Microsoft

Solorigate-yleiskatsaus

Tim Burrell

Partner Engineering Manager

Microsoft Threat Intelligence Center

18.2.2021

Solorigate-videosarja

Miten voit helpottaa organisaatiosi suojaamista Solorigaten kaltaisia hyökkäyksiä vastaan.

01 Solorigaten yleiskatsaus

02 Miten Solorigate tapahtui

03 Miten tunkeutuja voi käyttää tilejä

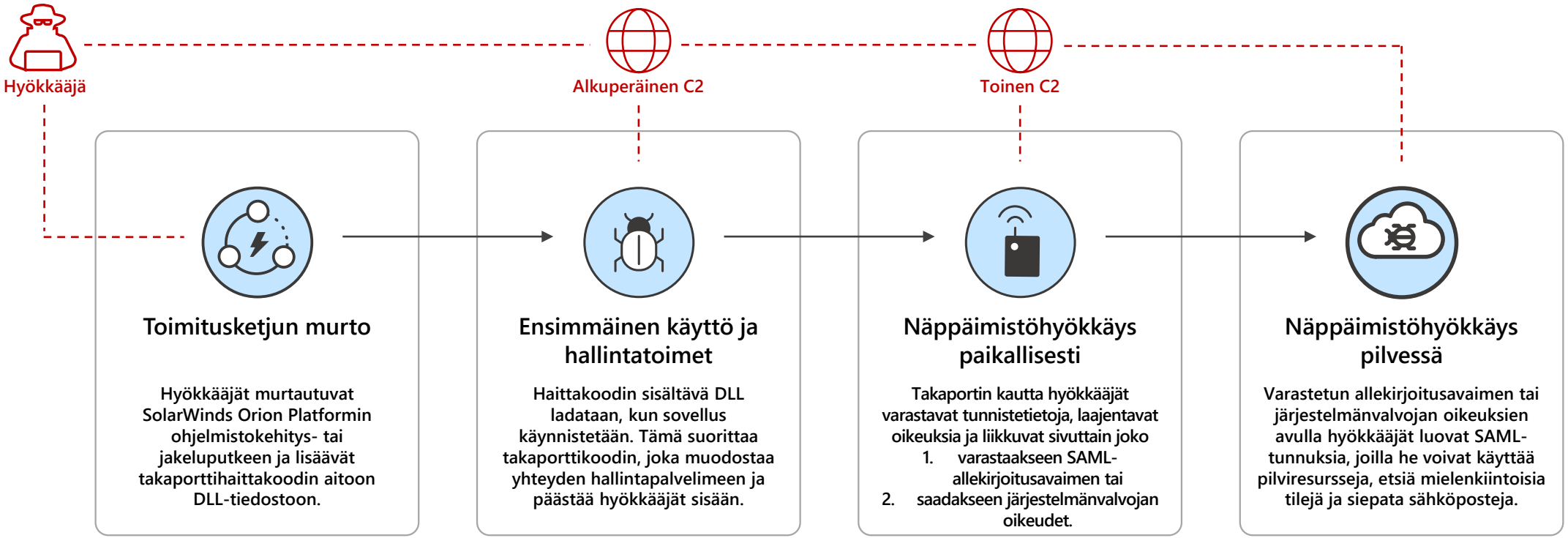
04 Seitsemän tapaa suojata organisaatio

05 Aika investoida SOC:n modernisointiin

Microsoft Security

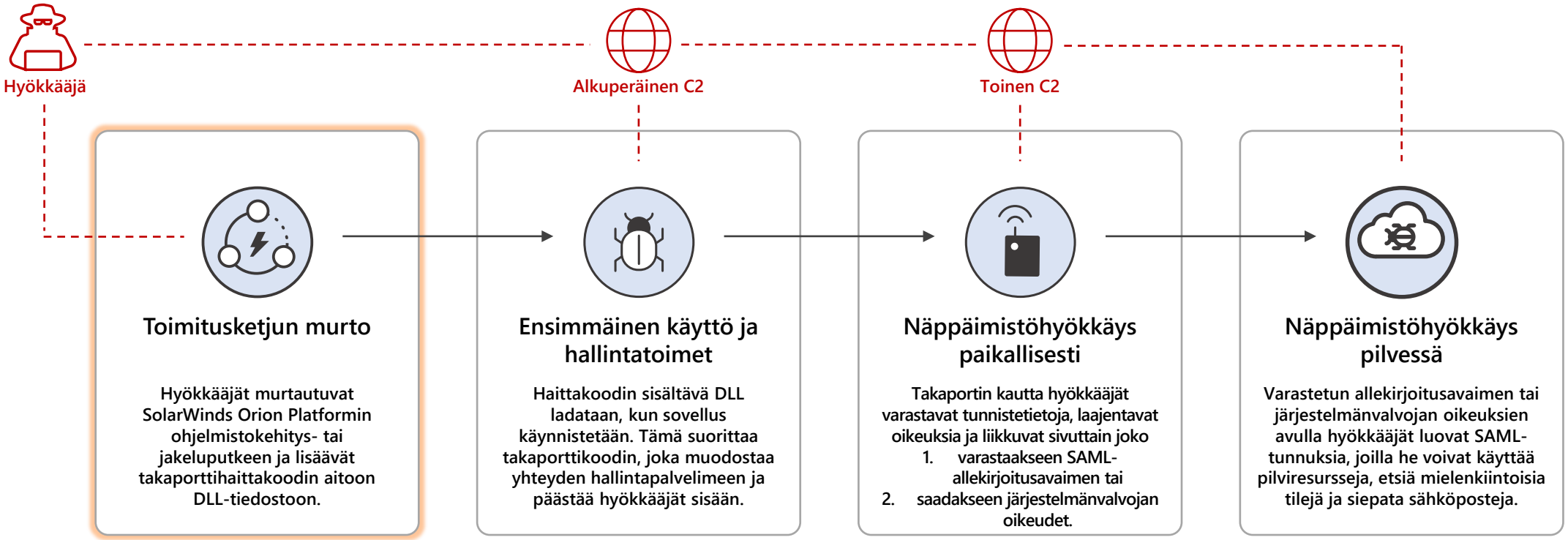
Solorigate-hyökkäys

Korkean tason päästä päähän -hyökkäysketju



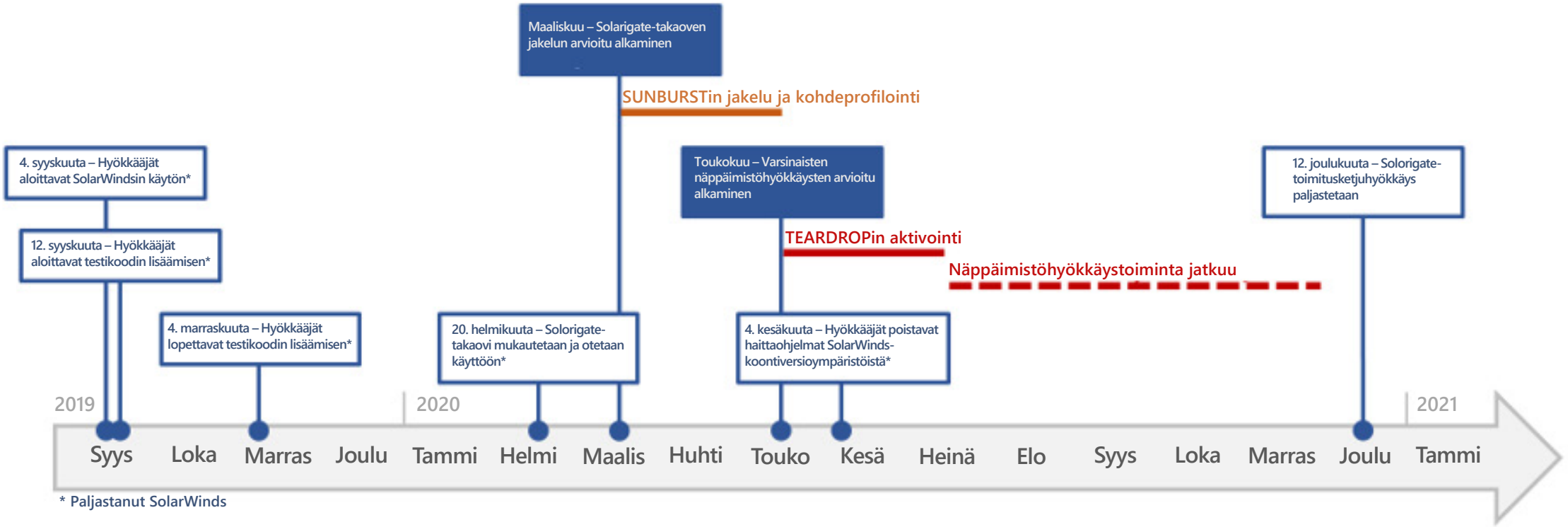
Solorigate-hyökkäys

Korkean tason päästä päähän -hyökkäysketju



