
WITH®
secure
The European Flagship of Cyber Security

Toimitusketjun kyberturvallisuus

Kuka kantaa vastuun tietomurrosta ja
kuka maksaa lopullisen hinnan

Samuel Kuosa
Global Sales Engineer

WITH secure

NIS 2 Direktiivi, Art. 21(1) ja 21(2)(d)

1. Jäsenvaltioiden on varmistettava, että keskeiset ja tärkeät toimijat toteuttavat asianmukaisia ja oikeasuhtaisia **teknisiä, operatiivisia ja organisatorisia** toimenpiteitä hallitakseen verkko- ja tietojärjestelmien turvallisuuteen kohdistuvia riskejä, joita ne käyttävät toiminnassaan tai palvelujensa tarjoamisessa, sekä estääkseen tai minimoidakseen häiriöiden vaikutukset palvelujen vastaanottajiin ja muihin palveluihin.

2. ...tulee sisältämään vähintään seuraavat:
   (d) Toimitusketjun turvallisuus, mukaan lukien turvallisuuteen liittyvät näkökohdat, jotka koskevat kunkin toimijan ja sen suoraan käyttämien toimittajien tai palveluntarjoajien välisiä suhteita.

AI -käännös alkuperäisestä: NIS 2 Direktiivi, Art. 21(1) ja 21(2)(d)

WITH secure

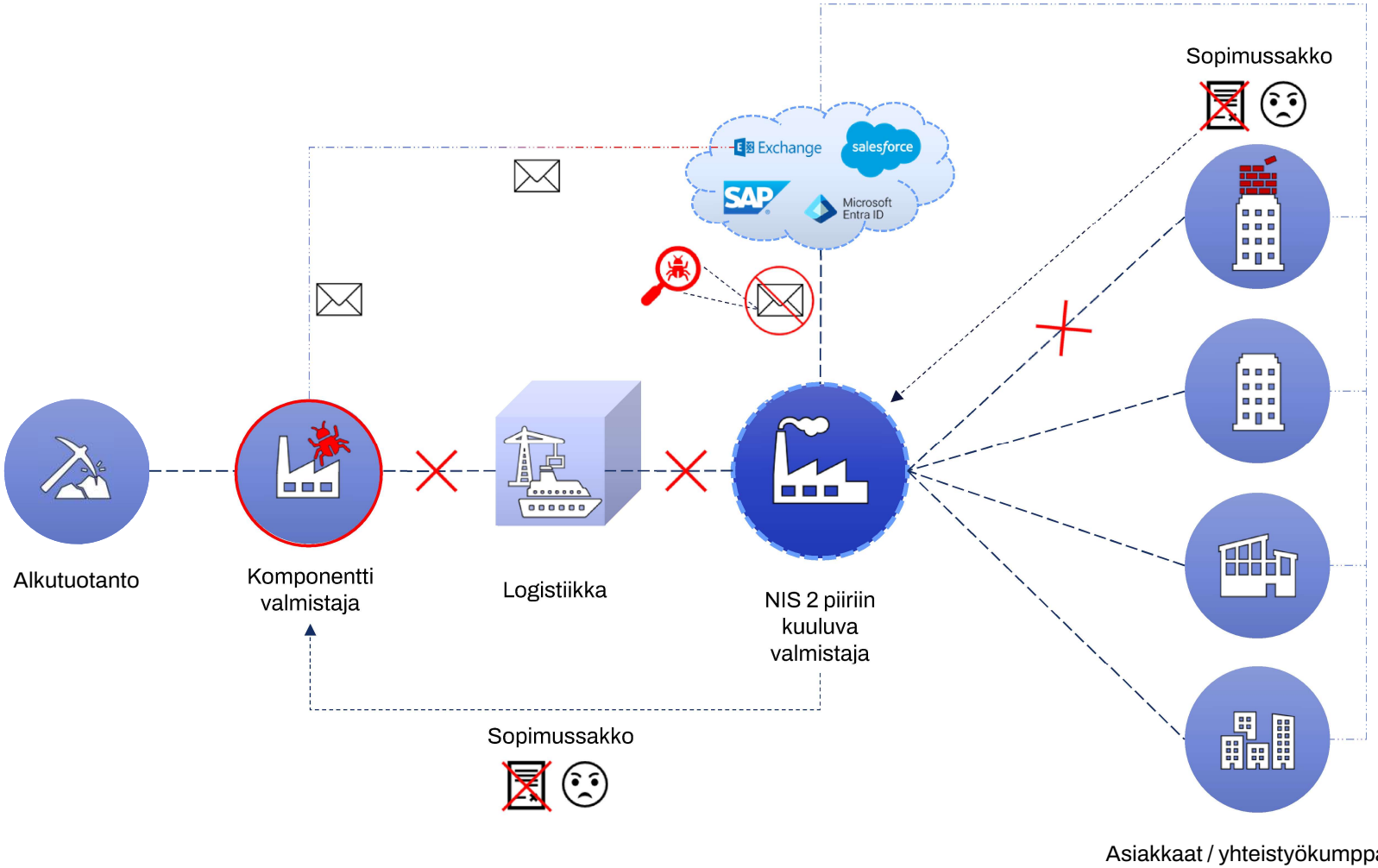
KOHDE VAI HEIKKO LENKKI?

