Microsoft

Επισκόπηση Solorigate

Tim Burrell

Partner Engineering Manager

Κέντρο Ευφυΐας προστασίας από απειλές της Microsoft

18 Φεβρουαρίου 2021

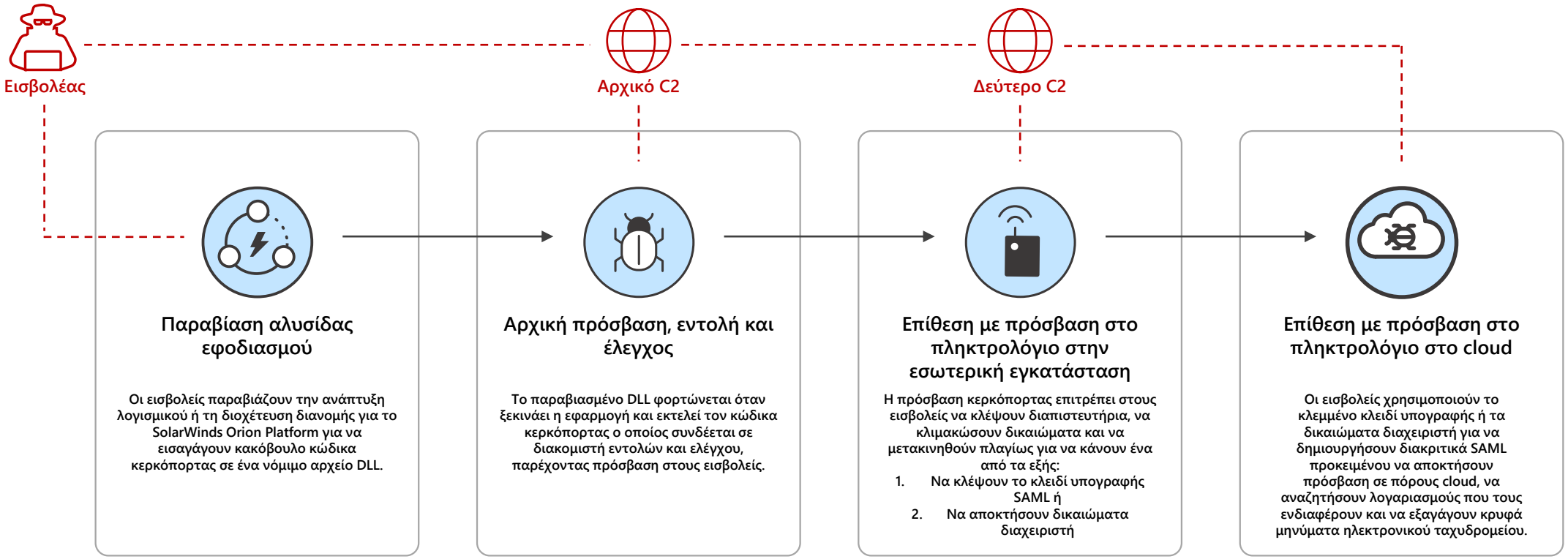
Σειρά βίντεο Solorigate

Πώς μπορείτε να προστατέψετε τον οργανισμό σας από επιθέσεις τύπου Solorigate.