Solorigate-hyökkäys

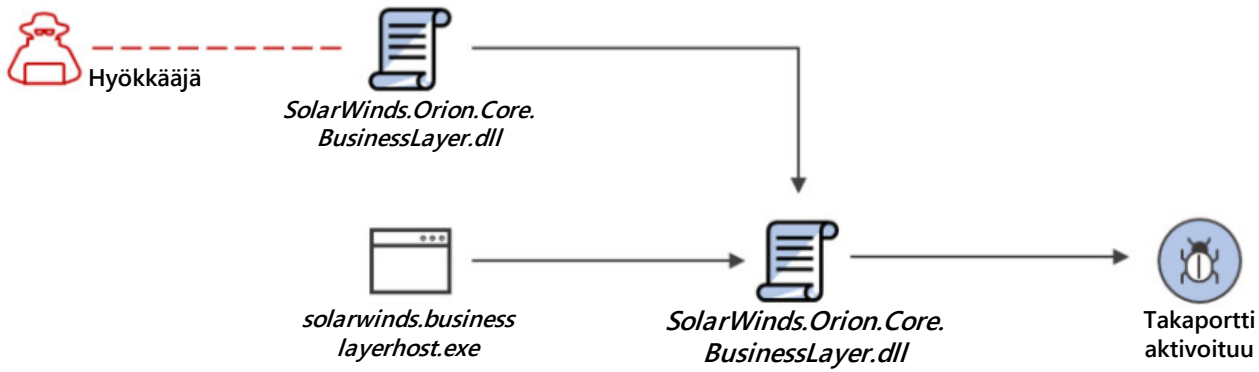
Aikajana



Tiedot ovat oikeat 21.1.2021. Katso uusimmat päivitykset osoitteesta aka.ms/solorigate

TOIMITUSKETJUN HYÖKKÄYS
Hyökkääjät lisäävät haitallisen koodin oikeutetun ohjelmiston DLL-komponenttiin. Vaarantunut DLL jaetaan organisaatioille, jotka käyttävät siihen liittyvää ohjelmistoa.

