Microsoft

Solorigate 概述

Tim Burrell
合作伙伴工程经理
Microsoft 威胁智能中心

2021 年 2 月 18 日

Solorigate 视频系列

如何帮助保护组织免遭 Solorigate 类型的攻击。

01 Solorigate 概述

02 Solorigate 是怎么发生的

03 入侵者如何访问帐户

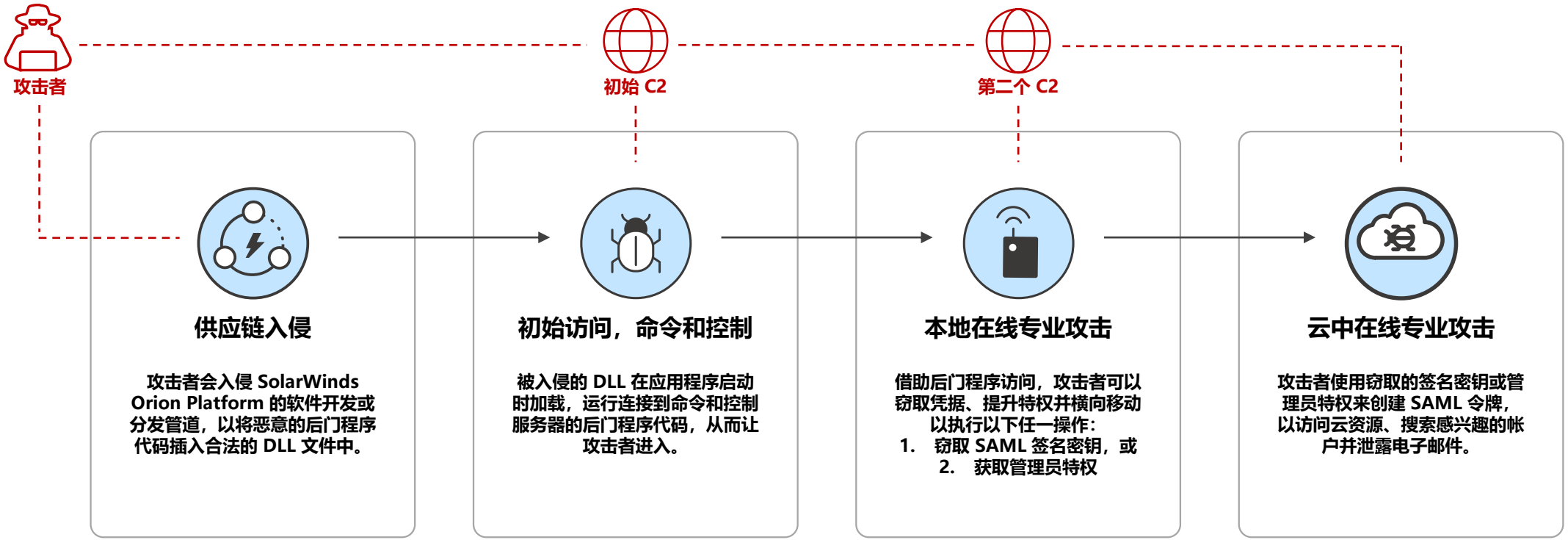