Microsoft Security

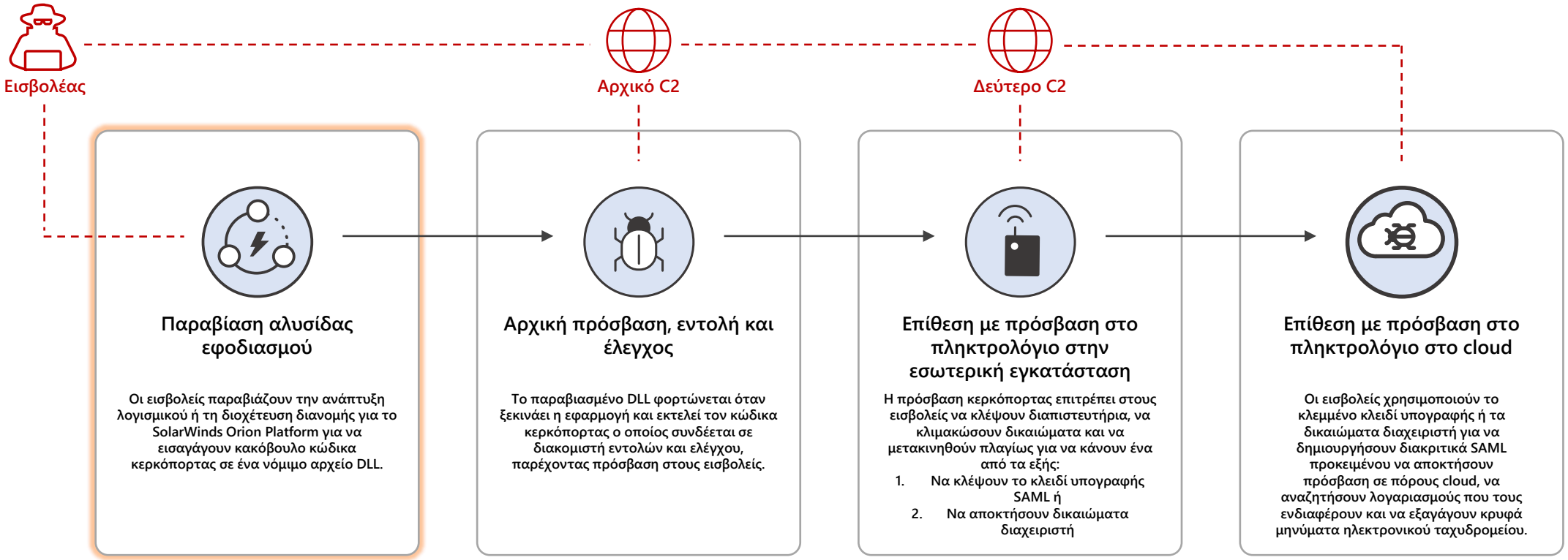
Επίθεση Solorigate

Αλυσίδα επιθέσεων από τερματικό σε τερματικό υψηλού επίπεδου



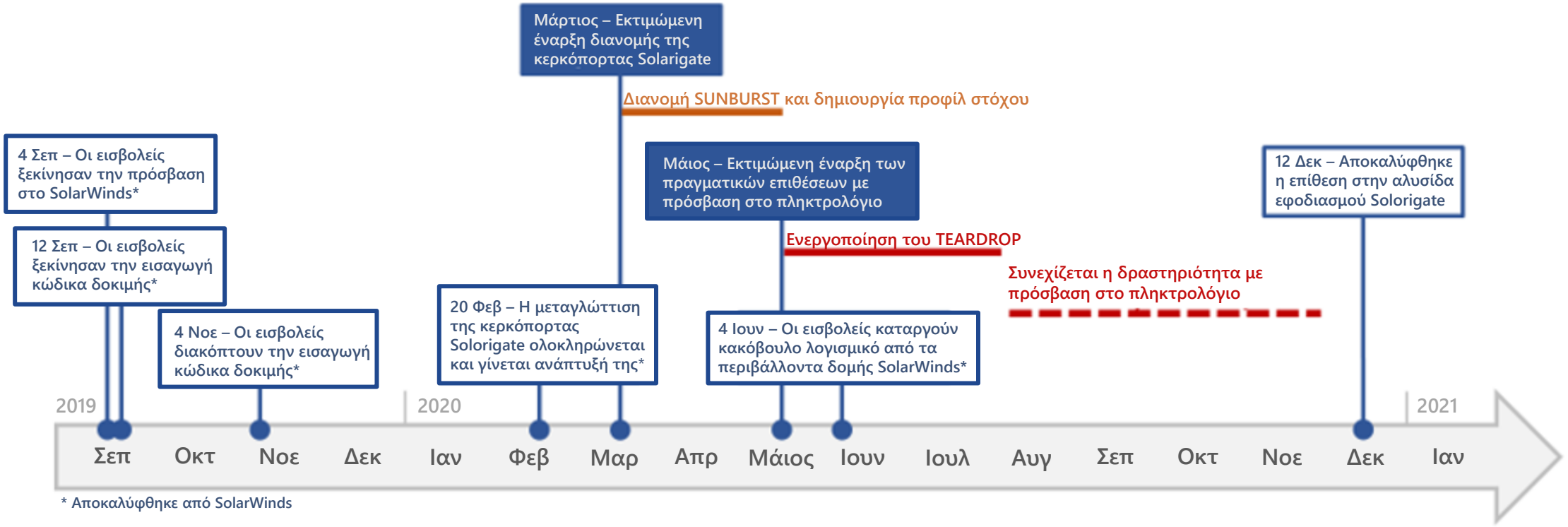
Επίθεση Solorigate

Αλυσίδα επιθέσεων από τερματικό σε τερματικό υψηλού επίπεδου



Επίθεση Solorigate

Λωρίδα χρόνου

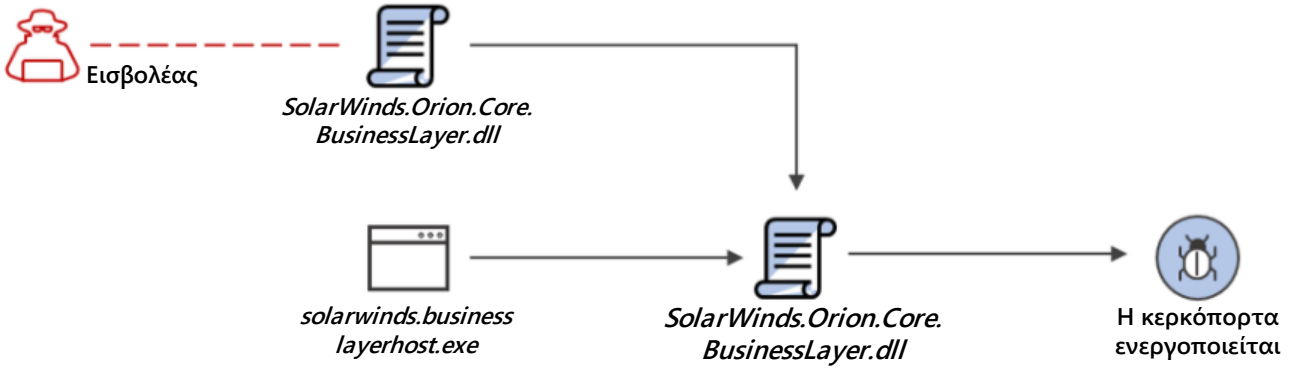


* Αποκαλύφθηκε από SolarWinds

Οι πληροφορίες είναι σωστές στις 21/1/2021. Ανατρέξτε στη διεύθυνση aka.ms/solorigate για τις πιο πρόσφατες ενημερώσεις

ΕΠΙΘΕΣΗ ΣΕ ΑΛΥΣΙΔΑ ΕΦΟΔΙΑΣΜΟΥ
Οι εισβολείς εισαγάγουν κακόβουλο κώδικα σε ένα στοιχείο DLL νόμιμου λογισμικού. Το παραβιασμένο DLL διανέμεται στους οργανισμούς που χρησιμοποιούν το σχετικό λογισμικό.

