Microsoft

M365 Defender

Корина Фюерщайн

Ръководител за управление на програмите

M365 Defender

18 февруари 2021 г.

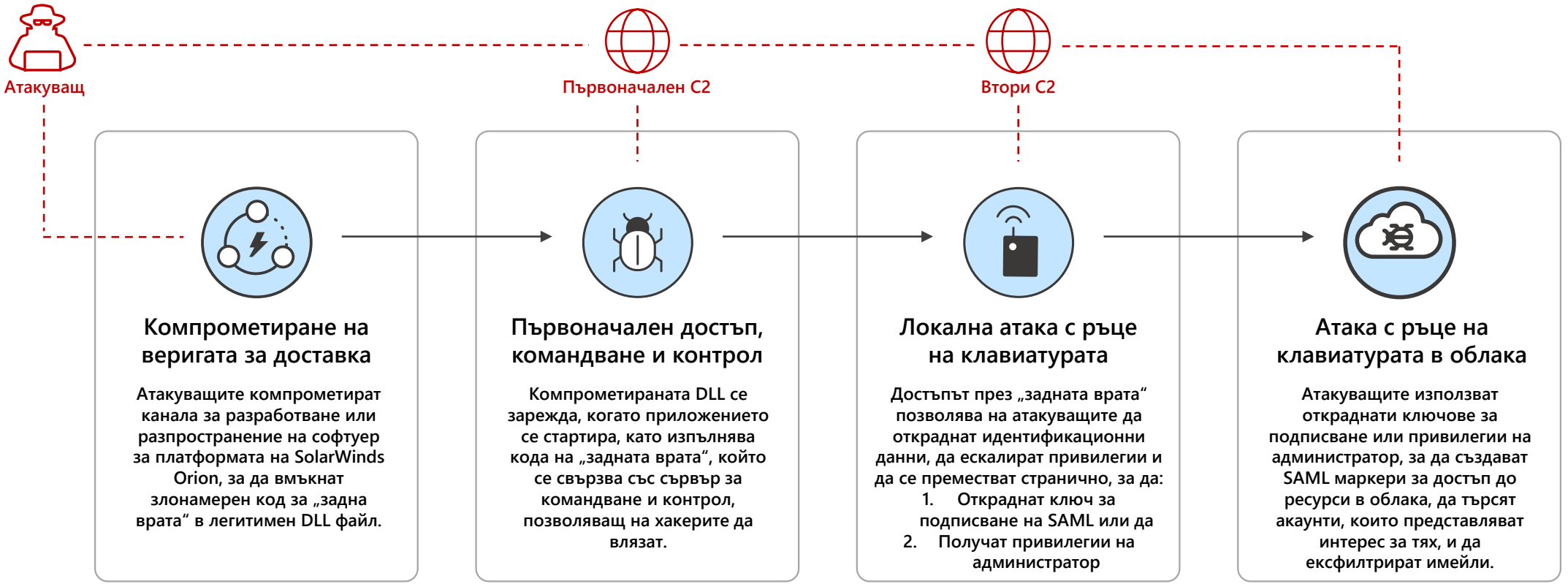
Общ преглед на Solorigate

Използване на Microsoft 365 Defender за откриване, защита и възстановяване

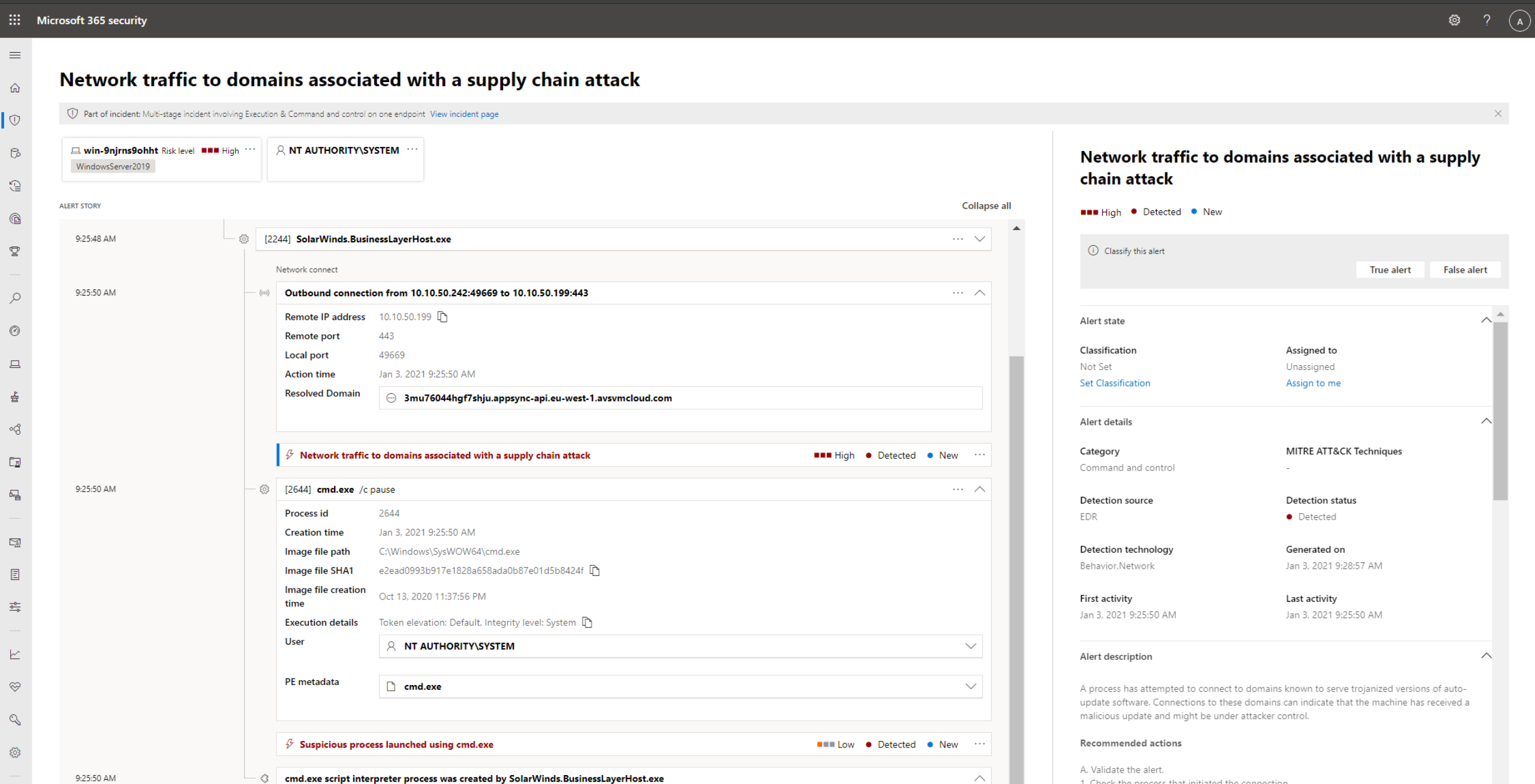
1. Как се случи атаката Solorigate
2. Откриване и блокиране на локална дейност на крайна точка
3. Откриване на компрометиране на самоличности и прехвърляне към облака
4. Откриване и реагиране на съмнителни действия в приложения в облака
5. Разбиране на излагането на риск на организацията и намаляване на риска с помощта на набор анализи за заплахи
6. Проактивно търсене в различни домейни с Microsoft 365 Defender