Raha → **Kiristäminen**

Tieto → **Varastaminen**

Henkilöt → **Toimitusketju**

Toimitusketjun riskit



WITH secure

Hyökkäysmetodeja

	Hyökkäysmetodi	Kuvaus	Seuraukset
1	**Tietojenkalastelu**	- Phishing - Spear phishing eli kohdistettu tietojenkalastelu - Smishing eli SMS tietojenkalastelu - Spoofing eli lähettäjän tietojen väärentäminen	- Kirjautumistunnusten menetys - Haittaohjelman levittäminen - Laskutushuijaukset - Varastettujen **Entra ID** –tunnusten väärinkäyttö on usein ensimmäinen askel organisaation laajuiselle hyökkäykselle hybridi ympäristöissä
2	**Haavoittuvuuksien hyväksikäyttö**	- Päivittämättömien ohjelmien hyväksikäyttö - Nollapäivä haavoittuvuuksien hyväksikäyttö - Konfiguraatioiden hyväksikäyttö esim. palomuurien ja pilvi-infrastruktuurin asetusten hyväksikäyttö - Heikko identiteettipolitiikka esim. **MFA:n** puute ja huono salasanahygienia	- Hyökkääjä voi ohittaa suojauskerroksia vakavia haavoittuvuuksia hyväksikäyttäen ja korottaa käyttöoikeuksia - Heikot sähköposti asetukset kuten **SPF** ja **DKIM (DMARC)** puute voivat johtaa onnistuneisiin kalasteluyrityksiin. - Julkiverkkoon avoimia palveluita voidaan hyväksikäyttää jos niitä ei ole rakennettu tai konfiguroitu tietoturvallisesti esim. avoin **Azure Blob storage**
3	**Kolmannen osapuolen murrot**	- Kumppaniyrityksen kautta tapahtuvat hyökkäykset	- Asiakastietojärjestelmien kautta levitetään haittaohjelmia ja kalasteluyrityksiä esim. Salessorce - Ohjelmisto päivitysten ja pakettien saastuttaminen
4	**Sisäpiiriläiset**	- Tahalliset tai tahattomat vuodot työntekijöiltä	- Hyökkääjä voi hyväksikäyttää esim. GitHub repositorioon jätettyjä kirjautumistunnuksia

WITH secure

Tietomurron hinta

Suorat vahingot tavarantoimittajalle

- **Liiketoiminnan keskeytyminen**
  - IT-järjestelmien kaatuminen voi rampauttaa tai pysäyttää toiminnan kokonaan.
  - Kiinteät ja juoksevat kustannukset eivät pysähdy vaikka tuotanto pysähtyisi.
- **Tietojen menetys tai vuoto**
  - Organisaation tiedostot voidaan salata lunnaita vastaan. Yleensä tiedot myös varastetaan ja myydään eteenpäin tai salassapidettävän tiedon paljastamisella kiristetään uhria.
- **Incident response -konsultaatio**
  - 5-20 konsultaatio päivää (12 000€ - 48 000€).
- **Sakot ja oikeudelliset seuraamukset**
  - GDPR- tai muiden säädösten rikkominen voi johtaa sakkoihin.
  - Sopimusrikkomuksesta voi seurata sopimussakko.

Epäsuorat vahingot tavarantoimittajalle

- **Maineen ja luottamuksen vahingoittuminen**
  - Pitkäaikaiset kumppanuudet voivat päättyä.
  - Asiakas alkaa suosimaan muita kumppaneita ja siirtää sopimuksiaan kilpailijoille.
- **Varmuuskopioiden ajantasaisuus**
  - Palautettujen tietojen eheys ja ajantasaisuus voi aiheuttaa organisaatiolle epäsuoria kustannuksia pitkään tietoturvaloukkauksen jälkeenkin.
- **Kilpailuedun menetys**
  - Vuotaneet innovaatiot tai tuotantomenetelmät voivat päätyä kilpailijoille.
- **Vakuutusmaksujen nousu**
  - Kyberturvavakuutusten ehdot voivat kiristyä.