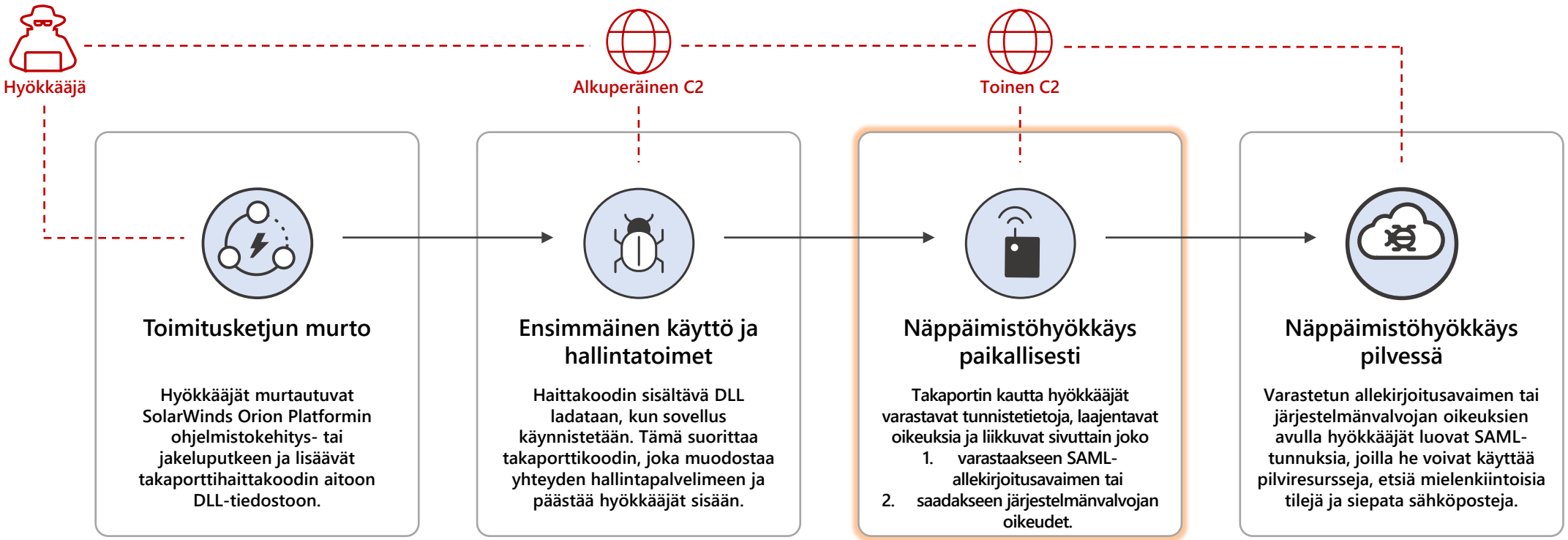
TOTEUTUS, PYSYVYYS
Kun ohjelmisto käynnistyy, vaarantunut DLL latautuu ja lisätty haittakoodi kutsuu toimintoa, joka sisältää takaportin ominaisuudet.




```
"Signer": "Solarwinds Worldwide, LLC",
"SignerHash": "47d92d49e6f7f296260da1af355f941eb25360c4",
```