04 保护组织的 7 个步骤

05 对 SOC 的现代化进行投资的时机

Microsoft Security

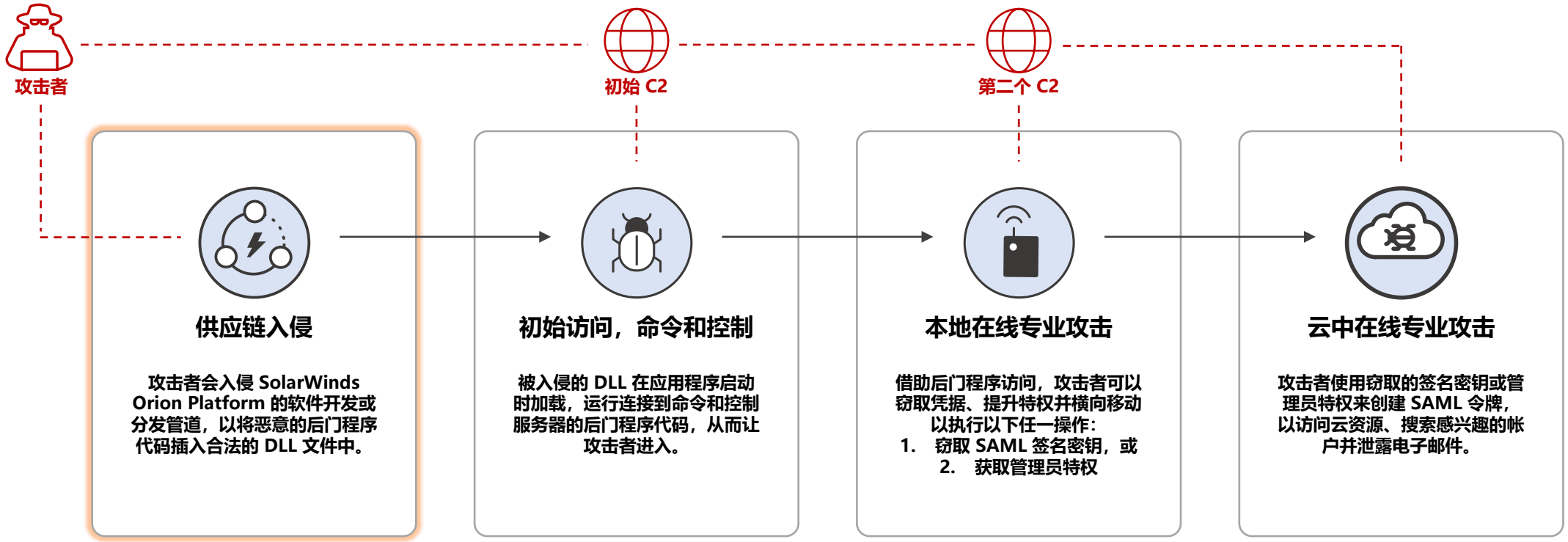
Solorigate 攻击

高级端到端攻击链



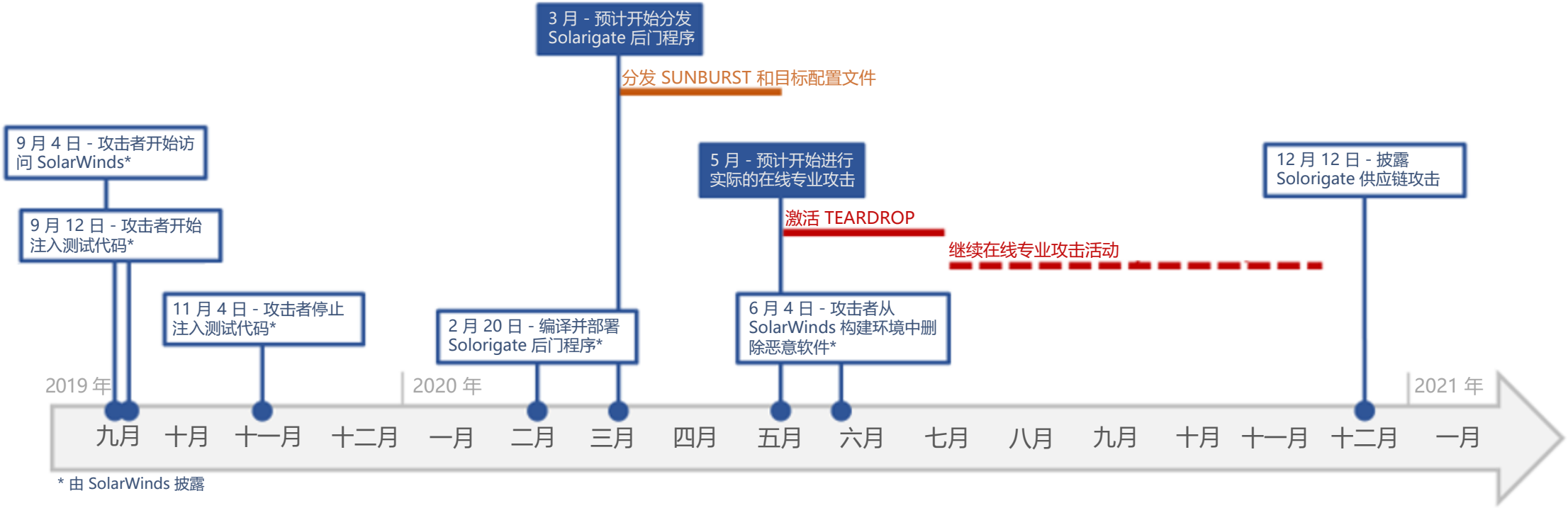
Solorigate 攻击

高级端到端攻击链



Solorigate 攻击

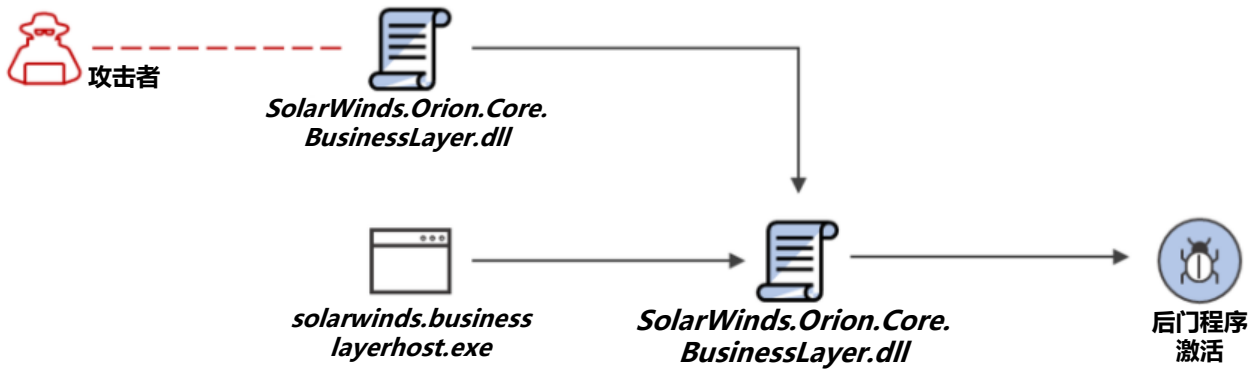