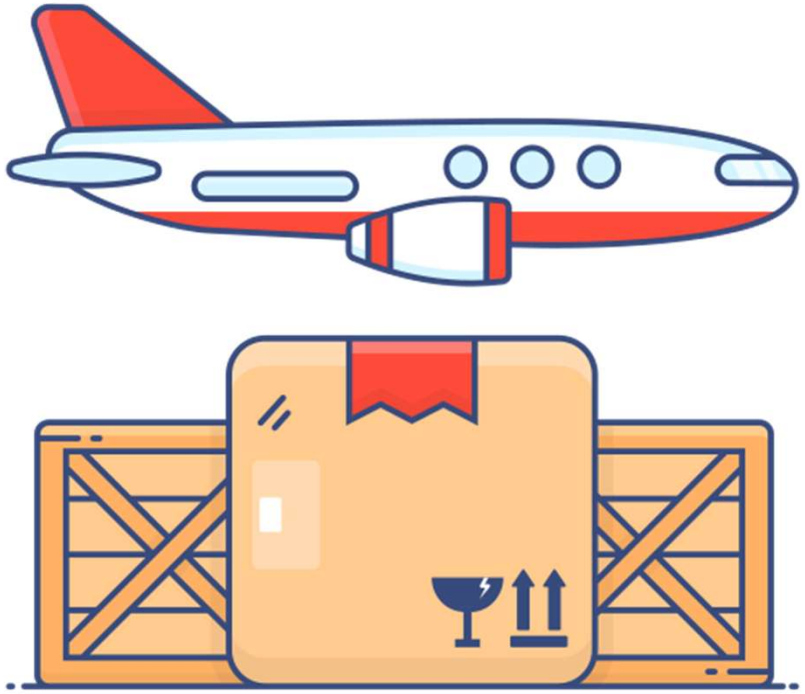
WITH secure

Tietomurron hinta

Välilliset seuraukset valmistajalle

- **Toimitusviiveet**
  - Komponenttien tai materiaalien toimitus voi viivästyä tai keskeytyä.
  - Sopimusrikkomuksesta voi seurata sopimussakko.
- **Tuotantokatkokset**
  - Valmistaja ei voi jatkaa tuotantoa ilman kriittisiä osia.
- **Laatuongelmat**
  - Korvaavat toimittajat eivät välttämättä täytä samoja laatustandardeja.
- **Luottamuksen heikentyminen**
  - Asiakkaat voivat kyseenalaistaa koko toimitusketjun turvallisuuden.
- **Sääntelyriskit**
  - Valmistaja voi joutua selvittämään viranomaisille, miksi toimitusketjussa tapahtui tietoturvaloukkaus.
- **Brändin maineen heikentyminen**
  - Vaikka valmistaja ei olisi suoraan vastuussa, media ja asiakkaat voivat yhdistää tapahtuman brändiin.

Pikarahti isoissa projekteissa voi syödä kannattavuuden (10 000€ - 100 000€)



WITH secure

Teknologiset, operatiiviset ja organisatoriset toimenpiteet

Miten osoitat yhteistyökumppanille että hoidatte kyberturvallisuuden asianmukaisesti ja oikeasuhtaisesti

WITH secure

TIETOTURVASTRATEGIA

ENNAKOI	ESTÄ		TUNNISTA JA REAGOI	
Haavoittuvuuksien hallinta	**Sähköpostin ja pilviympäristöjen turvaaminen**	**Verkon -ja päätelaitteiden suojaus**	**Tietoturva-poikkeamien tunnistaminen**	**Tietoturvan “ulkoistaminen”**
				
Teknologinen kyvykkyys systemaattisesti tunnistaa ja korjata haavoittuvuudet	SaaS/PaaS/IaaS – palvelujen suojaus konfiguraatioiden ja haitallisen sisällön osalta	Suojaa IT-ympäristösi käyttämällä mm. haittaohjelmien torjuntaa, palo-muureja ja salattuja yhteyksiä	Teknologinen kyvykkyys tunnistaa poikkeava käyttäytyminen sisäverkossa, päätelaitteilla ja pilvessä	“Ulkoista” osa tietoturvasta ammattilaisille Esim. 24/7 SOC/MDR/IR

Tietoturvaprosessit –ja proseduurit

WITH secure

ENNAKOI

Tunnista ja korjaa haavoittuvuudet ennen kuin hyökkääjä ehtii niitä väärinkäyttämään

WITH secure

Tarvitaan vain yksi haavoittuvuus

Hyökkääjät hyödyntävät haavoittuvuuksia tai houkuttelevat käyttäjiä murtaakseen organisaation suojauksen

