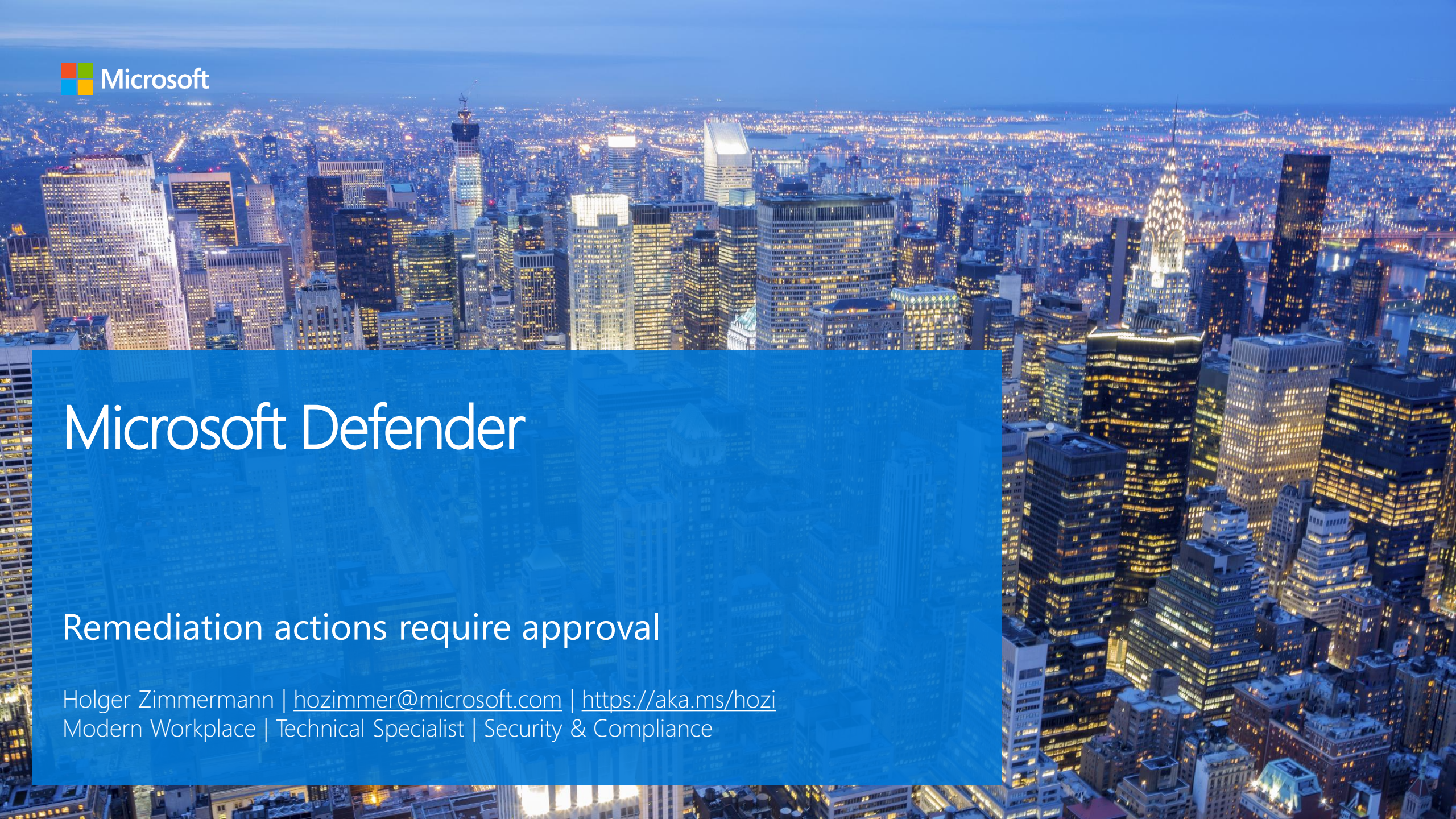


Microsoft Defender

Remediation actions require approval

Holger Zimmermann | hozimmer@microsoft.com | https://aka.ms/hozi
Modern Workplace | Technical Specialist | Security & Compliance

30 days

Incidents

Incident name	Severity	Categories	Alerts	Machines	Users	Last activity	Assigne
EICAR Test File	Informational	Malware	1	desktop-966uv3q		9/27/19, 1:48 PM	Unassig
4	High	Suspicious activity	1	hozimmer-slt2		9/27/19, 10:27 AM	Unassig
3	Medium	Execution, Defense evasion	2	hozimmer-slt2	hozimmer-slt2\zimme	9/27/19, 7:15 AM	holger