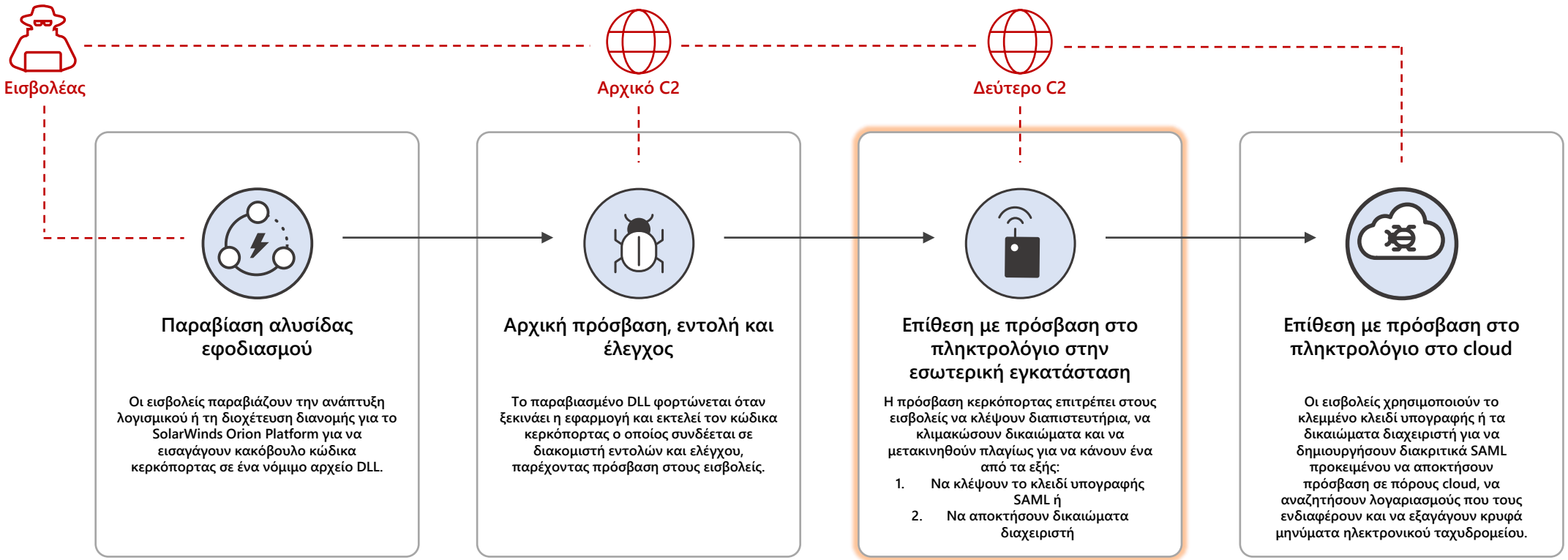
ΕΚΤΕΛΕΣΗ, ΔΙΑΤΗΡΗΣΗ
Όταν ξεκινάει το λογισμικό, φορτώνεται το παραβιασμένο DLL και ο εισηγμένος κακόβουλος κώδικας καλεί τη συνάρτηση που περιέχει τις δυνατότητες κερκόπορτας.




