisava põhjalikkusega enne intsidendi käsitlemise järgmisse faasi minekut
- Analüüsi faas peab olema teostatud piisava põhjalikkusega enne intsidendi käsitlemise järgmisse faasi minekut

Protsess: Analüüs

- Analüüsitakse süsteemide logisid
- Vajadusel seadistatakse logiserver või täiendatakse logianalüütikat ning suurendatakse logide detailsust olemasolevates süsteemides
- Vajadusel paigaldatakse võrguanalüüsi lahendus (NDR/XDR) et tuvastada võimalik külgliikumine ja juhtserverite liiklus
- Tehakse süsteemidest ekspertiistõmmised
- Kogutakse esmased ründeindikaatorid
- Kogutakse ründe kohta ohuteadmust kinnistest ja avalikest kanalitest
- Alustatakse intsidendi põhjalikuma dokumenteerimisega (lahendamise käik alates analüüsist kuni intsidendi lõpetamiseni)

Esmaregeerija

- Esimene inimene, kes alustab intsidendiga tegelemist
  - IT spetsialist
  - Süsteemiadministraator
- Kindlustab sündmuspaiga
- Tagab asitõndite puutumatuse

Esmaregeerija põhimõtted

- Ära satu paanikasse
- Tegutse tervemõistuslikult vastavalt olukorrale
- Kogu esmane informatsioon juhtunu kohta

Esmaregeerija põhimõtted

- Kellaaeg ja ajavöönd kirja!
- Kui arvuti on sees, siis ära lülita seda välja ja kui arvuti on väljas, siis ära lülita seda sisse!
  - Eemalda võrgukaabel
  - Väljalülitamisel juhe seinast
- Kui on vaja süsteemis, midagi teha, siis dokumenteeri kõik tegevused (nt telefoniga pildistades, filmides)
- Vajadusel teavita infoturbejuhti, juhtkonda või turvatiimi

Asitõendite volatiilsus

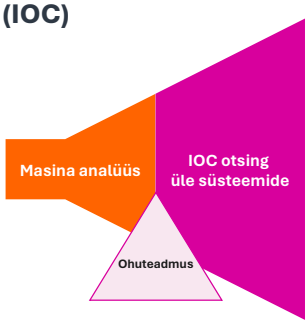
- Andmed kogutakse volatiilsuse järjekorras
  Volatiilsed andmed kaovad süsteemi väljalülitamisel
- **Volatiilsed:** võrguühendused, käivitunud protsessid, vahemälu, avatud failid, DNS & Arp vahemälu, ühendatud võrgukaustad
- **Mittevolatiilsed:** kõvakettale salvestatud info, logid, pahavara, failid, register, kontod, ajastatud tegumid

Esmaregeerija tarkvara

- **Mälutõmmise tegemine**
  MagnetRESPONSE, Belkasoft RAM Capture, Winpmem
  https://www.magnetforensics.com/resources/magnet-response/
- **Triaažitõmmise tegemine**
  MagnetRESPONSE (Windows), Catscale (Linux)
  https://github.com/WithSecureLabs/LinuxCatScale
- **Kettatõmmise tegemine**
  FTK Imager (Windows), DD (Linux)
  https://www.exterro.com/ftk-product-downloads/ftk-imager-4-7-3-81

Ründeindikaatorid (IOC)

- IP aadress
  193.40.120.130
- URL
  http://server.xxx.com/malware.jpg
- Domeeninimi
  sjhdhdye.m1crosoft.com
- Failinimi
  pahavara.exe
- Räsi
  93847fgs37274hdj4556632ddffe3



Analüüsi metoodika

Analüüs I

- Käivitunud rakendused (process)
  - *Process Explorer, Process Hacker, Security Task Manager, Sysinspector*
  - *Get-Process, Get-Service*
- Käivitunud teenused (services)
- Rakenduste puu ja sõltuvussuhe
  - Kust fail on käivitunud
  - Failinimega manipuleerimine: svchost.exe vs scvhost.exe
- Rakenduste ja teenuste terviklus (kontroll räsi järgi)
- Paigaldatud tarkvara

Analüüs III

- Run Keys
  - *Autoruns*
- Aktiivsed pordid ja rakendused
  - *Netstat, TCPView, Get-NetTCPConnection*
- DNS Cache
  - *Ipconfig /displaydns, Get-DnsClientCache*
- Ühendused teiste süsteemidega
  - *Arp -a*
- Ajastatud tegumid (Scheduled Tasks)

