Microsoft

Bộ bảo vệ M365

Corina Feuerstein

Trưởng nhóm Quản lý Chương trình

Bộ bảo vệ M365

18/02/2021

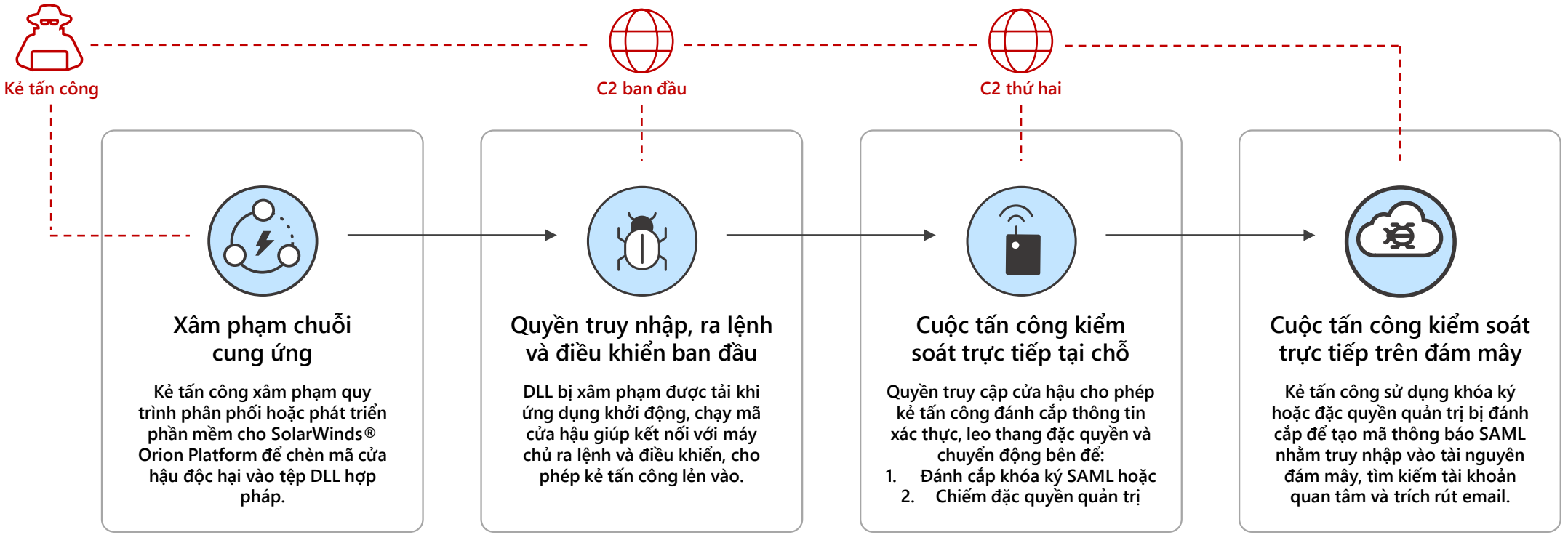
Tổng quan về Solorigate

Sử dụng Bộ bảo vệ Microsoft 365 để phát hiện, bảo vệ và khắc phục

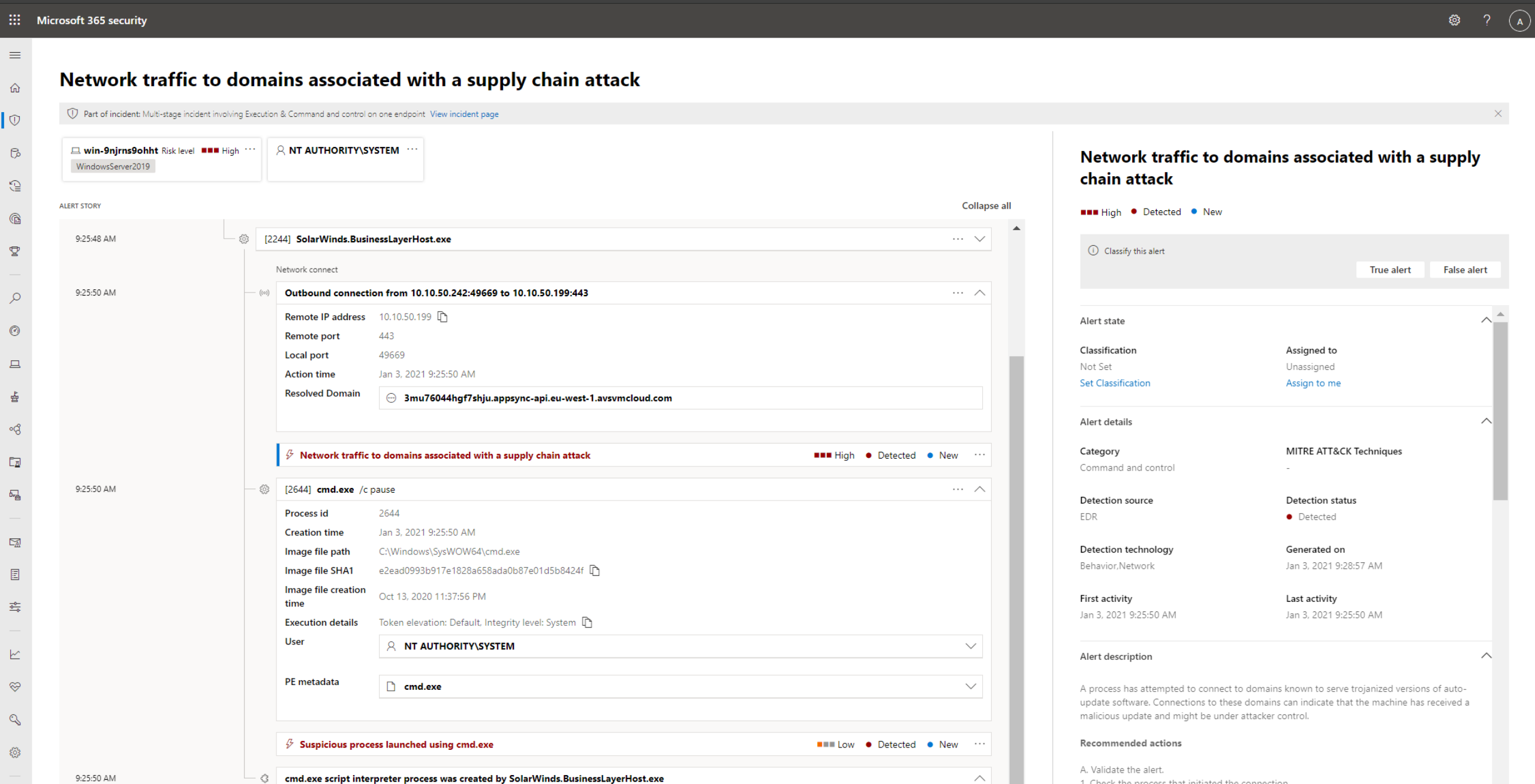
1. Cách cuộc tấn công Solorigate diễn ra
2. Phát hiện và chặn hoạt động điểm cuối tại chỗ
3. Phát hiện sự xâm phạm danh tính và chuyển sang đám mây
4. Phát hiện và ứng phó với hoạt động đáng ngờ của ứng dụng đám mây
5. Hiểu mức độ tiếp xúc của tổ chức và các biện pháp giảm thiểu bằng cách sử dụng Phân tích Mối đe dọa
6. Tìm kiếm trên toàn bộ miền với Bộ bảo vệ Microsoft 365