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

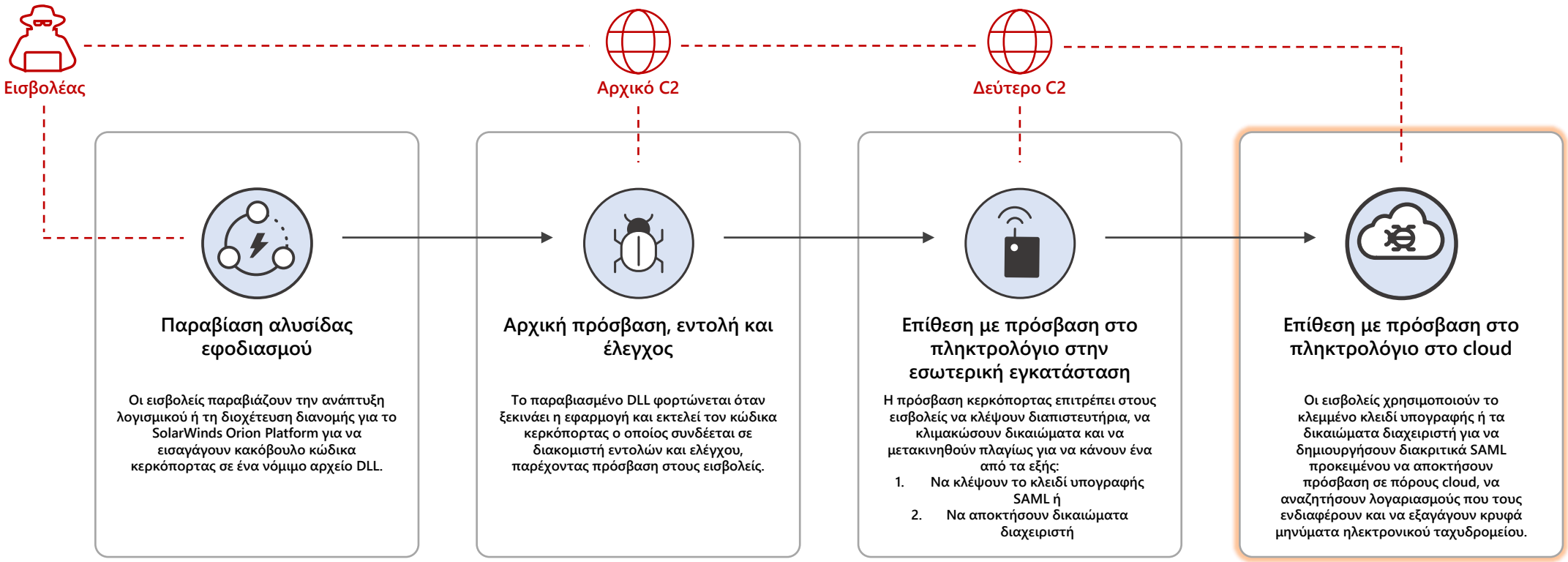
Επίθεση Solorigate

Αλυσίδα επιθέσεων από τερματικό σε τερματικό υψηλού επίπεδου



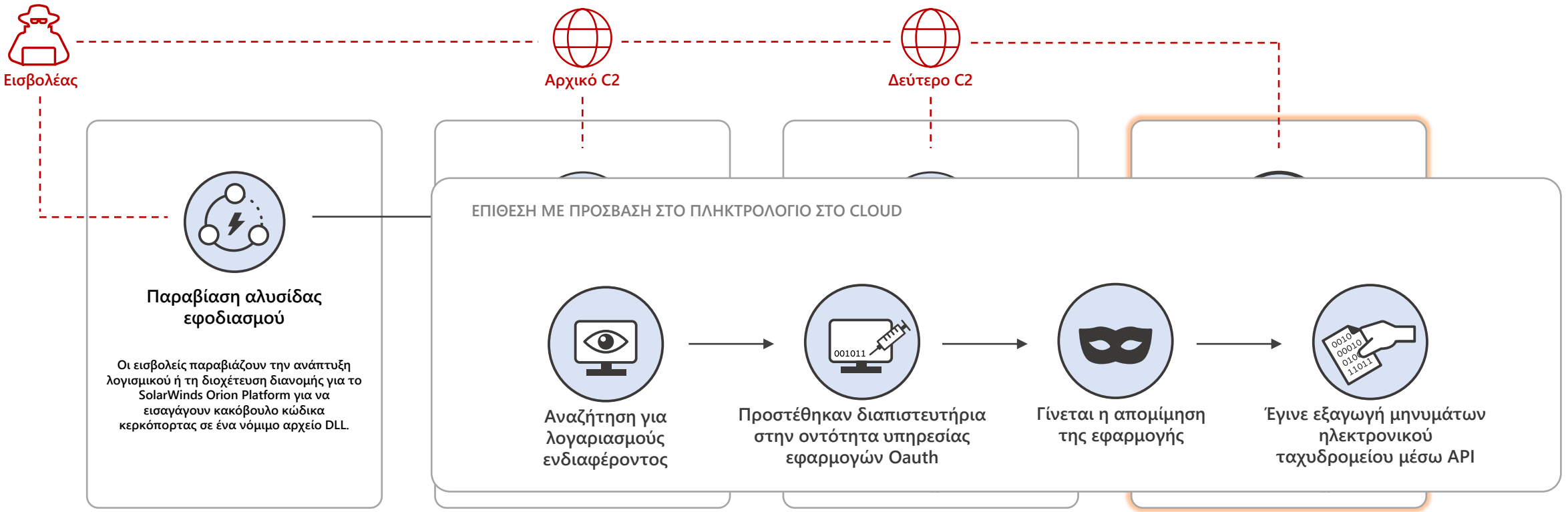
Επίθεση Solorigate

Αλυσίδα επιθέσεων από τερματικό σε τερματικό υψηλού επίπεδου



Επίθεση Solorigate

Αλυσίδα επιθέσεων από τερματικό σε τερματικό υψηλού επίπεδου



Προτεινόμενες άμυνες

7 βήματα για να προστατευτείτε από τεχνικές που χρησιμοποιήθηκαν στο Solorigate

1. Εκτελέστε ενημερωμένο λογισμικό προστασίας από ιούς και προϊόντα EDR.

2. Αποκλείστε γνωστά τελικά σημεία C2 που χρησιμοποιούν την υποδομή του δικτύου σας.

3. Ασφαλίστε τα κλειδιά υπογραφής διακριτικών SAML και σκεφτείτε το ενδεχόμενο χρήσης εξοπλισμού ασφάλειας για τα πιστοποιητικά υπογραφής διακριτικών SAML. Για τις Υπηρεσίες Active Directory Federation Services, διαβάστε τις προτάσεις βέλτιστων πρακτικών της Microsoft: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/best-practices-securing-ad-fs

4. Ακολουθήστε τις βέλτιστες πρακτικές για τα δικαιώματα διαχειριστών και μειώστε τον αριθμό των χρηστών που κατέχουν ρόλους καταλόγου με πολλά προνόμια.