EICAR Test File

Open incident page | Assign to me

Status: Active
Assigned to: Unassigned
Severity: Informational
Classification: (Not set)
Set status and classification
Category: Malware
Activity time: First - Sep 27, 2019, 1:48:42 PM
Last - Sep 27, 2019, 1:48:42 PM

Alerts (1)

Title	Severity	Status
'EICAR_Test_File' malware was detected	Informational	New

Dashboards
Incidents
Machines list
Alerts queue
Automated investigations
Automated investigations
Action center
Advanced hunting
Reports
Partners & APIs
Threat & Vulnerability Management
Dashboard
Security recommendations
Remediation
Software inventory
Weaknesses
Evaluation and tutorials
Service health
Configuration management
Settings

Last Week | Customize columns | Export | 30 items per page

Automated Investigations

Triggering alert	ID	Status	Detection Source	Entities	Start Date	Duration
'EICAR_Test_File' malware was detected	4	Waiting for machine	Antivirus	desktop-966uv3q	9/27/19, 1:50 PM	40:03m
Suspicious process injection observed	3	Remediated	EDR	hozimmer-slt2	9/27/19, 7:17 AM	32:35m
'Tiggre' malware was detected	2	Remediated	Antivirus	hz-surfacego	9/27/19, 6:33 AM	27:58m

Filters

Status
- [x] Any
- [ ] Remediated 2
- [ ] Waiting for machine 1

Triggering alert
- [x] Any
- [ ] 'EICAR_Test_File' malware was detected 1
- [ ] 'Tiggre' malware was detected 1
- [ ] Suspicious process injection observed 1

Detection Source
- [x] Any
- [ ] Antivirus 2
- [ ] EDR 1

Entities
- [x] Any
- [ ] desktop-966uv3q 1
- [ ] hozimmer-slt2 1
- [ ] hz-surfacego 1

Dashboards
Incidents
Machines list
Alerts queue
Automated investigations
Advanced hunting
Reports
Partners & APIs
Threat & Vulnerability Management
Evaluation and tutorials
Service health
Configuration management
Settings

Last Week

Automated Investigations

Triggering alert	ID	Status	Detection Source	Entities
'EICAR_Test_File' malware was detected	4	Waiting for machine	Antivirus	desktop-966uv3c
Suspicious process injection observed	3	Remediated	EDR	hozimmer-slt2
'Tiggre' malware was detected	2	Remediated	Antivirus	hz-surfacego

'EICAR_Test_File' malware was detected

Open investigation page | Cancel

ID	'EICAR_Test_File' malware was detected
Status	Pending approval
Duration	00:41:07
Started	Sep 27, 2019, 1:[illegible] PM
Pending time	2s

Triggering alert

Severity	Informational
Incident	5
Threat found	EICAR_Test_File
Category	Malware
Detection source	Antivirus
Generated on	Sep 27, 2019, 1:50:54 PM
First activity	Sep 27, 2019, 1:48:42 PM
Last activity	Sep 27, 2019, 1:48:42 PM
Assigned to	(Unassigned)
Alert description	Malware and unwanted software are undesirable applications that perform annoying, disruptive, or harmful actions on affected machines. Some of these undesirable applications can replicate and spread from one machine to another. Others are able to receive commands from remote attackers and perform ac...

Go to alert page to see full description

Open alert page

Related machine

Name:	desktop-966uv3q
Domain	AAD joined
OS	Windows 10 x64 (version 1903 build 18362)
Risk level	No known risks
Exposure level	No data available

Dashboards
Incidents
Machines list
Alerts queue
Automated investigations
Advanced hunting
Reports
Partners & APIs
Threat & Vulnerability Management
Evaluation and tutorials
Service health
Configuration management
Settings

'EICAR_Test_File' malware was detected

Investigation #4 is running - Pending approval

Started
Sep 27, 2019, 1:50:56 PM
Total pending time: 2s

00:41:59
Pending approval

Cancel Investigation

Comments (0)