时间线



截至 2021 年 1 月 21 日，信息是正确的。请参阅 aka.ms/solorigate 以了解最新更新

供应链攻击
攻击者将恶意代码插入合法软件的 DLL 组件中。将被入侵的 DLL 分发给使用相关软件的组织。

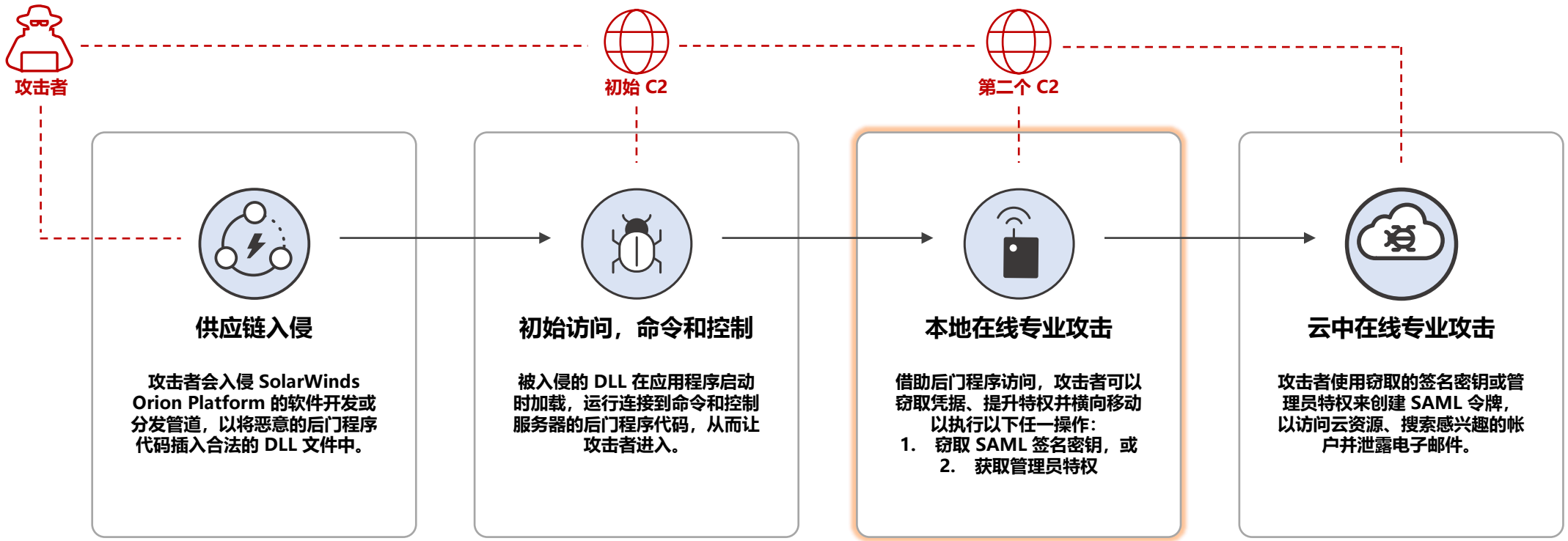
执行，持久性
启动软件时，会加载被入侵的 DLL，并且插入的恶意代码会调用包含后门程序功能的函数。