Microsoft Security

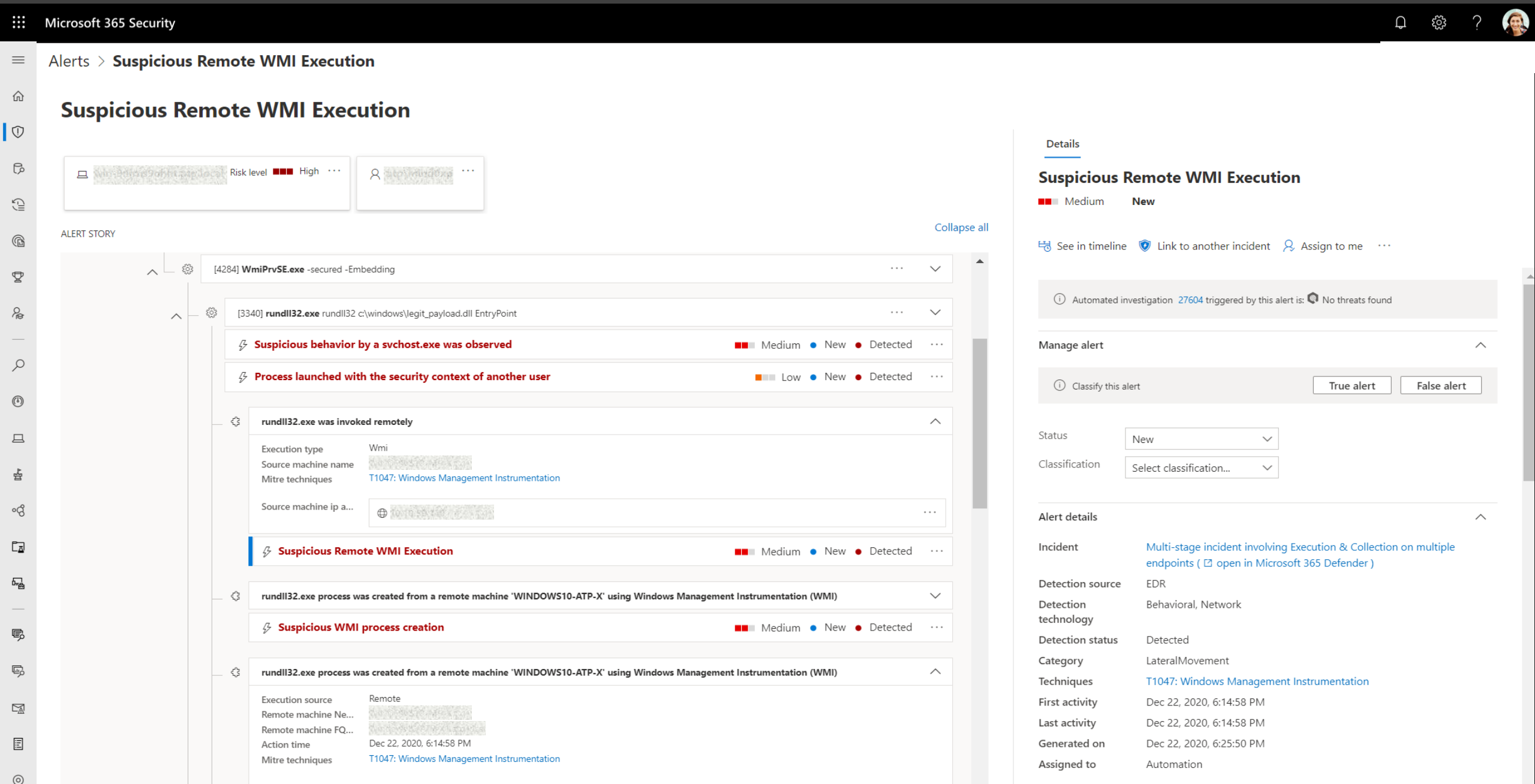
Tổng quan về Solorigate



Liên lạc C2 độc hại bị MDE chặn

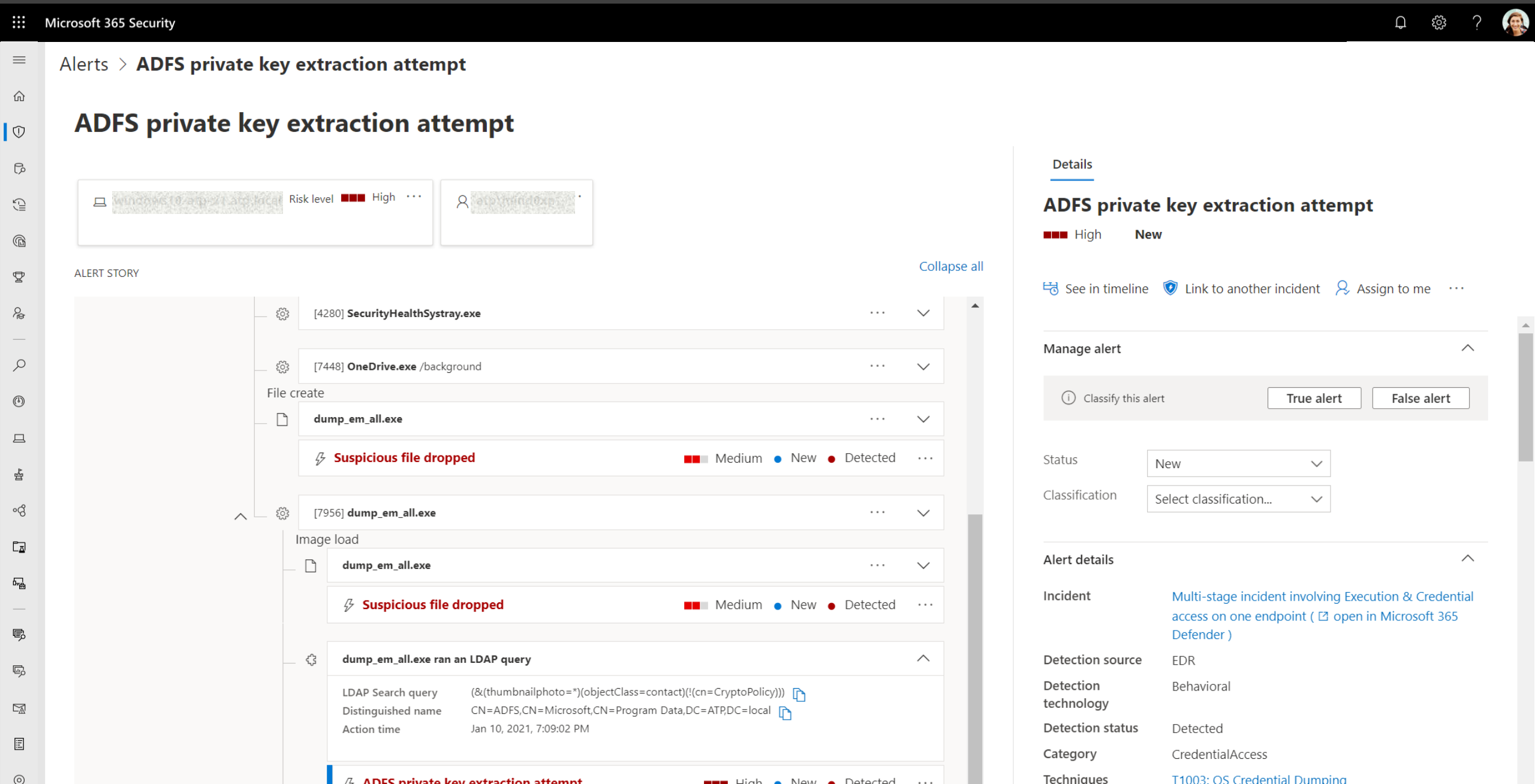