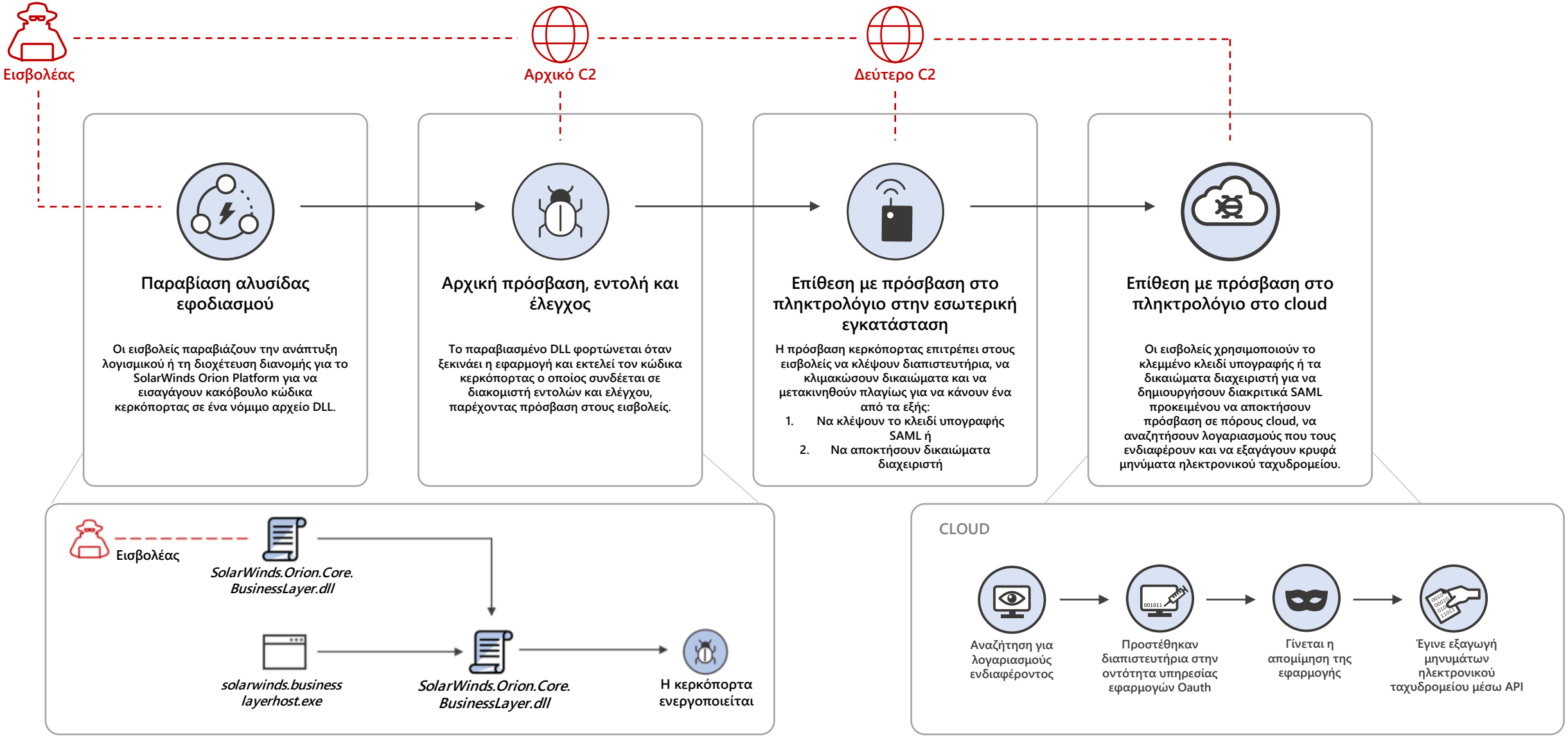
5. Βεβαιωθείτε ότι οι λογαριασμοί υπηρεσίας με δικαιώματα διαχείρισης χρησιμοποιούν μυστικά υψηλής εντροπίας (δηλ. πιστοποιητικά) τα οποία είναι αποθηκευμένα με ασφάλεια. Παρακολουθείτε τυχόν αλλαγές, εισόδους και χρήση μη κανονικών λογαριασμών υπηρεσίας.