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

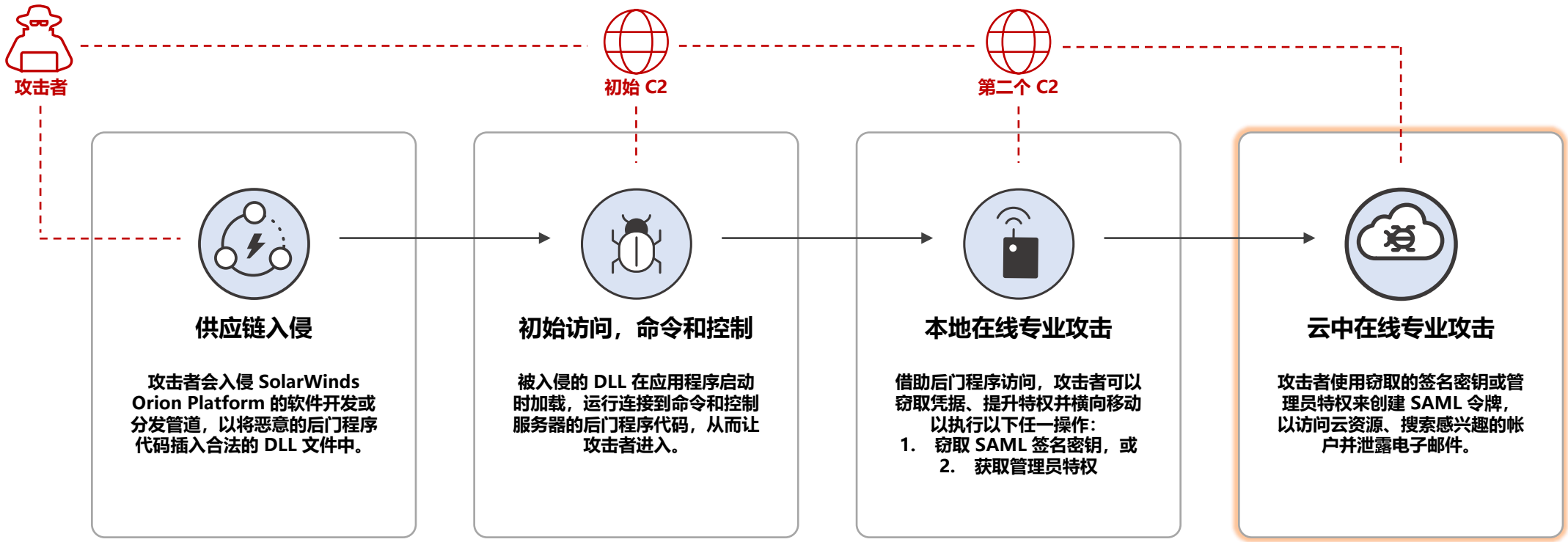
Solorigate 攻击

高级端到端攻击链



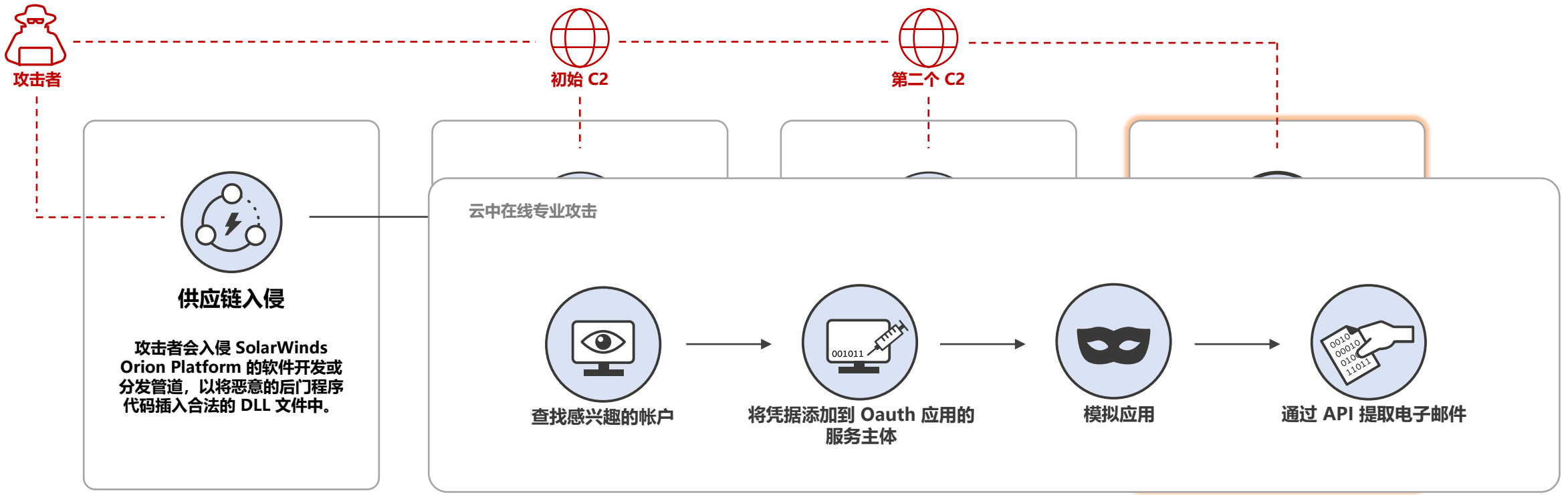
Solorigate 攻击

高级端到端攻击链



Solorigate 攻击

高级端到端攻击链



推荐的防御措施

帮助防御 Solorigate 中出现的技术的 7 个步骤

1. 运行最新的防病毒和 EDR 产品。

2. 使用网络基础结构来阻止已知的 C2 端点。

3. 保护 SAML 令牌签名密钥，并考虑 SAML 令牌签名证书的硬件安全性。对于 Active Directory 联合身份验证服务，请查看 Microsoft 的最佳做法建议：https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/best-practices-securing-ad-fs