6 487 → **18 103** → **40 009**
2015 2020 2024

Uusien haavoittuvuuksien määrä kasvaa vuodesta toiseen

~2 kuukautta

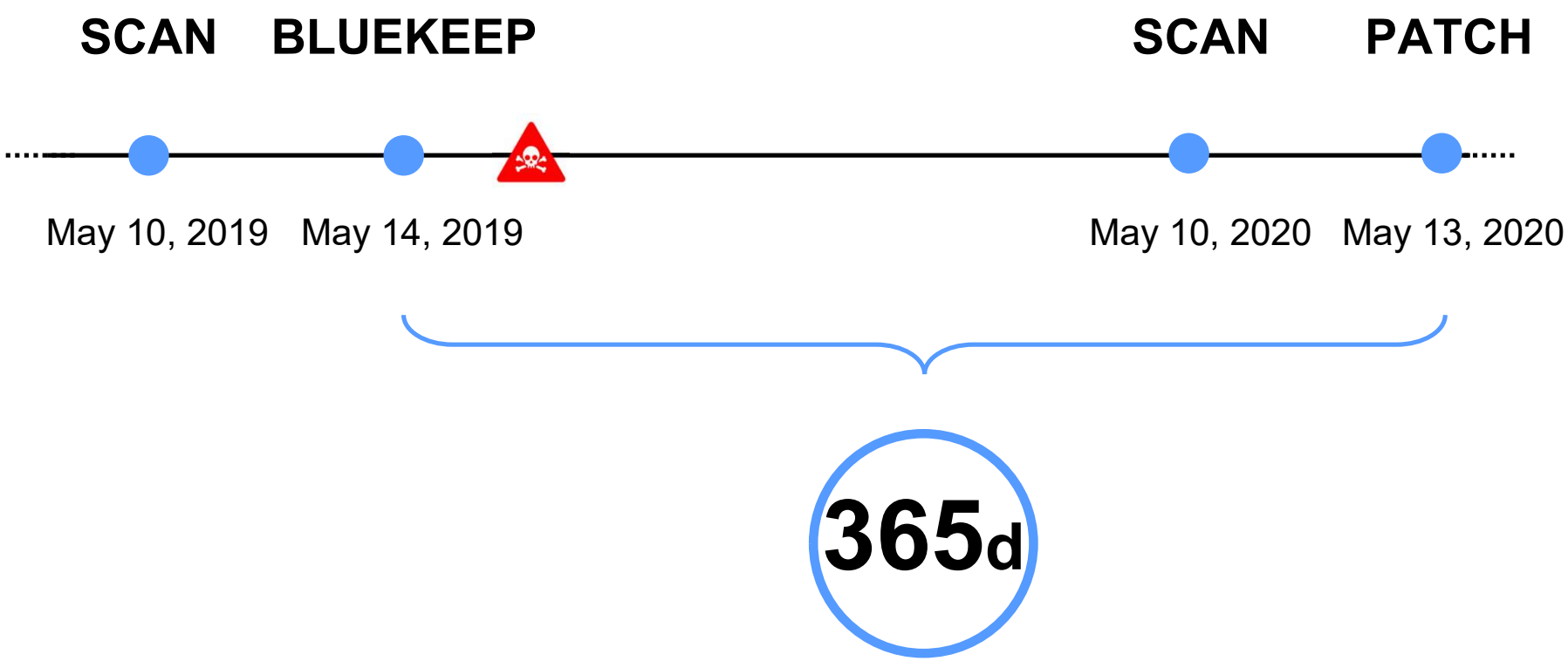
Keskimääräinen aika, joka kuluu tunnetun haavoittuvuuden korjaamiseen