Logide analüüs

- Viirusetõrje / EDR-i logid
- Süsteemilogid
  - C:\Windows\System32\winevt\logs
  - Autentimislogid
    - Ebatavalised sisselogimised
  - Powershell
  - Windowsi komponentide logid
- Windows Event Viewer, Eventlog Explorer, EventLog Expert, FullEventLogView, LogViewer
- Event ID 1102 – Audit Log Was Cleared

Pahavara käitlemine I

- Levinud kaustad, kust pahavara käivitub:
  - \Temp folders
  - \AppData
  - \ProgramData
  - \$Recycle.Bin
  - \Windows
  - \Windows\System32
  - \Windows\WinSxS
  - \System Volume Information
  - \Program Files ja \Program Files (x86)

Pahavara käitlemine II

- Pahavara käitlemist töökeskkonnas tuleb vältida
- Deaktiveeri pahavara läbi ümbernimetamise viirus.exe > viirus.bin
  Paki parooliga „infected”kaitstud ZIP faili
- Ära lae tundmatuid faile avalikesse liivakastidesse ja ohuteadmuse allikatesse, vaid otsi räsi järgi

Pahavara käitlemine III

- Enamus hästi kirjutatud pahavarast ei käivitu avalikes liivakastides
  - Vajalik staatiline analüüs ja pöördkonstrueerimine
- Räsi genereerimine
  - Get-Filehash
  - Hashmyfiles
- Viiruste kontroll: KVRT, Hitman, Getsusp, EEK

Ohuteamuse kasutamine

- Failid, URL-id
  - VirusTotal
  - Open Threat Intelligence Portal (OpenTIP)
  - Open Threat Exchange (OTX)
- Failid
  - Malware Bazaar
- Urlid
  - Urlscan
- Liivakastid: Any.RUN, Intenzer, CERT EE Cuckoo

Protsess: Ohjeldamine

- Ohjeldamise faasis viiakse läbi toimingud turvaintsidendi peatamiseks või mõju vähendamiseks. Iga intsidendi puhul töötatakse välja asjakohane ohjeldamise strateegia
- Ohjeldamise tegevused tuleks viia läbi võimalikult märkamatult ründaja jaoks
- Arvestada tuleb võimalusega, et ohjeldamise tegevused võivad põhjustada lisakahju, kui intsidendi tegelik ulatus pole piisavalt hästi teada. Eesmärk on piirata rünnak võimalikult väheste muutustega süsteemides

Protsess: Ohjeldamine

- Juhtserverite IP aadresside, DNS nimede blokeerimine
- Kommutaatorite portide väljalülitamine
- Nakatunud seadmete võrgukaabli lahti ühendamine
- Liikluse piiramine tulemüürireeglitega
- Liikluse kiiruse ja mahu piiramine
- Seadmete isoleerimine eraldi VLAN-idesse
- Kasutajakontode paroolide vahetamine või kontode keelamine
- Teenuste keelamine
- Turvanõrkuste paikamine
- Honeypotide ja Canarytokenide paigaldamine taristusse

Protsess: Ohjeldamine

- Ohjeldamise faasis on oluline arvestada intsidendi võimaliku mõju ning ulatusega. Ohjeldamise tegevused viiakse läbi vastavalt tajutavale riskitasemele. Ohjeldamise strateegia sõltub:
  - Võimalikust kahjust ning andmete varguse tõenäosusest
  - Vajadusest säilitada asitõendeid (süsteemide väljalülitamisel hävinevad lendandmed)
  - Teenuste käideldavuse nõuetest
  - Strateegia rakendamise ajast
  - Strateegia rakendamise ulatusest (osaline ohjeldamine, täielik ohjeldamine)
  - Ohjeldamise tegevuste ajalisest mõjust (ajutised muutused, püsimuutused)

Protsess: Väljajuurimine ja taastamine

- Pärast ohjeldusmeetmete rakendamist viiakse läbi tegevused ründaja süsteemidest väljaajamiseks
- Enne taastamistegevuste lõpule viimist tuleb veenduda, et ründe juurpõhjus on välja selgitatud
- Taastamine toimub lühikeses ja pikas perspektiivis – esmalt taastatakse kriitilised süsteemid ning tagatakse turbetaseme kiire tõstmine ning äri talituspidevuse jätkumine; seejärel tegeletakse süsteemiarhitektuuri probleemidega
- Konsulteeritakse äri talituspidevuse- ja taasteplaaniga ning viiakse neile vastavalt läbi taastetegevused