4. 遵循管理员用户权限的最佳做法，减少属于高特权目录角色成员的用户数量。

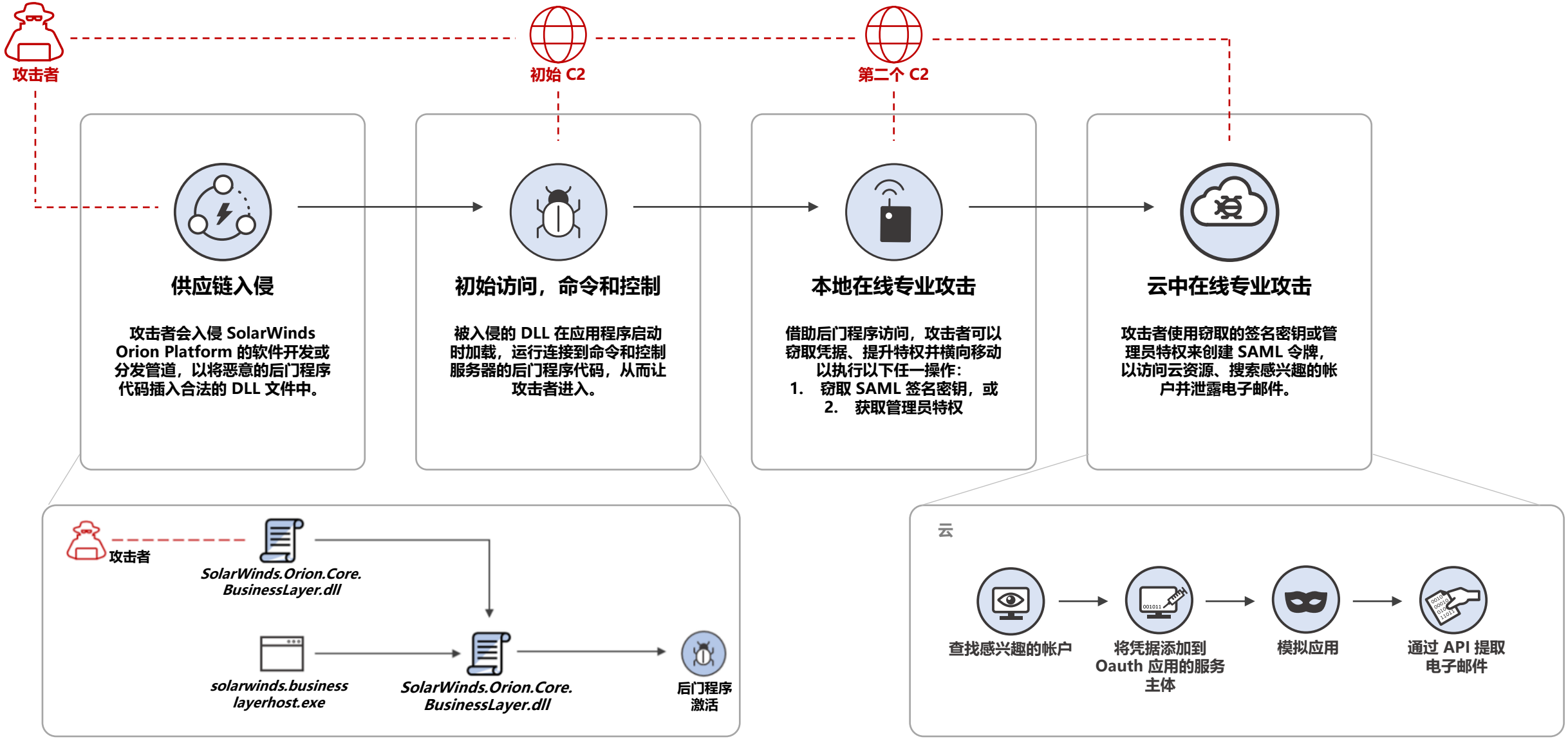
5. 确保具有管理权限的服务帐户使用安全存储的高熵机密（即证书）。监视对异常服务帐户的更改、登录和使用。