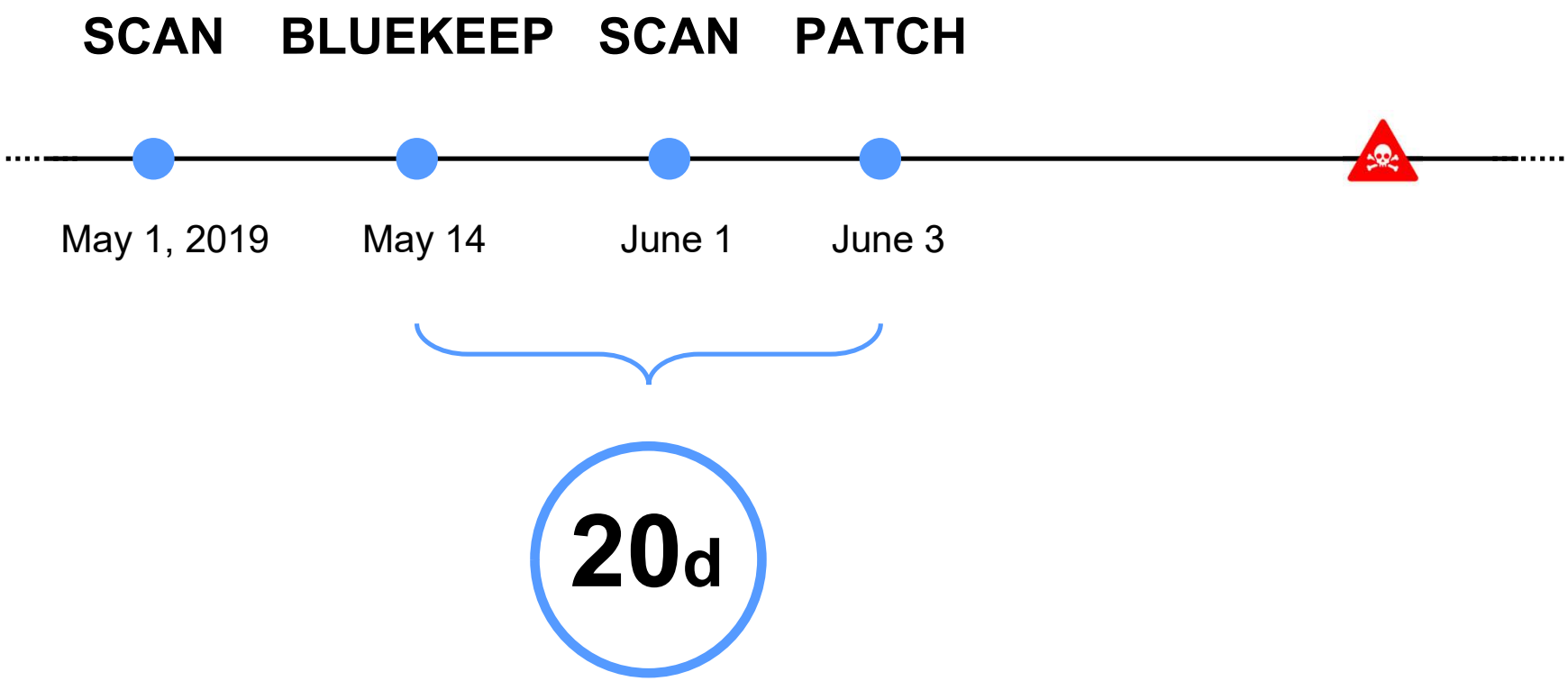
~ 1 viikko

Keskimääräinen aika, jonka kuluessa hyökkääjät käyttävät haavoittuvuutta hyväkseen

Lähteet:
NIST National Vulnerability Database 2021.
Guru Baran. “40,000+ CVEs Published In 2024, Marking A 38% Increase From 2023.” Cyber Security News, January 7, 2025.
Linder, Jannik. “Patch Management Statistics: Market Data Report 2025.” Gitnux, April 29, 2025.

WITH secure


SCAN
BLUEKEEP
SCAN
PATCH
May 10, 2019
May 14, 2019
May 10, 2020
May 13, 2020
365d