Microsoft Security

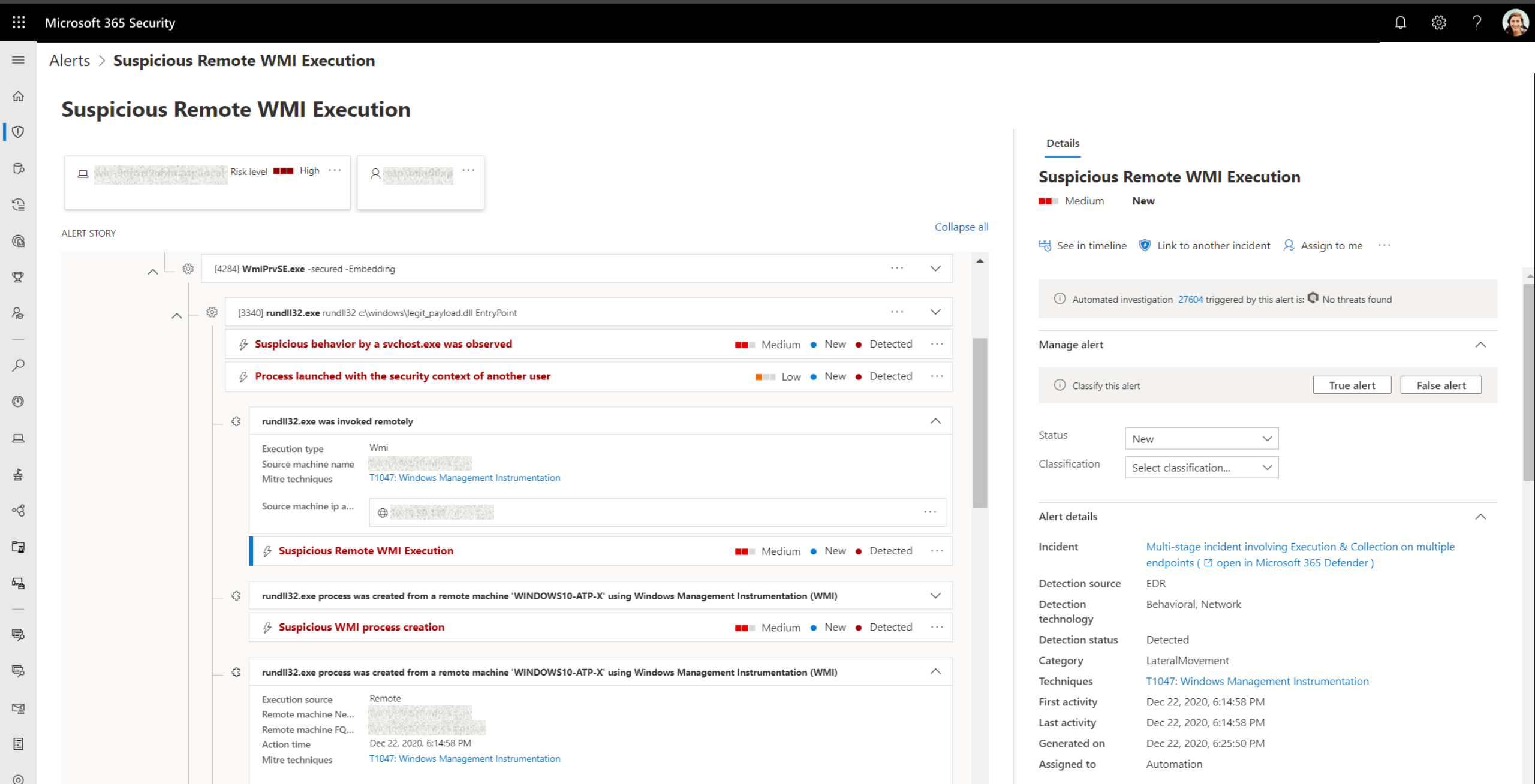
Общ преглед на Solorigate



Злонамерена комуникация с C2, блокирана от MDE

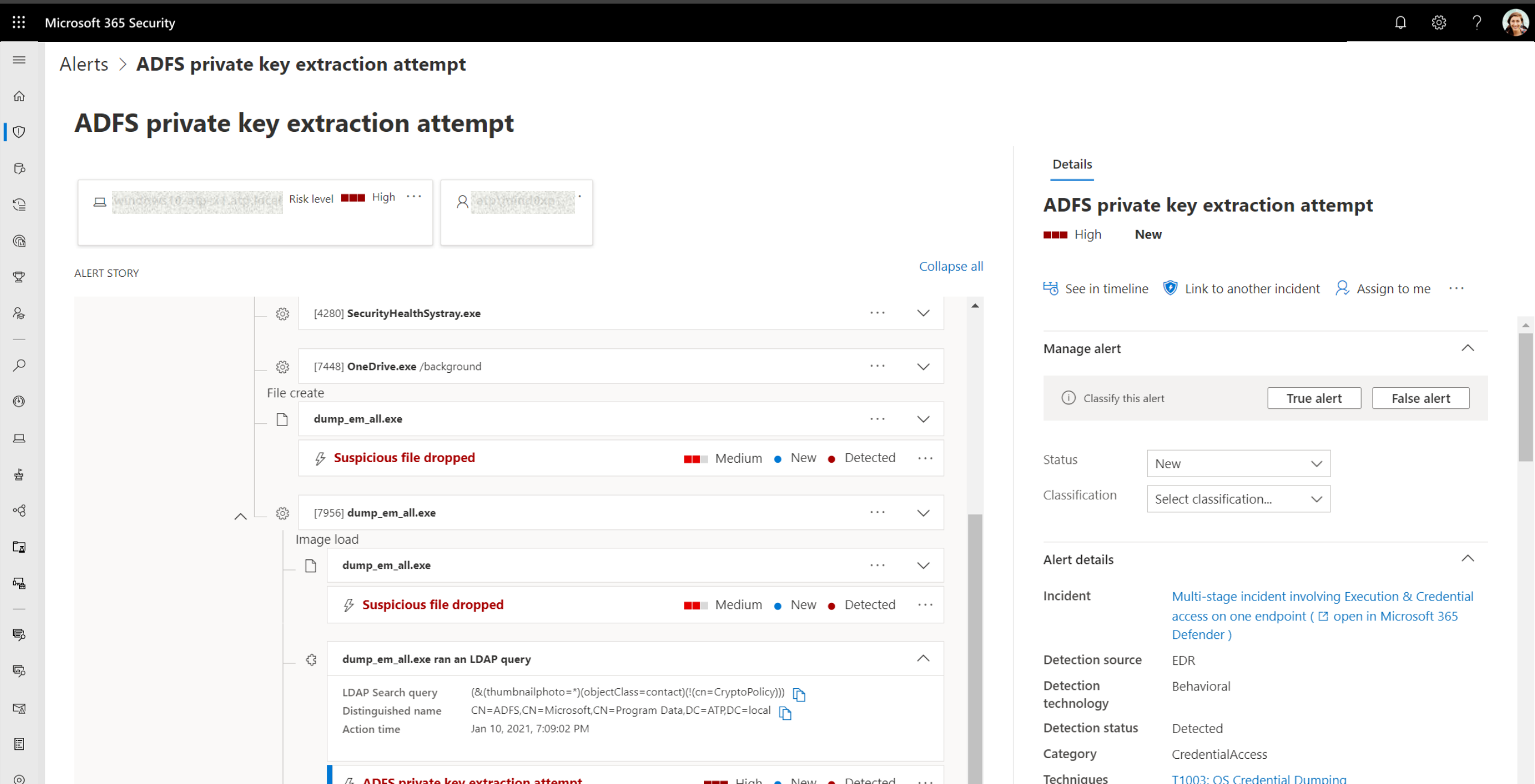