Hoạt động chuyển động bên được MDE phát hiện



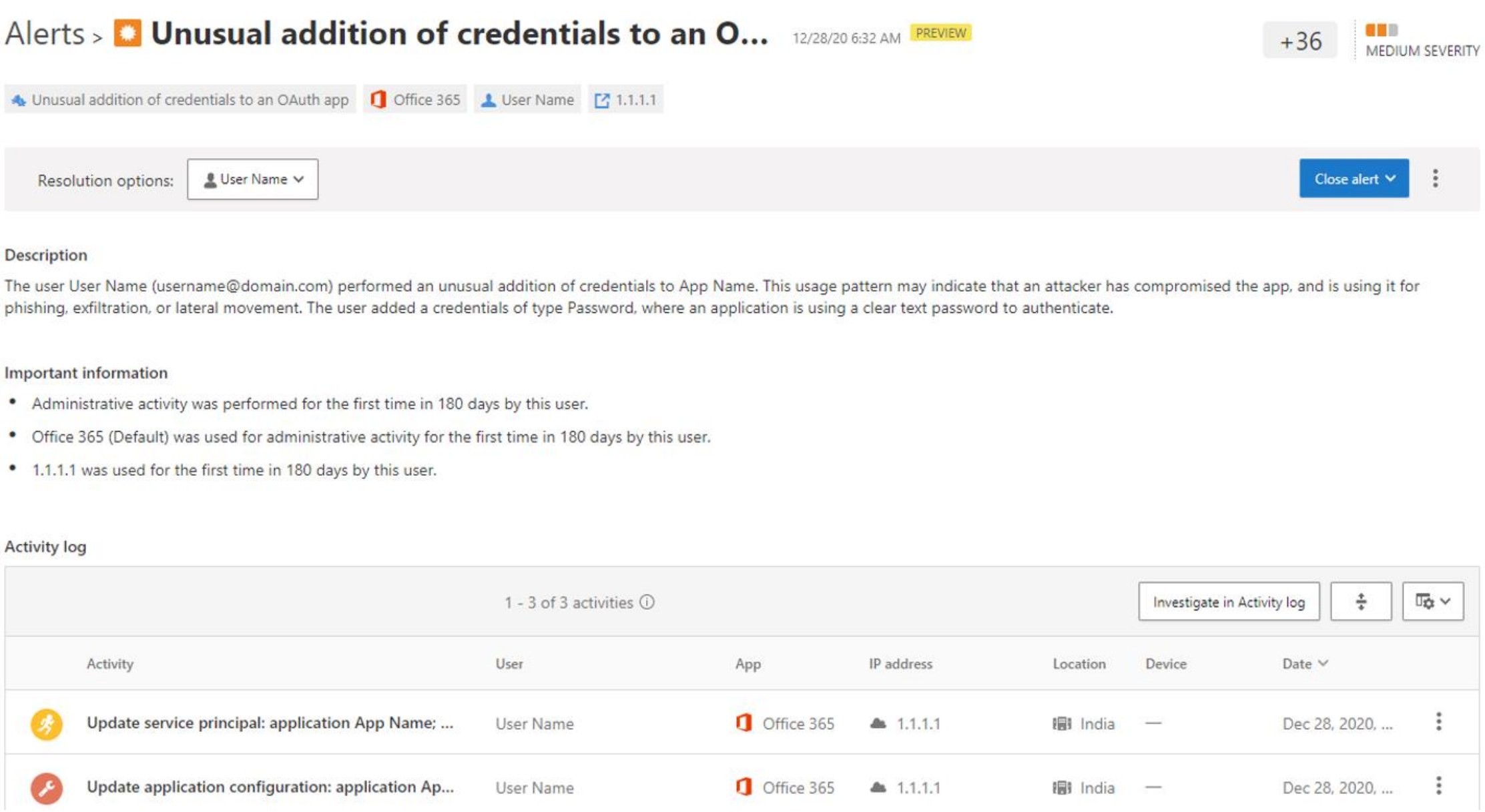
Xâm phạm ADFS bằng cách đánh cắp khóa chứng chỉ SAML hoặc sửa đổi các mục tin cậy của liên kết

Nghi ngờ hoạt động truy nhập khóa ADFS



Sử dụng mã thông báo SAML giả mạo để tồn tại trong đám mây, truy nhập tài nguyên đám mây và trích rút email.