Investigation details

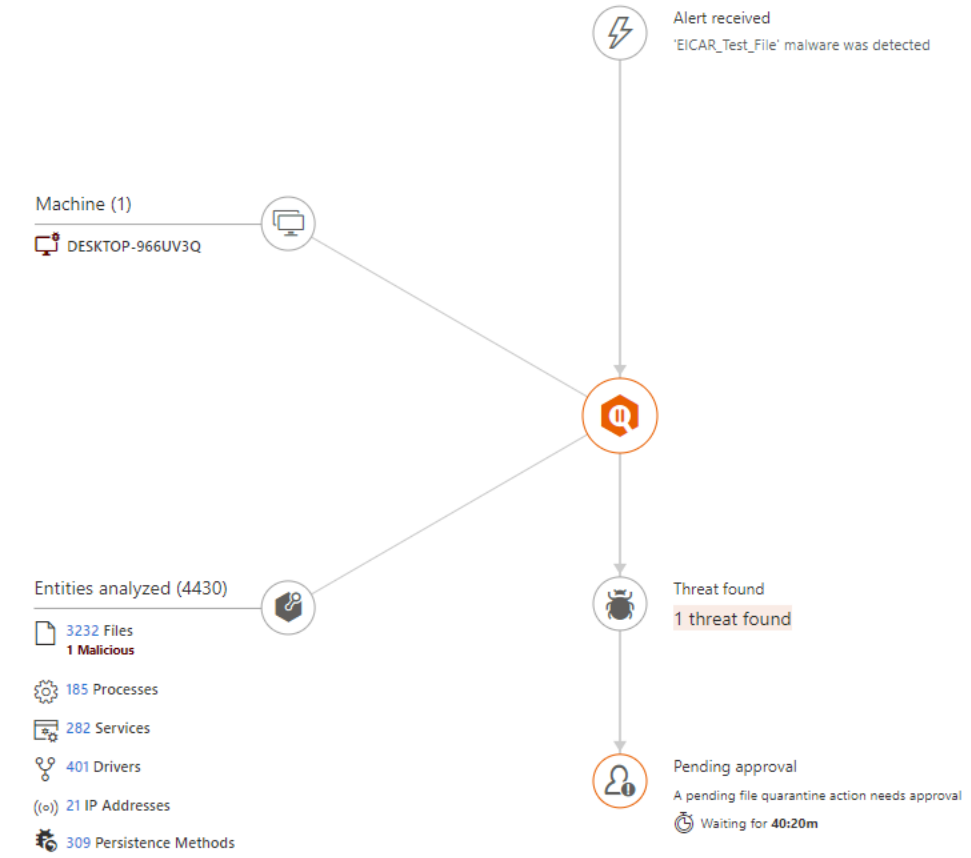
Status
Pending approval
Remediation actions require review and approval.

Alert severity
Informational

Category
Malware

Detection source
Antivirus

Investigation graph | Alerts (1) | Machines (1) | Key findings (1) | Entities (4.43k) | Log (98) | Pending actions 1



Dashboards
Incidents
Machines list
Alerts queue
Automated investigations
Advanced hunting
Reports
Partners & APIs
Threat & Vulnerability Management
Evaluation and tutorials
Service health
Configuration management
Settings

'EICAR_Test_File' malware was detected

Investigation #4 is running - Pending approval

Started
Sep 27, 2019, 1:50:56 PM

Total pending time: 2s

00:43:29
Pending approval

Cancel Investigation

Comments (0)

Investigation details

Status
Pending approval
Remediation actions require review and approval.

Alert severity
Informational

Category
Malware

Detection source
Antivirus

Investigation graph | Alerts (1) | Machines (1) | Key findings (1) | Entities (4.43k) | Log (98) | Pending actions 1

Quarantine file (1)

Customize columns | Export | 30 items per page

Suspicious files have been identified, requiring user approval to quarantine.

Investigation number	Machine	File Path	Remediation bundle	File Created Date	Threat Type
4	desktop-966uv3q	c:\test.txt	0 entity	9/27/19, 11:47 AM	Trojan

Dashboards
Incidents
Machines list
Alerts queue
Automated investigations
Advanced hunting
Reports
Partners & APIs
Threat & Vulnerability Management
Evaluation and tutorials
Service health
Configuration management
Settings

'EICAR_Test_File' malware was detected

Investigation #4 is running - Pending approval

Cancel Investigation

Investigation details

Status
Pending approval
Remediation actions require review and approval.