Странично движение, открито от MDE



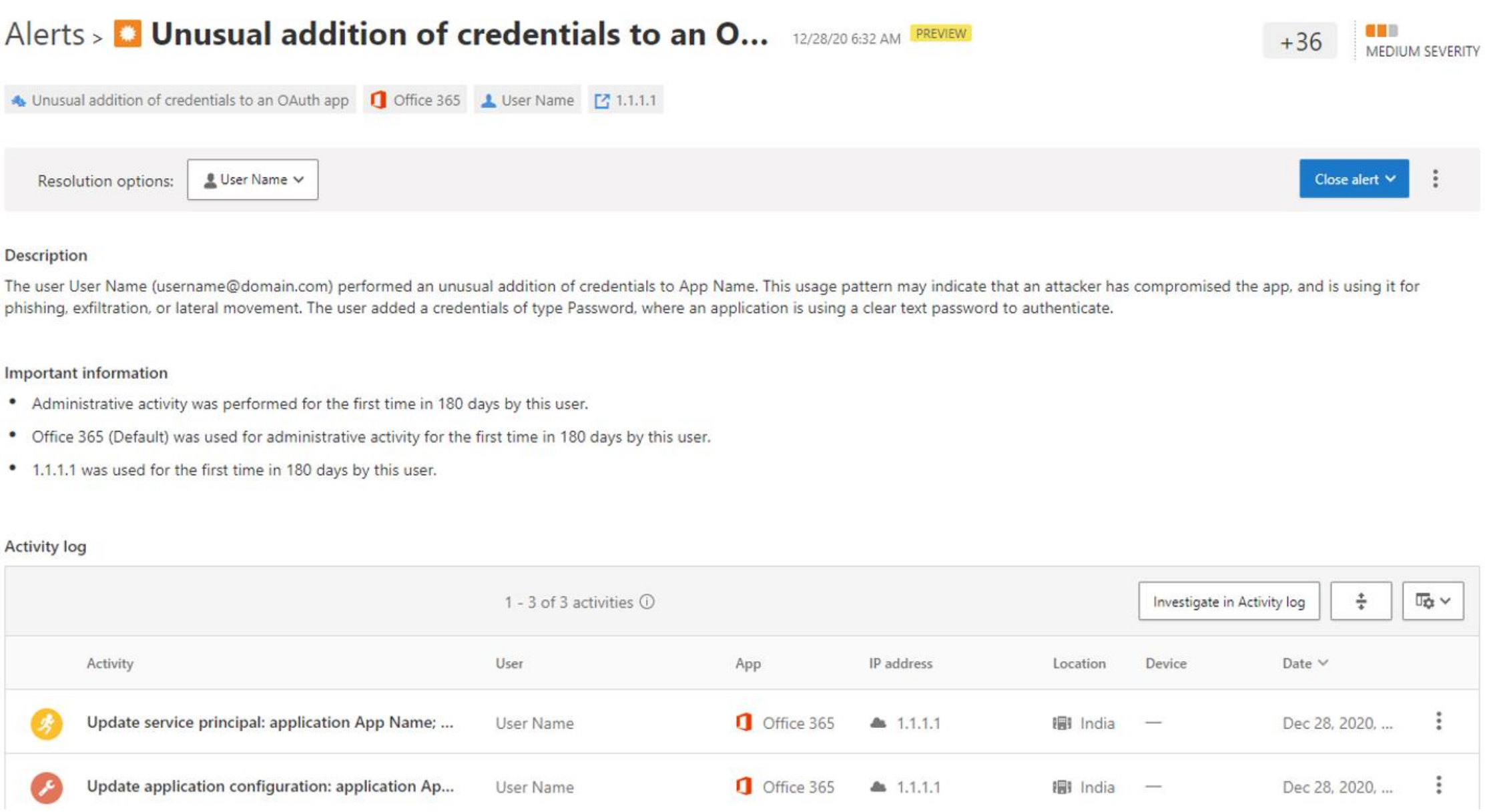
Компрометиране на ADFS чрез кражба на SAML ключа за сертификат или промяна на гаранти за федериране

Подозрителен достъп до ключове в ADFS



Използване на фалшиви SAML маркери, за да останат в облака, да имат достъп до ресурси в облака и да ексфилтрират имейли.