Thao tác bất thường đối với ứng dụng Oauth được MCAS phát hiện



Báo cáo Solorigate về Phân tích mối đe dọa

Microsoft 365 Security

Threats > Solorigate supply chain attack

Overview | Analyst report | Related incidents | Impacted assets | Prevented email attempts | Mitigations

Microsoft security researchers recently discovered a sophisticated attack where an adversary inserted malicious code into a supply chain development process. A malicious software class was included among many other legitimate classes and then signed with a legitimate certificate. The resulting binary included a backdoor and was then discreetly distributed into targeted organizations. This attack was discovered as part of an ongoing investigation.

Cybercriminals target supply chains and look for weaknesses they can exploit to discreetly enter another target environment. In this case, attackers targeted the SolarWinds Orion Platform to infiltrate the supply chain that helps businesses manage networks, systems, and information technology infrastructure. This attack leveraged the trust associated with the supplier and certificate to insert targeted code to use in a larger campaign.

Based on research, this attack represents nation-state activity at significant scale, aimed at both the government and private sector. The actor is known to be focused on high value targets such as government agencies and cybersecurity companies.

Microsoft Defender Antivirus protects against this threat. It blocks the known malicious SolarWinds binaries associated with this threat on your device.

Read the full analyst report

Report details

Report type	Published	Last updated
Attack campaigns	12/14/20, 7:59 AM	12/21/20, 9:38 AM

Related incidents

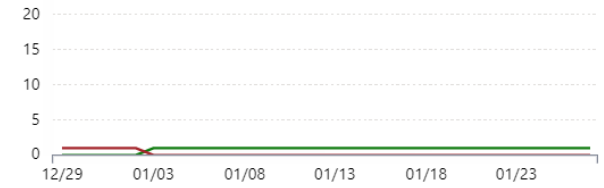
0 related alerts in your org

Incidents severity

High | Medium | Low | Informational | No active incidents

View all related incidents

Alerts over time



Resolved alerts | Active alerts

Impacted assets

0 impacted devices

Devices 0 / 1

Mailboxes**

** Access needed. Contact a global administrator to access Office 365 data.

Assets with active alerts | Assets with resolved alerts | Assets with no alerts

View all impacted assets

Prevented email attempts

Secure configuration status

1.43k misconfigured devices

Vulnerability patching status

0 vulnerable devices

Báo cáo Solorigate về Phân tích mối đe dọa

Microsoft 365 Security

Threats > Solorigate supply chain attack

Overview | Analyst report | Related incidents | Impacted assets | Prevented email attempts | **Mitigations**