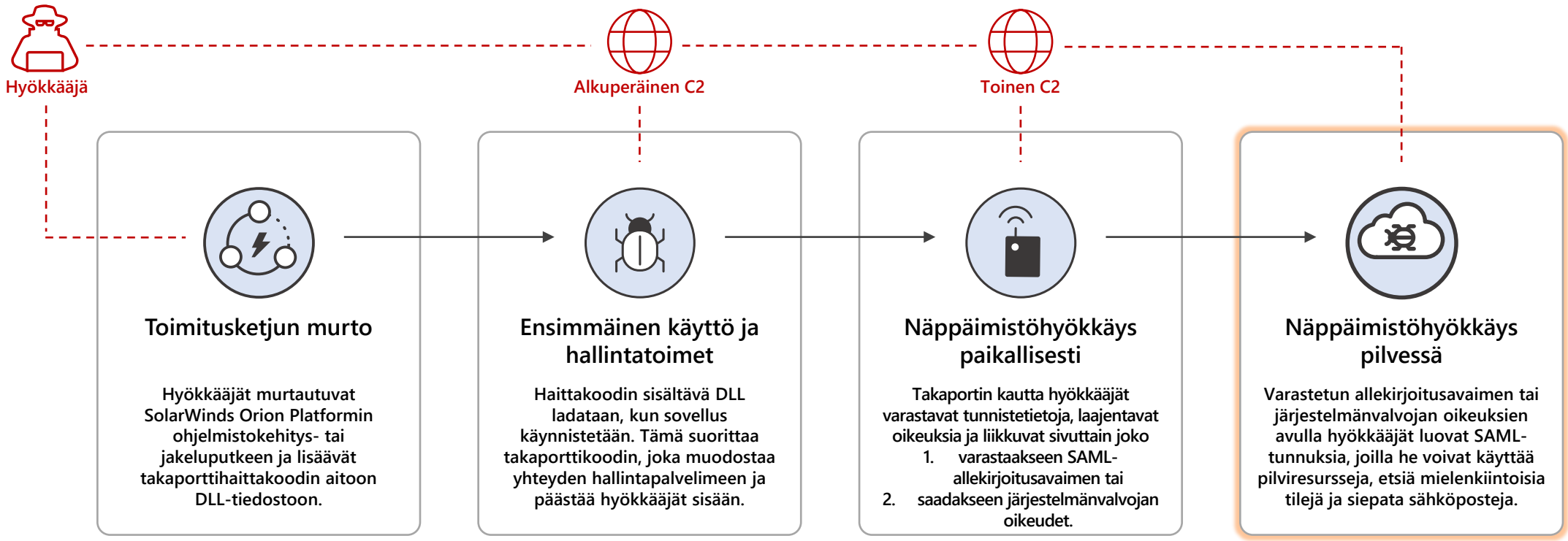
Solorigate-hyökkäys

Korkean tason päästä päähän -hyökkäysketju



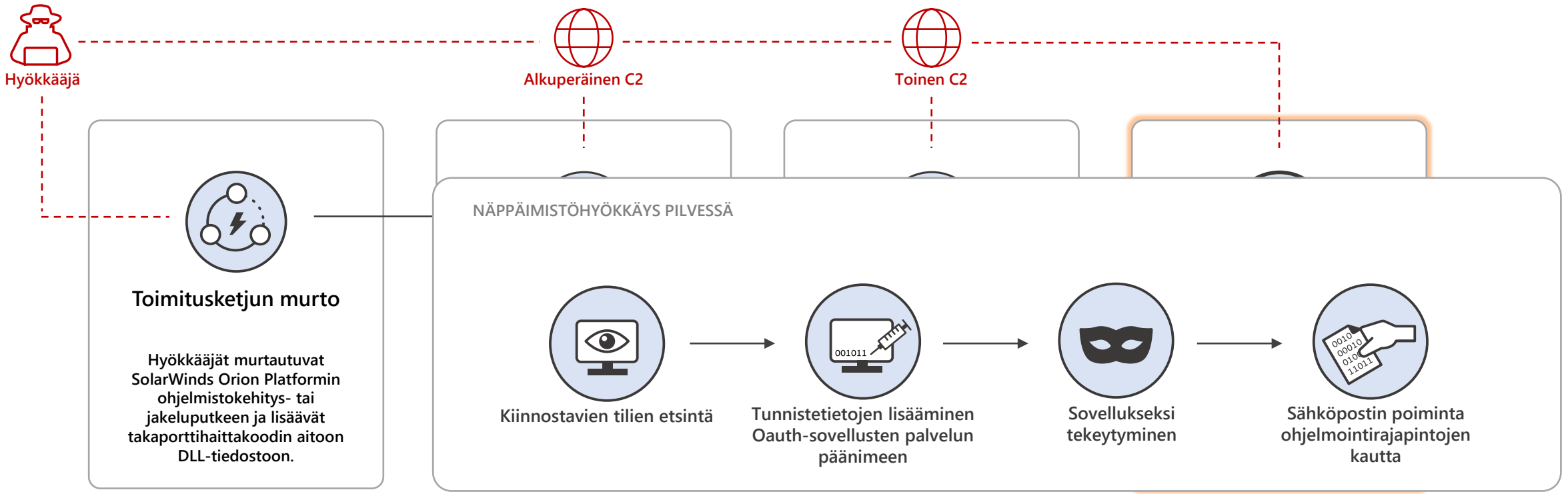
Solorigate-hyökkäys

Korkean tason päästä päähän -hyökkäysketju



Solorigate-hyökkäys

Korkean tason päästä päähän -hyökkäysketju



Suositellut puolustustoimet

Seitsemän vaihetta, jotka helpottavat suojautumista Solorigaten tekniikoita vastaan