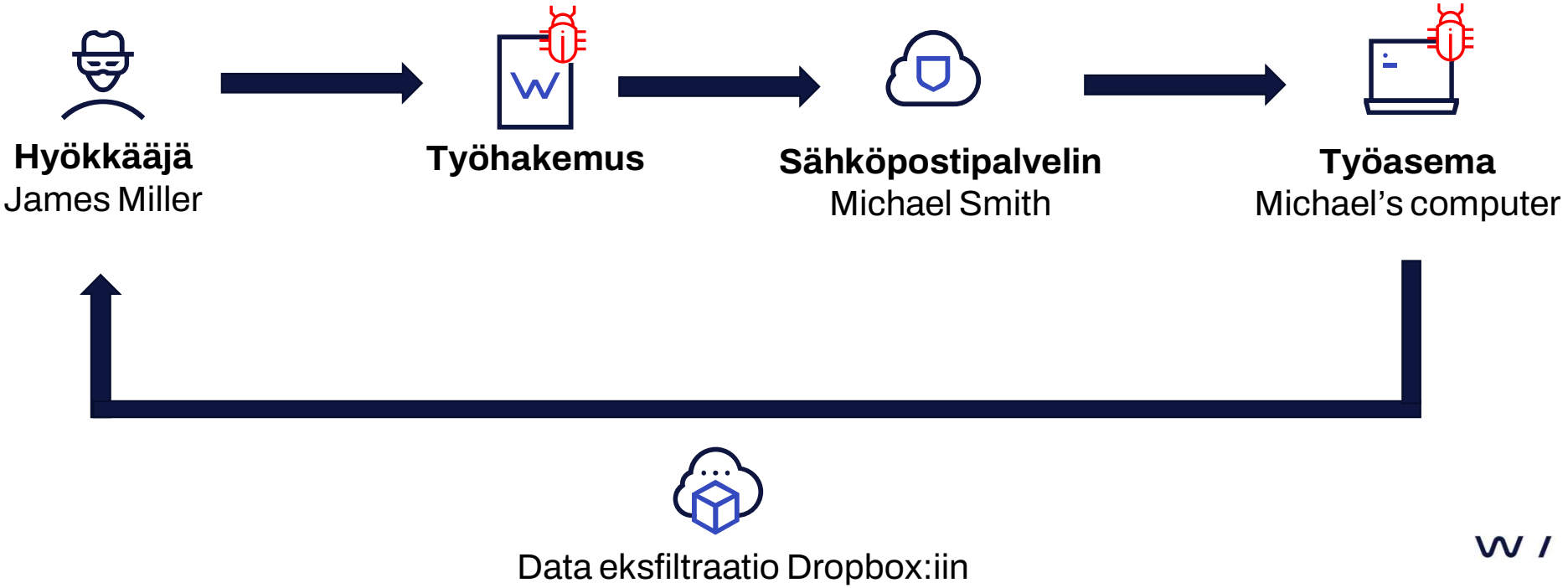

SCAN
BLUEKEEP
SCAN
PATCH
May 1, 2019
May 14
June 1
June 3
20d

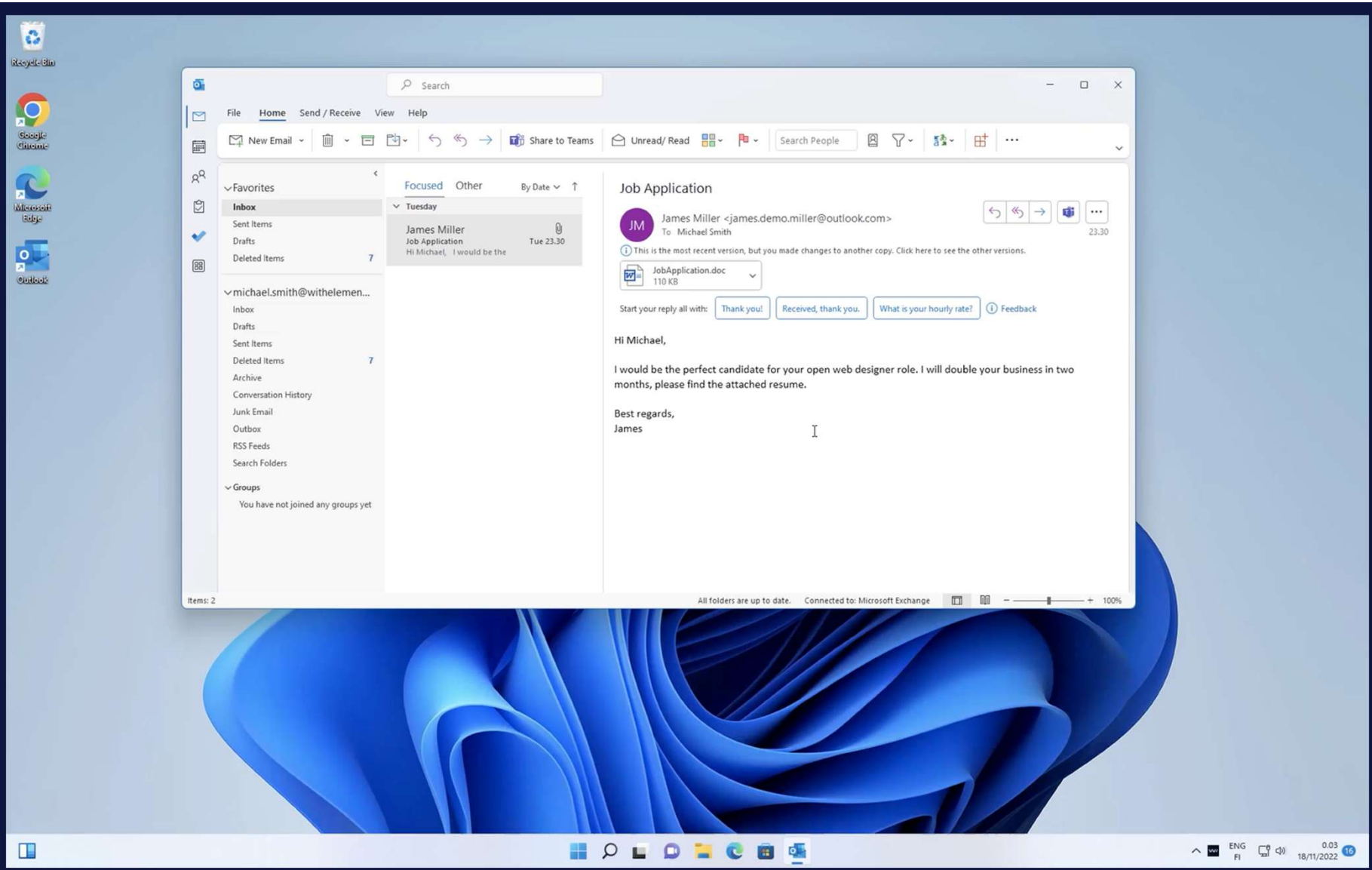
ESTÄ, TUNNISTA JA REAGOI

Kavenna hyökkäys pinta-alaa suojaamalla kriittiset järjestelmät ja tunnistamalla tietoturvapoikkeamat ja reagoimalla niihin oikea-aikaisesti

WITH secure

Rekrytointi prosessi demo




Recycle Bin
Google Chrome
Microsoft Edge
Outlook
Search
File
Home
Send / Receive
View
Help
New Email
Share to Teams
Unread/ Read
Search People
Favorites
Inbox
Sent Items
Drafts
Deleted Items 7
michael.smith@withelemen...
Inbox
Drafts
Sent Items
Deleted Items 7
Archive
Conversation History
Junk Email
Outbox
RSS Feeds
Search Folders
Groups
You have not joined any groups yet
Focused
Other
By Date
Tuesday
James Miller
Job Application
Hi Michael, I would be the
Tue 23.30
Job Application
JM
James Miller <james.demo.miller@outlook.com>
To Michael Smith
23.30
This is the most recent version, but you made changes to another copy. Click here to see the other versions.
JobApplication.doc
110 KB
Start your reply all with:
Thank you!
Received, thank you.
What is your hourly rate?
Feedback
Hi Michael,
I would be the perfect candidate for your open web designer role. I will double your business in two months, please find the attached resume.
Best regards,
James
Items: 2
All folders are up to date.
Connected to: Microsoft Exchange
100%
ENG
FI
0.03
18/11/2022
16

WITH secure

Miksi näkyvyydellä on merkitystä?

Security Events

Select field | Equals | Select value | Apply | Cancel | Clear all filters

Time After 01/08/2022

63 events

Time	Severity	Source	Device	Description	Acknowledged	Menu
14 minutes ago Feb 2, 2023, 09:52:57	Attention	File scanning Real-time scanning	WIN-WKS-01	The product detected "EICAR_Test_File" in "example_ransomware_payload.exe" and quarantined the file.	None	•••

Details