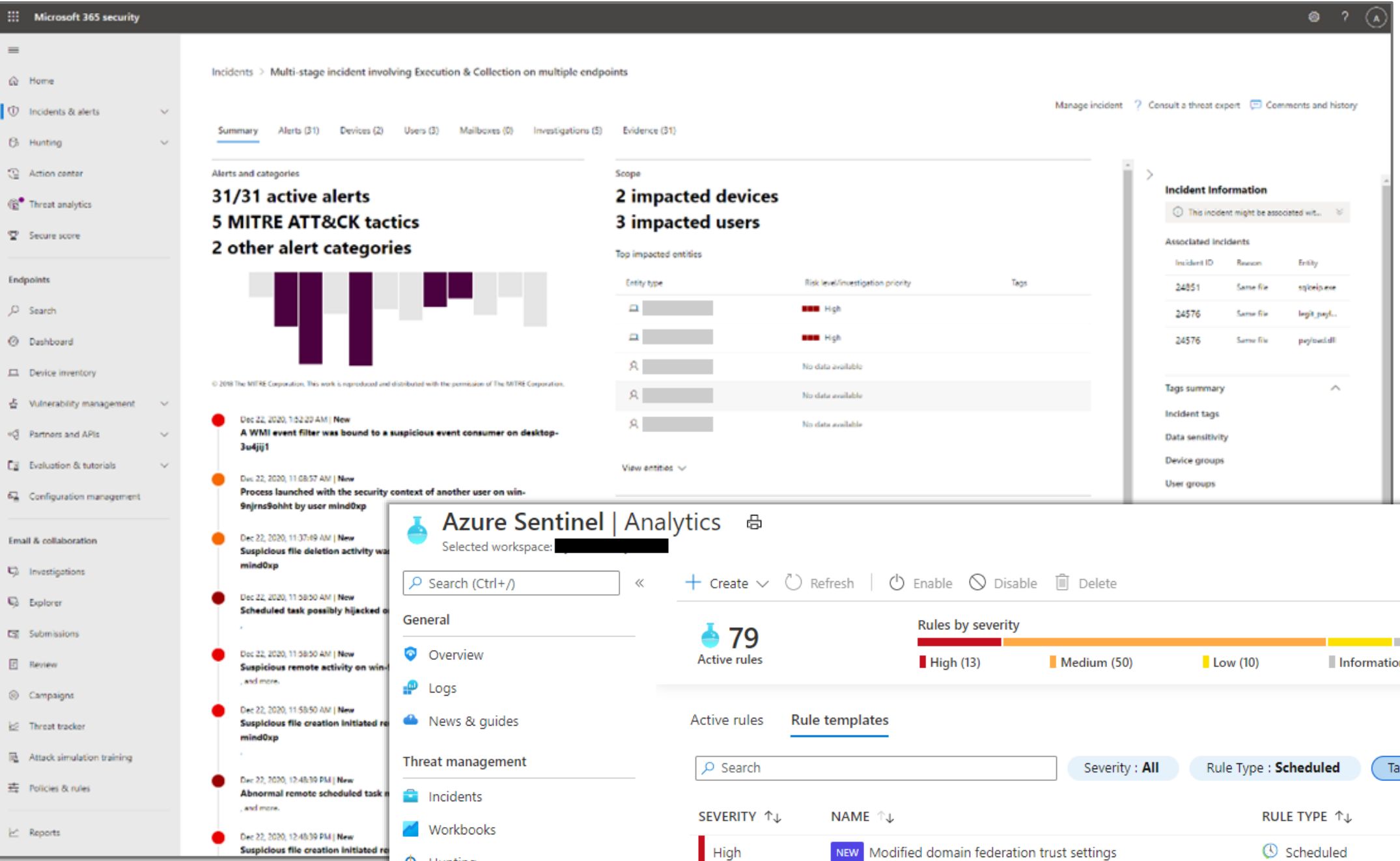
6. Καταργήστε ή απενεργοποιήστε εφαρμογές και οντότητες υπηρεσίας που δεν χρησιμοποιούνται ή δεν είναι απαραίτητες. Μειώστε τα δικαιώματα σε αυτές που εξακολουθείτε να έχετε.

7. Δείτε πρόσθετες προτάσεις για την ασφάλεια της υποδομής ταυτοτήτων Azure Active Directory: https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity

Επίθεση Solorigate

Αλυσίδα επιθέσεων από τερματικό σε τερματικό υψηλού επίπεδου




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

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

Σειρά βίντεο Solorigate

Επόμενα βήματα

01 Παρακολουθήστε τη σειρά βίντεο Solorigate σε αυτήν την τοποθεσία

02 Επισκεφθείτε την Ασφάλεια της Microsoft για περισσότερες ενημερώσεις: www.microsoft.com/en-us/security/business

03 Διαβάστε τις δημοσιεύσεις ιστολογίου στη διεύθυνση: www.microsoft.com/security/blog

https://aka.ms/solorigate

Microsoft Security

Microsoft