1. Käytä ajantasaisia virustorjunta- ja EDR-tuotteita.

2. Estä tunnetut C2-päätepisteet verkkosi infrastruktuurin avulla.

3. Suojaa SAML-tunnusten allekirjoitusavaimet, ja harkitse SAML-tunnusten allekirjoitusvarmenteiden laitteistosuojausta. Lue Active Directory -liittoutumispalveluja koskevat Microsoftin parhaat suositukset: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/best-practices-securing-ad-fs

4. Noudata järjestelmänvalvojan käyttöoikeuksien parhaita käytäntöjä, ja vähennä niiden käyttäjien määrää, jotka ovat paljon oikeuksia omaavien hakemistoroolien jäseniä.

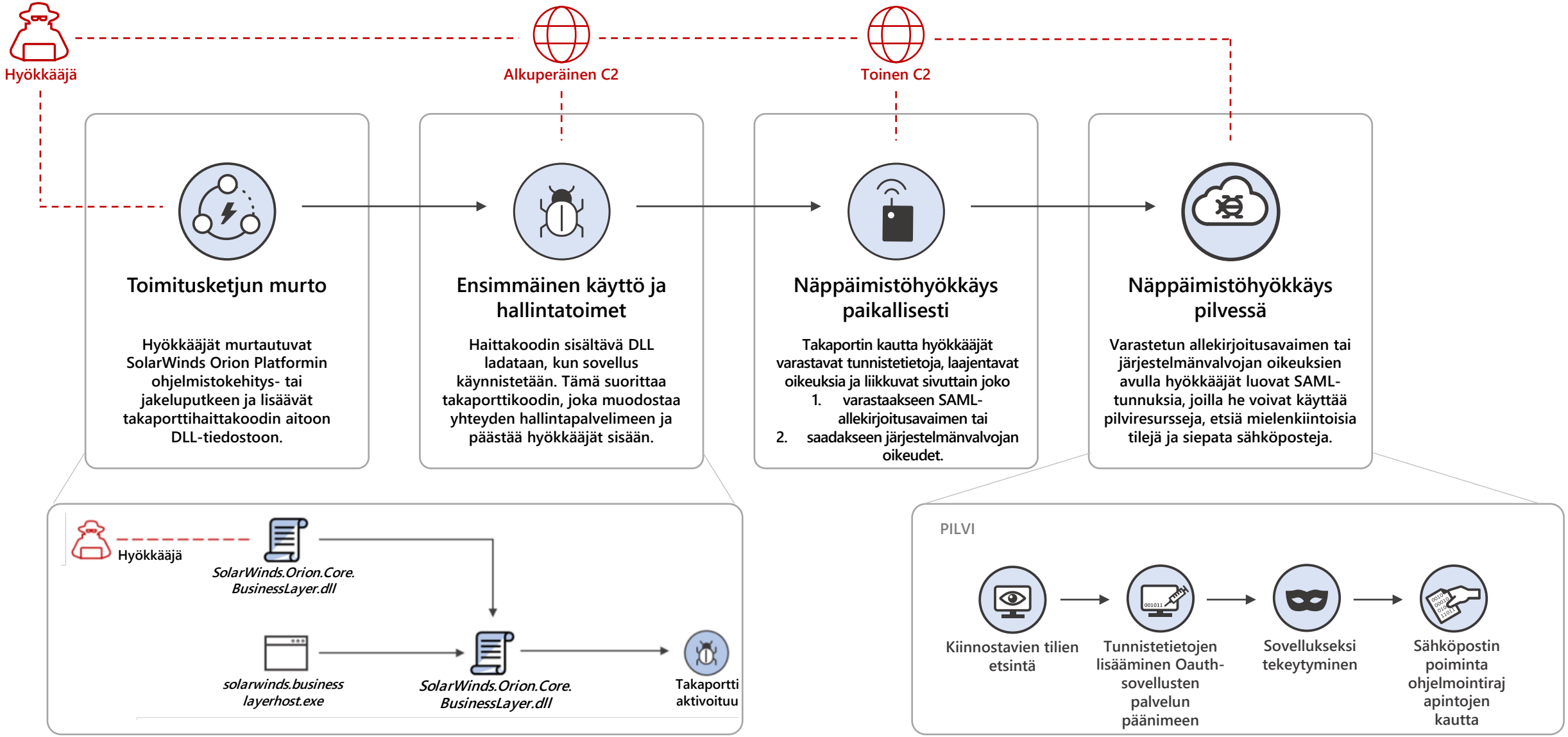
5. Varmista, että järjestelmänvalvojan oikeuksin varustetut palvelutilit käyttävät suuren entropian salaisuuksia (eli varmenteita), jotka on tallennettu turvallisesti. Valvo muutoksia, kirjautumisia ja poikkeavien palvelutilien käyttöä.