Secure configuration status

1.43k misconfigured devices

Exposed | Secure | Unknown | Not applicable

Vulnerability patching status

0 vulnerable devices

Exposed | Secure

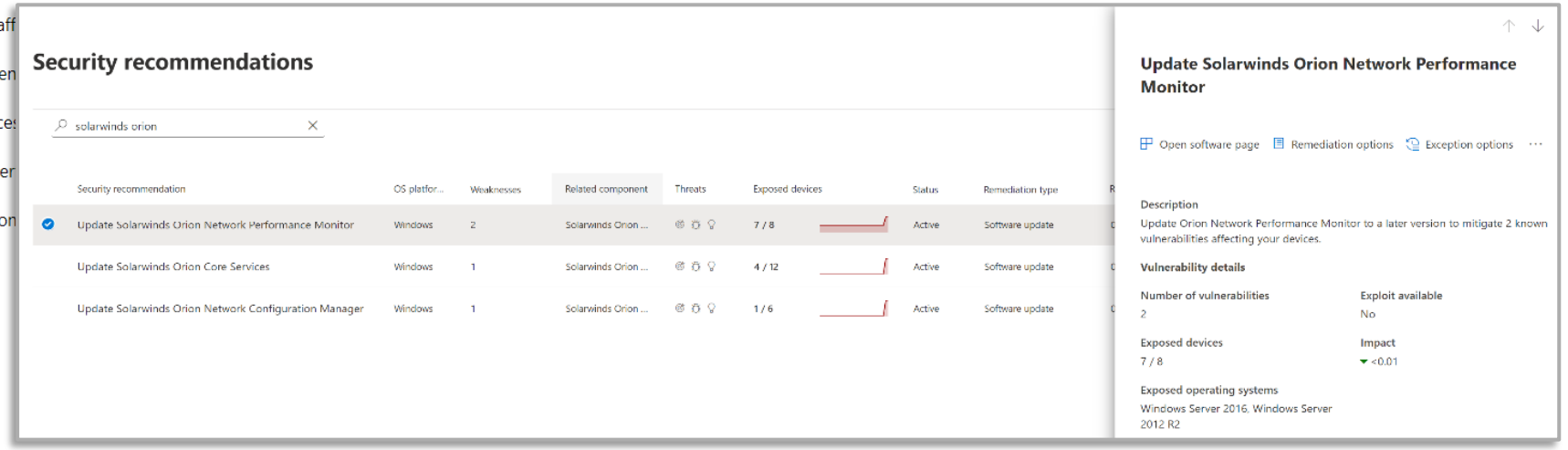
Mitigation details

Secure configuration

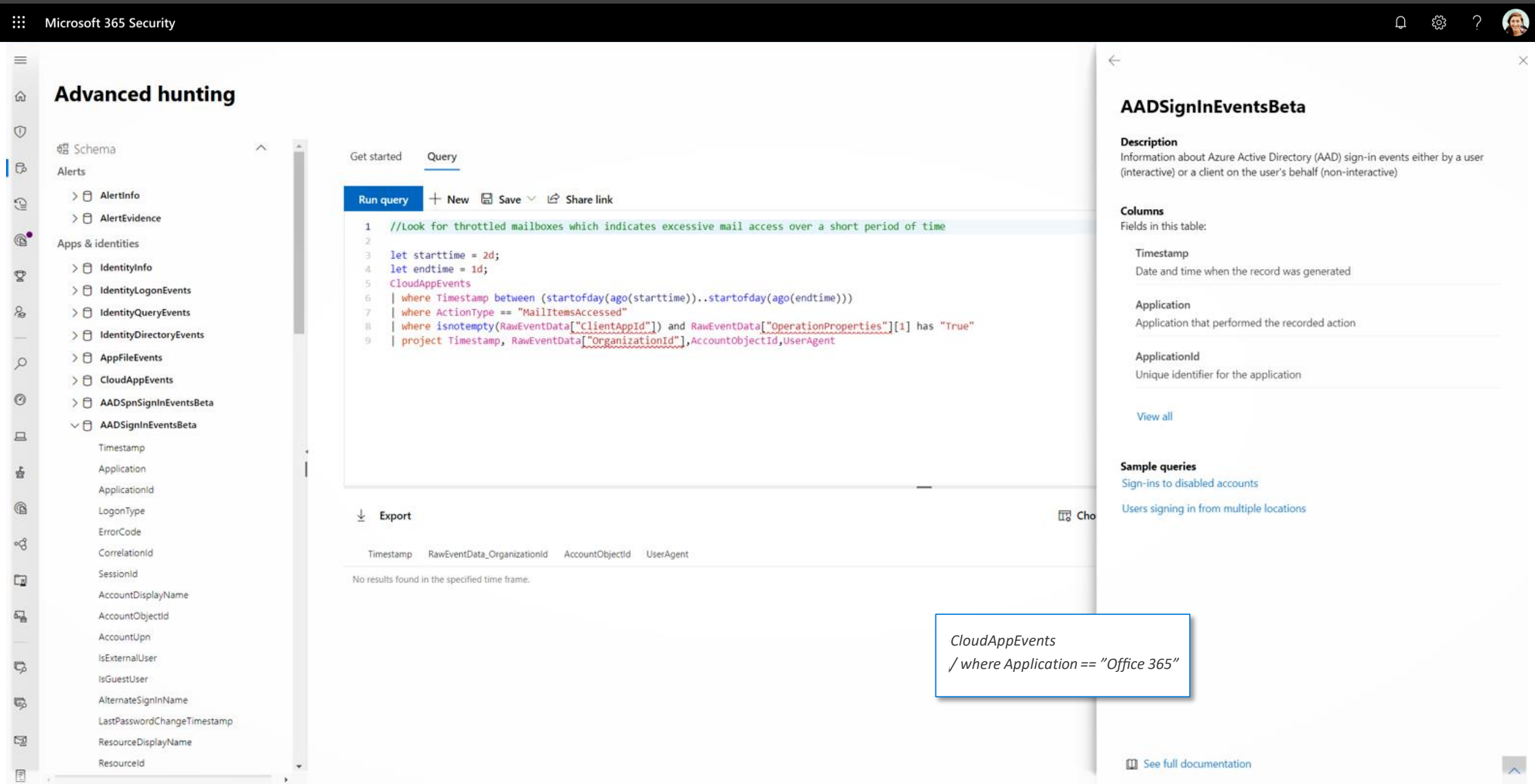
Vulnerabilities

Product/Component	Vulnerability IDs	Exposed devices
orion_user_device_tracker	TVM-2020-0002	0
highavailability_orion_plugin	TVM-2020-0002	0
orion_netflow_traff		
orion_improvemen		
orion_core_service		
orion_network_per		
orion_network_con		

ID lỗ hổng:
TVM-2020-0002



Dữ liệu về Azure AD và Ứng dụng Đám mây mới trong Tìm kiếm Nâng cao



CloudAppEvents
/ where Application == "Office 365"

Điều tra các cảnh báo và sự cố liên quan đến Solorigate trong Bộ bảo vệ Microsoft 365

Microsoft 365 Security

Incidents > Multi-stage incident involving Execution & Collection on multiple endpoints

Manage incident | Consult a threat expert | Comments and history

Summary | Alerts (50) | Devices (2) | Users (3) | Mailboxes (0) | Investigations (6) | Evidence (154)

Alerts and categories

50/50 active alerts
7 MITRE ATT&CK tactics
2 other alert categories

Dec 22, 2020, 1:52:20 AM | **New**
A WMI event filter was bound to a suspicious event consumer on

Dec 22, 2020, 11:08:57 AM | **New**
Process launched with the security context of another user on **by user**

Dec 22, 2020, 11:37:49 AM | **New**