Alert type : on_access_scanner.file_infection.quarantine
Infection name : EICAR_Test_File
Path : C:\PayloadDrop\example_ransomware_payload.exe
File size: 68 B

Reputation : harmful (99)
Prevalence : common (60)
SHA-1: 3395856ce81f2b7382dee72602f798b642f14140
Available actions : disinfect,delete,rename,quarantine

Recommended actions : disinfect
Attempted operation : Close

Päätelaitesuojaus on estänyt haittaohjelman, mutta missä kontekstissa hyökkäys on tapahtunut?

Miten voin estää tämän jatkossa tapahtumasta?

WITH secure

Miksi näkyvyydellä on merkitystä?

Päätelaitteiden suojaus- ja havaitsemisratkaisujen avulla uhka estettiin, ja saatiin näkyvyys hyökkäyksen luonteeseen ja alkuperään.

Process details

WIN-WKS-01
4 processes added

outlook.exe Remove

Command line	"C:\Program Files (x86)\Microsoft Office\Office15\OUTLOOK.EXE"
Path	%program files%\microsoft office\office15
PID	9932
SHA1	c4e096925c8fbe5a4c723735340ac7c538ff9425
Execution start	02.02.2023 09:52:06 UTC+02:00
Execution end	02.02.2023 09:52:06 UTC+02:00

winword.exe Remove

Command line	"C:\Program Files (x86)\Microsoft Office\Office15\WINWORD.EXE" /n "C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\MF905DX4\JobApplication (35).doc" /o ""
Path	%program files%\microsoft office\office15
PID	9100
SHA1	81852cb9950604eda0918f625c71b0962865db23
Execution start	02.02.2023 09:52:22 UTC+02:00
Execution end	02.02.2023 09:52:23 UTC+02:00

powershell.exe Remove

Command line	"powershell" -NoP -NonI -W Hidden -Exec Bypass C:\windows\temp\example_payload_server.ps1
Path	%systemroot%\system32\windowspowershell\v1.0
PID	10136
SHA1	f43d9bb316e30ae1a3494ac5b0624f6bea1bf054
Execution start	02.02.2023 09:52:34 UTC+02:00
Execution end	02.02.2023 09:52:36 UTC+02:00

certutil.exe

Execution end 02.02.2023 09:52:42 UTC+02:00

Detections: Expand all

Detection 1/3 : Powershell.exe spawned certutil.exe Low
02.02.2023 09:52:37 UTC+02:00