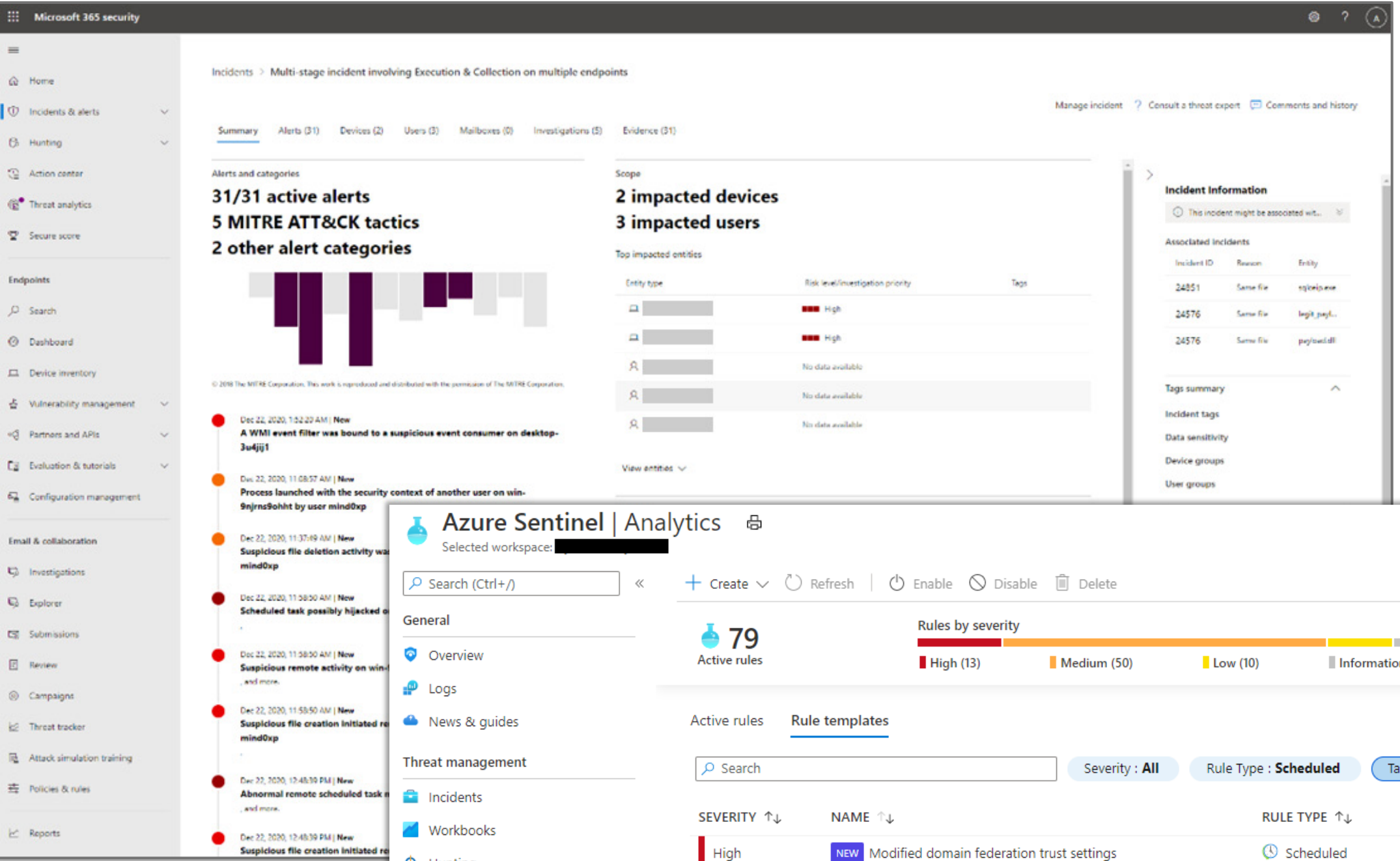
6. Poista tai poista käytöstä käyttämättömät tai tarpeettomat sovelluksen ja palvelun päänimet. Vähennä käyttöoikeuksia niihin, jotka vielä jäävät.