Alert severity
Informational

Category
Malware

Detection source
Antivirus

Investigation graph | Alerts (1) | Machines (1) | Key findings (1) | Entities (4.43k) | Log (98)

Quarantine file (1)

Suspicious files have been identified, requiring user approval to quar

Investigation number	Machine
4	desktop-966uv3q

File Pending Quarantine

Open investigation page | Approve | Reject

Perform the pending action as soon as the machine is available

File details

Verdict	Malicious
Machine	DESKTOP-966UV3Q
File Name	test.txt
File Path	test.txt
File Type	text/plain
File Size	68
Created Date	9/27/19, 1:47 PM
Directory	c:\
Endpoint Operating System	Windows10
Hashes	Show Hashes
Worldwide prevalence	2.02M
Prevalence in organization	1
Virus Total	61/63

Report

This file was determined to be **malicious** using reports from 2 providers.

Details

Malicious Windows Defender Static Analysis Engines

Malicious Virus Total

Properties

Compressed No

Dashboards
Incidents
Machines list
Alerts queue
Automated investigations
Advanced hunting
Reports
Partners & APIs
Threat & Vulnerability Management
Evaluation and tutorials
Service health
Configuration management
Settings

'EICAR_Test_File' malware was detected

Investigation #4 is running

Started
Sep 27, 2019, 1:50:56 PM
Total pending time: 43:40m

00:45:34
Running

Cancel Investigation

Comments (1)

Investigation details

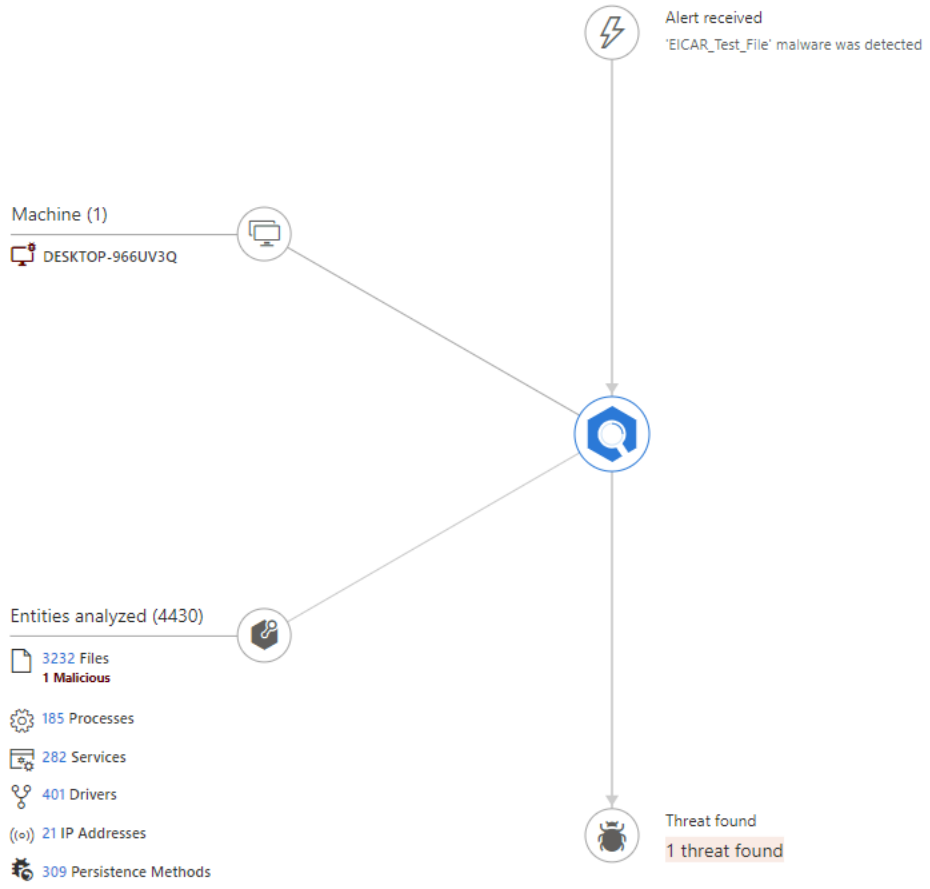
Status
Running
Investigation ongoing. Malicious entities found will be remediated.