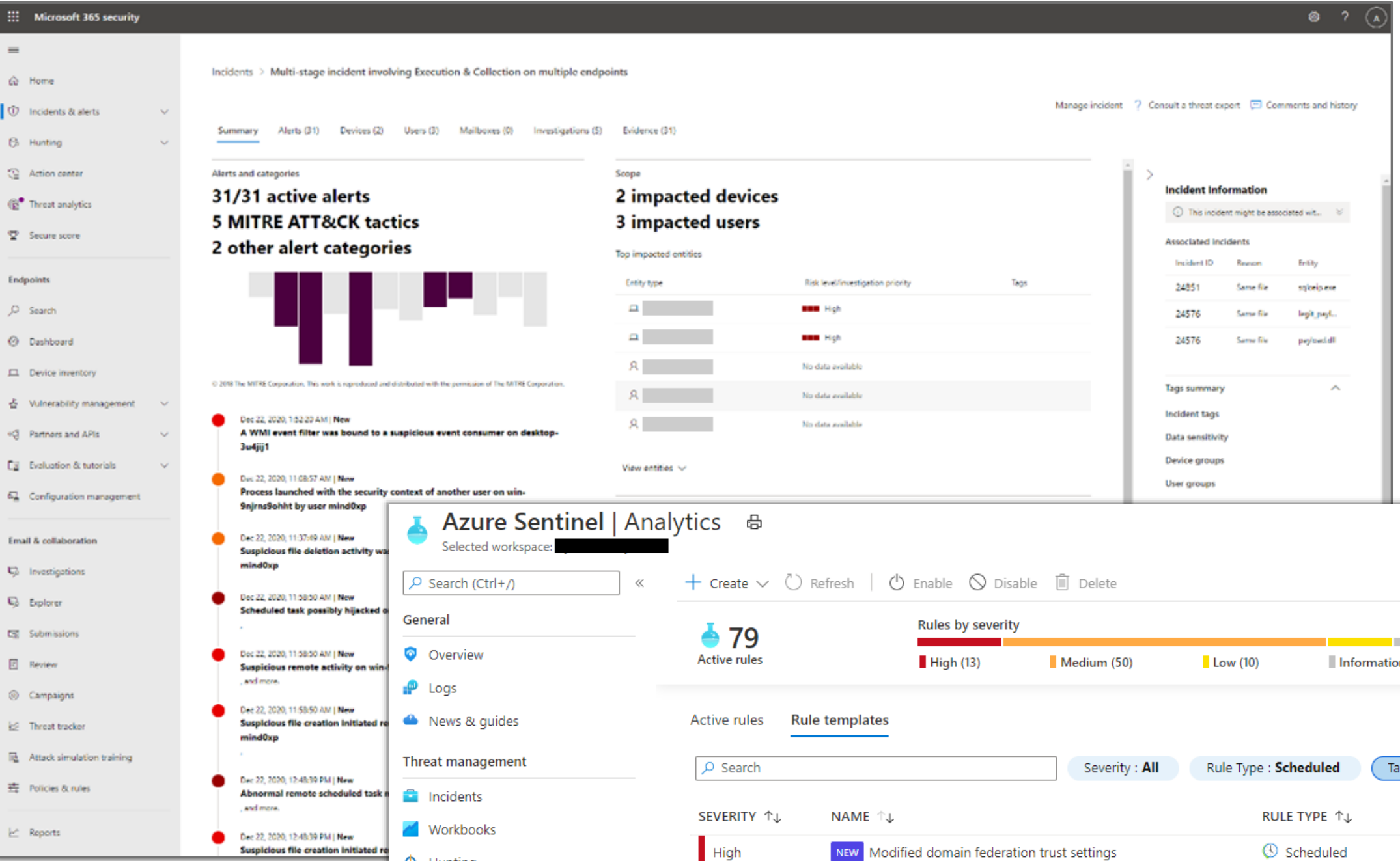
6. 删除或禁用未使用或不必要的应用程序和服务主体。减少对仍拥有的应用程序和服务主体的权限。

7. 请参阅以下附加建议，以保护 Azure AD 身份基础结构：https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity

Solorigate 攻击

高级端到端攻击链




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

Solorigate 视频系列

后续步骤

01 在此位置观看 Solorigate 视频系列

02 请访问 Microsoft 安全以获取更多更新：www.microsoft.com/en-us/security/business

03 阅读博客文章：www.microsoft.com/security/blog

https://aka.ms/solorigate

Microsoft Security

Microsoft

© Microsoft Corporation 版权所有。保留所有权利。