Protsess: Väljajuurimine ja taastamine

- Pahavara eemaldamine süsteemidest
- (Parema) viirusetõrje / EDR-i paigaldus
- Paroolide vahetus (sh Kerberose kontod)
- PAM lahenduse paigaldamine
- Uute domeenikontrollerite paigaldamine
- Andmete taastamine varukoopiatest
- Turvanõrkuste paikamine
- Kasutajaõiguste piiramine juurdepääsuloenditega

Protsess: Väljajuurimine ja taastamine

- Viiakse läbi kogu taristu turvanõrkuste kontroll, et välistada turvanõrkuste ärakasutamist ründaja poolt süsteemidesse tagasitulekuks
- Jälgitakse kasutajakontode kasutust, et välistada kontode väärkasutus ning tuvastada võimalikud kasutajakontod, mis võivad olla kompromiteeritud
- Viiakse läbi sõltumatu audit süsteemide tervikluse kontrollimiseks

Protsess: Intsidendi lõpetamine

- Intsidendi lõpetamise faasis viiakse läbi intsidendi järgsed tegevused nagu aruannete koostamine ning intsidendi lahenduse käigu reflektsioon
- Koostatakse juhtkonna aruanne ning põhjalikum tehniline aruanne
- Teostatakse intsidendi lahendamise analüüs – mis läks hästi ja mis ebaõnnestus või oleks võinud olla paremini korraldatud

Protsess: Intsidendi lõpetamine

- Aruanne peab vastama küsimustele:
  - Kes? - Kes olid intsidendiga seotud (kasutajad, uurijad);
  - Millal? - Intsidendi ja selle lahendamise ajatelg;
  - Kus? - Kus intsident toimus;
  - Mis? - Mis juhtus ja millised olid intsidendi lahendamise tegevused;
  - Miks? - Miks ründaja ning intsidendi lahendaja tegi mingeid tegevusi;
  - Kuidas? - Kuidas rünnak läbi viidi ning kuidas rakendati vastutegevusi.

Protsess: Intsidendi lõpetamine

- Mis tegelikult juhtus ja millal?
- Kuidas tuli meeskond intsidendi lahendamisega toime? Mis oleks võinud parem olla?
- Kas dokumentatsioon, protseduurid, töövahendid ja teadmised olid piisavad?
- Kas tegevuste prioriteedid olid õigesti seatud?
- Millisest informatsioonist puudu jäi?
- Kas intsidendi kommunikatsioon töötas?
- Mida oleks võinud teha teistmoodi?
- Mis segas intsidendi kiiret lahendamist?
- Palju kulus aega ning ressurssi intsidendi lahendamiseks?
- Kuidas parendada turvameetmeid, et tulevikus sarnaseid intsidente ära hoida?

Protsess: Intsidendi lõpetamine

Poliitikate ja protseduuride täiendamine

Raha küsimine!!!

Levinumad vead

- Rünnaku piiritlemine süsteemis enne, kui rünnaku ulatus on välja selgitatud
  - Volatiilsete asitõendite hävitamine
  - Vastutegevuse paljastamine – ründaja muudab oma taktikaid, tehnikaid, protseduure
- Ründaja taristu puutumine (pingimine, DNS päringud, traceroute vms)
- Avalike liivakastide kasutamine / failide laadimine VirusTotalisse

Levinumad vead

- Ründaja taristu ennatlik blokeerimine
- Ennatlik kontode blokeerimine või paroolide vahetus
- Logide rotatsiooniperioodiga mitte arvestamine
- Läbistatud taristu kasutamine IR tegevuste koordineerimiseks
- Juurpõhjuse välja selgitamata jätmine
- Viirusetõrje usaldamine

Kuidas õpetada?

- Sihtrühm: IT või küberturbespetsialist?
  - IT – rõhk ettevalmistusel
    - Esmareageerimine, tehnoloogiate juurutamine
  - Küberturbe spetsialist – rõhk prakilisel analüüsil
    - Masina analüüs, võrguliikluse analüüs
- Realistlik keskkond
  - Teha käsitsi
  - Adversary emulation
    - PurpleSharp, Atomic Red Team, Caldera
  - Harjutuskeskkonnad
    - Hackthebox, TryHackMe

Livio Nimmer
livio.nimmer@oixio.eu
LinkedIn:

OIXIO