Suspicious file deletion activity was observed on : by user

Dec 22, 2020, 11:58:50 AM | **New**
Scheduled task possibly hijacked on : by user

Dec 22, 2020, 11:58:50 AM | **New**
Suspicious remote activity on : by user
, and more.

Dec 22, 2020, 11:58:50 AM | **New**
Suspicious file creation initiated remotely on : by user

Scope

2 impacted devices
3 impacted users

Top impacted entities

Entity type	Risk level/investigation priority	Tags
	High	
	High	
	No data available	
	No data available	
	No data available	

View entities

Evidence

154 entities found

Evidence remediation status

Not Found | Other

View all entities

Incident Information

This incident might be associated w...

Associated incidents

Incident ID	Reason	Entity
24851	Same file	sqlceip.exe
24576	Same file	legit_payl...
24576	Same file	payload.dll

Tags summary

Incident tags

Incident details

Status
Active

Severity
High

Incident ID
24963

First activity
First - Dec 22, 2020, 1:52:20 AM

Last activity
Last - Dec 28, 2020, 3:04:12 PM

Classification
Not set

Determination
Not set

Chuỗi video về Solorigate

Bước tiếp theo

01. Xem chuỗi video về Solorigate tại vị trí này

02. Truy nhập Microsoft Security để biết thêm thông tin cập nhật: https://www.microsoft.com/vi-vn/security/business

03. Đọc bài đăng blog trên: www.microsoft.com/security/blog

https://aka.ms/solorigate

Microsoft Security

Microsoft