Необичайна манипулация на Oauth приложение, открито от MCAS



Отчет за Solorigate на набора анализи за заплахи

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

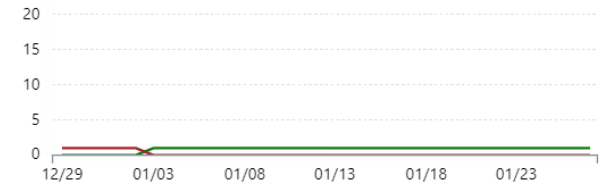
0 related alerts in your org

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

Отчет за Solorigate на набора анализи за заплахи

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

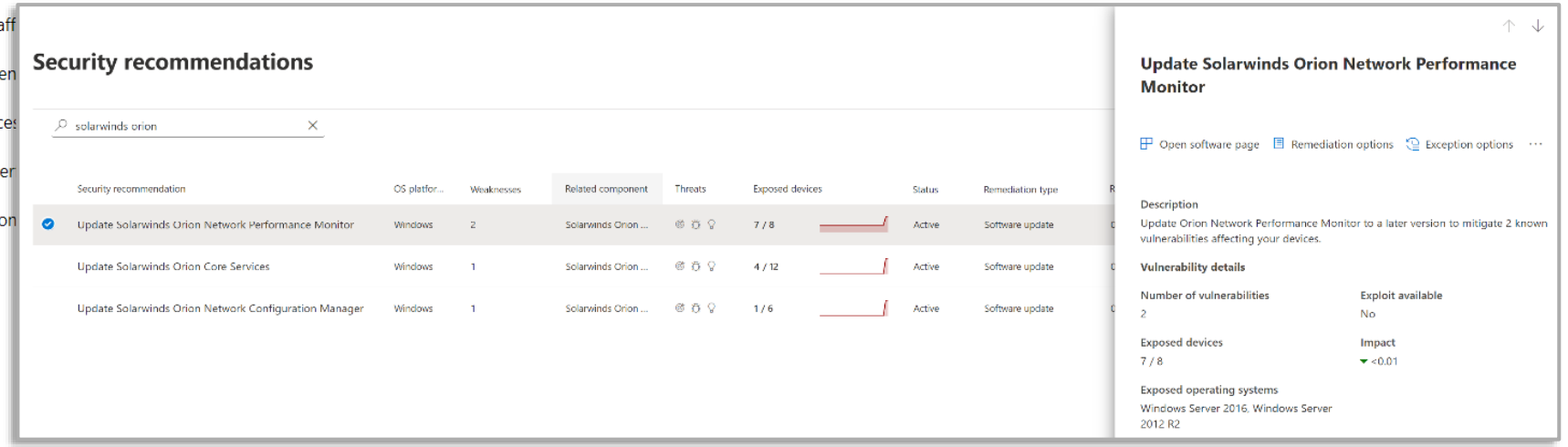
Mitigation details

Secure configuration

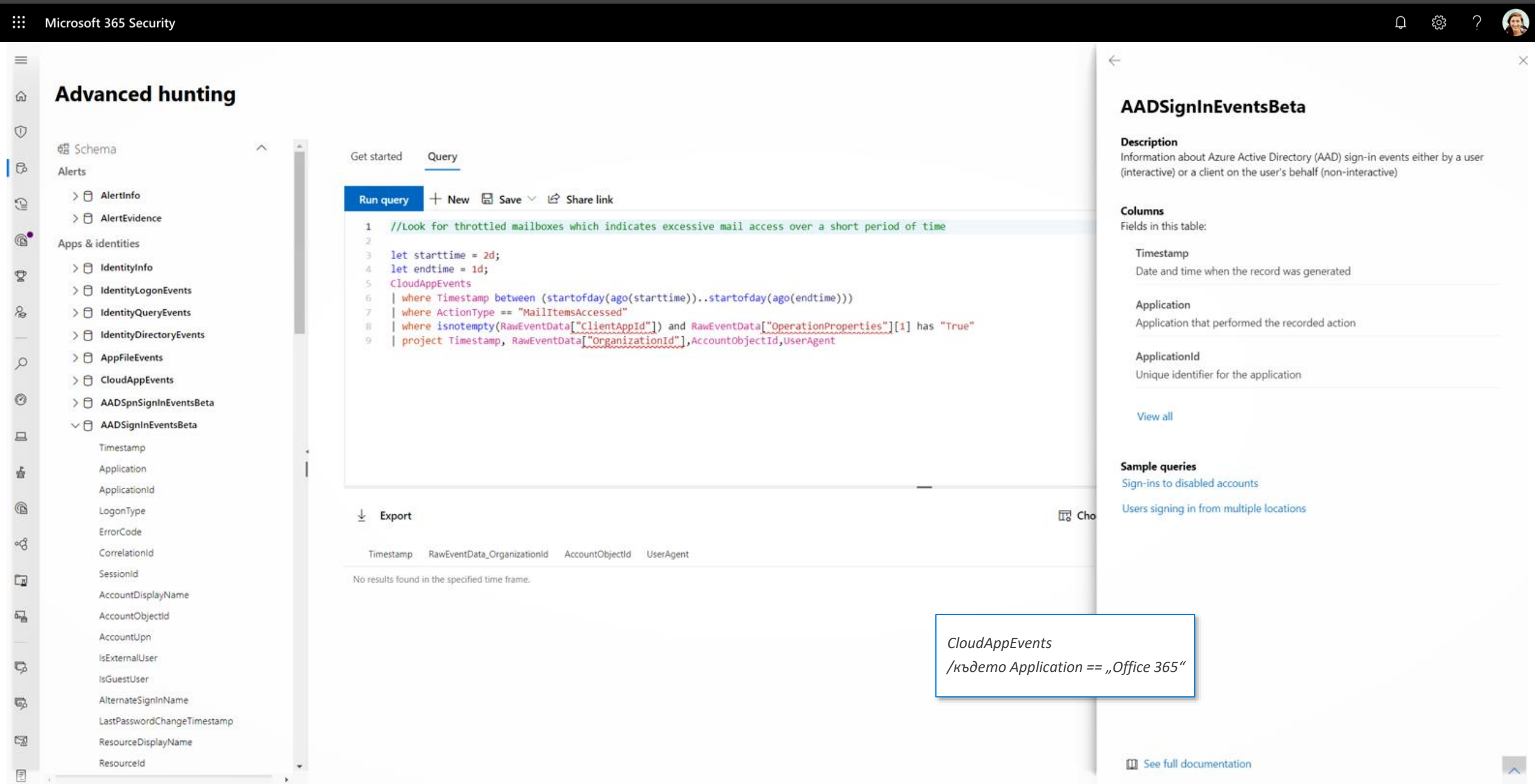
Vulnerabilities

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		

ИД на уязвимост:
TVM-2020-0002



Нови данни за Azure AD и приложения в облака в „Разширено проактивно търсене“



CloudAppEvents
/където Application == „Office 365“

Проучване на свързани със Solorigate известявания и инциденти в Microsoft 365 Defender

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

Поредица от видеоклипове за Solorigate

Следващи стъпки

01. Гледайте поредицата видеоклипове за Solorigate на това място

02. Посетете Microsoft Security за още актуализации: www.microsoft.com/en-us/security/business

03. Прочетете публикациите в блога на адрес: www.microsoft.com/security/blog

https://aka.ms/solorigate

Microsoft Security