7. Katso lisäsuosituksia Azure AD -käyttäjätietojen infrastruktuurin suojaamiseen: https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity

Solorigate-hyökkäys

Korkean tason päästä päähän -hyökkäysketju




Microsoft 365 security
Home
Incidents & alerts
Hunting
Action center
Threat analytics
Secure score
Endpoints
Search
Dashboard
Device inventory
Vulnerability management
Partners and APIs
Evaluation & tutorials
Configuration management
Email & collaboration
Investigations
Explorer
Submissions
Review
Campaigns
Threat tracker
Attack simulation training
Policies & rules
Reports
Incidents > Multi-stage incident involving Execution & Collection on multiple endpoints
Manage incident
Consult a threat expert
Comments and history
Summary
Alerts (31)
Devices (2)
Users (3)
Mailboxes (0)
Investigations (5)
Evidence (31)
Alerts and categories
31/31 active alerts
5 MITRE ATT&CK tactics
2 other alert categories
Scope
2 impacted devices
3 impacted users
Top impacted entities
Entity type
Risk level/investigation priority
Tags
High
No data available
View entities
Incident Information
Associated incidents
Tags summary
Incident tags
Data sensitivity
Device groups
User groups
A WMI event filter was bound to a suspicious event consumer on desktop-3u4jij1
Process launched with the security context of another user on win-9njrns9ohht by user mind0xp
Suspicious file deletion activity
Scheduled task possibly hijacked
Suspicious remote activity on win-
Suspicious file creation initiated
Abnormal remote scheduled task

Azure Sentinel | Analytics
Selected workspace:
Search (Ctrl+/)
General
Overview
Logs
News & guides
Threat management
Incidents
Workbooks
Hunting
Notebooks (Preview)
Entity behavior
Create
Refresh
Enable
Disable
Delete
79
Active rules
Rules by severity
High (13)
Medium (50)
Low (10)
Informational (6)
Active rules
Rule templates
Search
Severity : All
Rule Type : Scheduled
Tactics : 2 selected
Data Sources : 3 sel
SEVERITY
NAME
RULE TYPE
DATA SOURCES
High
NEW
Modified domain federation trust settings
Scheduled
Azure Active Directory
Low
NEW
Interactive STS refresh token modifications
Scheduled
Azure Active Directory
Low
NEW
Azure Active Directory PowerShell accessing non-AAD resou...
Scheduled
Azure Active Directory

Solorigate-videosarja

Seuraavat vaiheet

01 Katso Solorigate-videosarja tästä sijainnista

02 Saat lisää päivityksiä Microsoft Security -sivustosta: www.microsoft.com/en-us/security/business

03 Lue blogijulkaisut osoitteesta on: www.microsoft.com/security/blog

https://aka.ms/solorigate

Microsoft Security

Microsoft