Detection 2/3 : New process certutil.exe executed Low
02.02.2023 09:52:3[illegible]UTC+02:00

Detection 3/3 : Epp on access detection Medium
02.02.2023 09:52:42 UTC+02:00

Description	File access attempt on file detected with scan engine
Event ID(s)	bc8048c9-eb99-4691-a235-7f56aa9b4f95

EPP scan

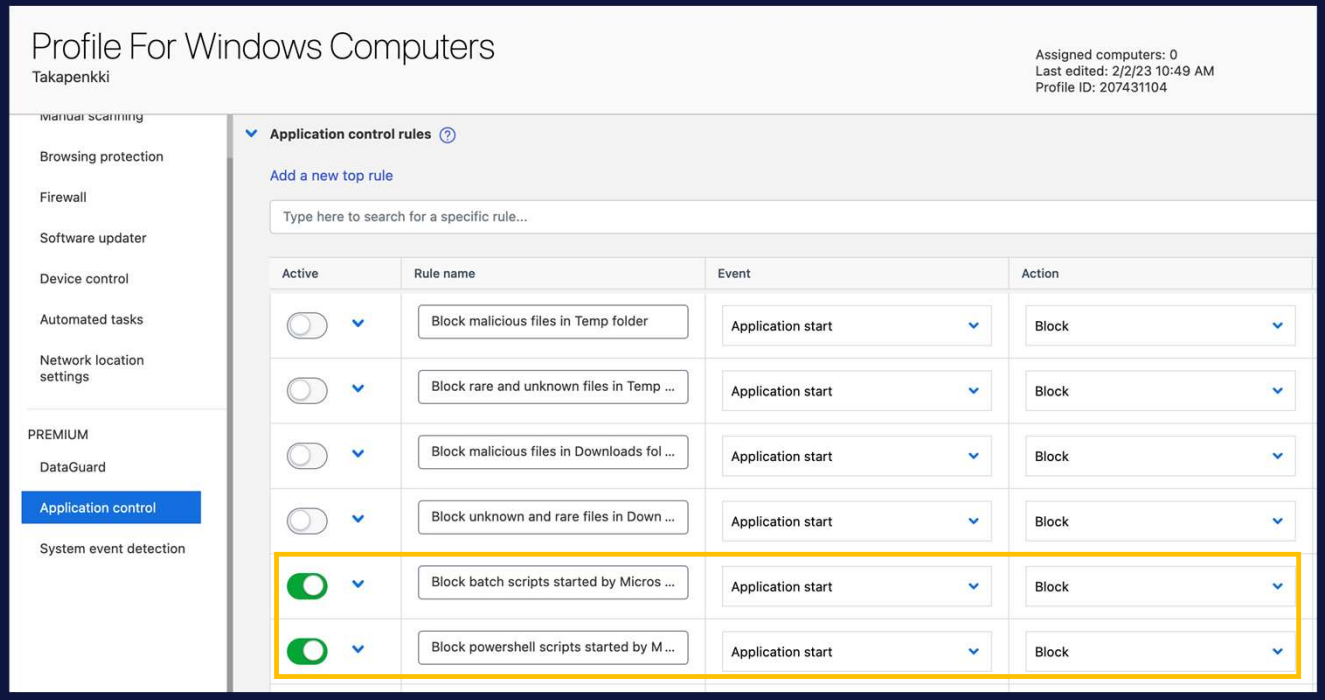
Infection name	EICAR_Test_File
Type	FILE
Reference	C:\PayloadDrop\example_ransomware_payload.exe
SHA1	3395856ce81f2b7382dee72602f798b642f14140
Performed action	DELETE
System wide	false

WITH secure

Opitut läksyt:
Kuinka estää tapahtuma teknologisesti

Estä Microsoft Office -sovellusten käynnistämät PowerShell-komentosarjat

Estä Microsoft Office -sovellusten käynnistämät batch-skriptit



WITH secure

Miksi näkyvyydellä on merkitystä?

Pystytkö löytämään juurisyyn jotta tietoturvapoikkeama ei toistu uudestaan?

Pystytkö teknologisesti estämään ettei samaa tekniikkaa voida käyttää uudestaan?

FROM

Tutkimus ilman teknologista kyvykkyyttä
~3 hours

TO

Tutkimus teknologisilla kyvykkyyksillä
~15 minutes

12 x nopeus tietoturvapoikkeaman tutkimisessa

WITH secure


WITH®
secure