Alert severity
Informational

Category
Malware

Detection source
Antivirus

Investigation graph | Alerts (1) | Machines (1) | Key findings (1) | Entities (4.43k) | Log (98)



Dashboards
Incidents
Machines list
Alerts queue
Automated investigations
Automated investigations
Action center
Advanced hunting
Reports
Partners & APIs
Threat & Vulnerability Management
Evaluation and tutorials
Service health
Configuration management
Settings

'EICAR_Test_File' malware was detected

Investigation #4 is complete - Remediated

Started
Sep 27, 2019, 1:50:56 PM
Ended
Sep 27, 2019, 2:37:27 PM
Total pending time: 43:40m

00:46:31
Complete

Comments (1)

Investigation details

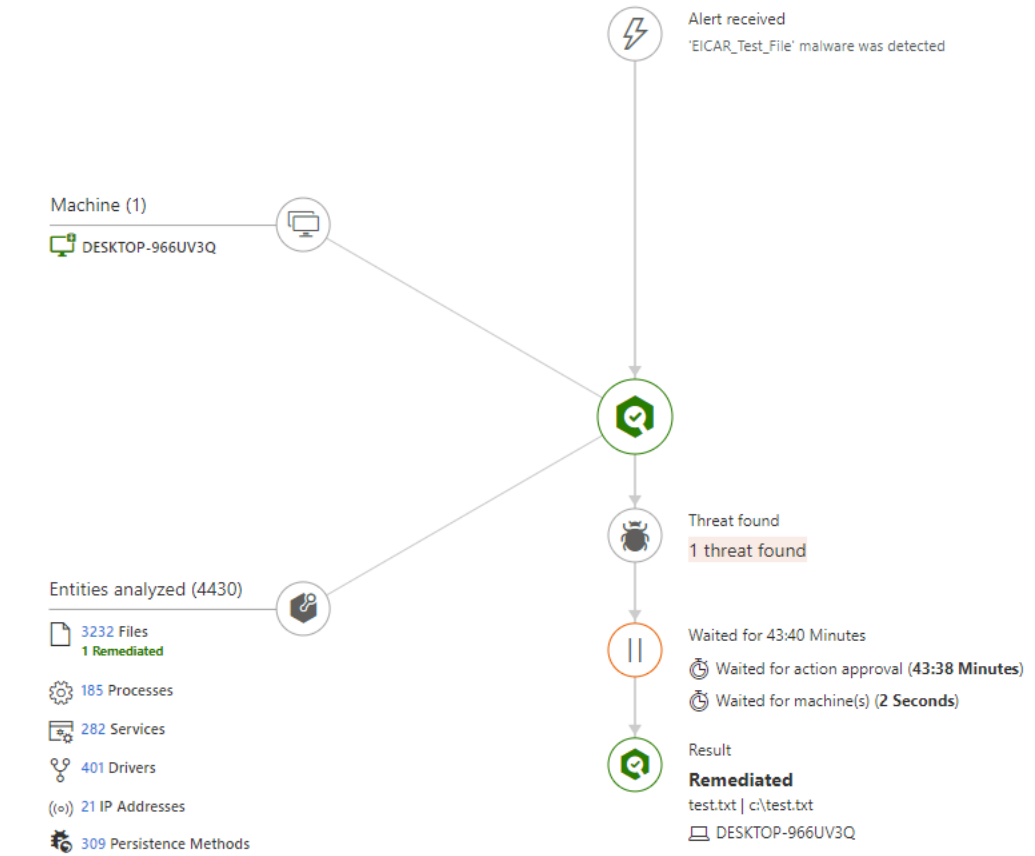
Status
Remediated
Malicious entities found were successfully remediated.

Alert severity
Informational

Category
Malware

Detection source
Antivirus

Investigation graph | Alerts (1) | Machines (1) | Key findings (1) | Entities (4.43k) | Log (98) | Pending actions history (1)



'EICAR_Test_File' malware was detected

Investigation #4 is complete - Remediated

Started
Sep 27, 2019, 1:50:56 PM
Ended
Sep 27, 2019, 2:37:27 PM
Total pending time: 43:40m

00:46:31
Complete

Comments (1)

Investigation details

Status
Remediated
Malicious entities found were successfully remediated.

Alert severity
Informational

Category
Malware

Detection source
Antivirus

Investigation graph | Alerts (1) | Machines (1) | Key findings (1) | Entities (4.43k) | Log (98) | **Pending actions history (1)**

Waited For: 43:38 Minutes

The investigation waited for user approval to perform the following action(s):

Action type	Wait time	Entity	Status	Handled by	Time
Quarantine file	43:38m	test.txt	Approved	Holger Zimmermann	Sep 27, 2019, 1:52:36 PM

Machines > desktop-966uv3q > **'EICAR_Test_File' malware was detected**

'EICAR_Test_File' malware was detected

This alert is part of incident (EICAR Test File)

Actions

Automated investigation
remediated all identified threats
(4)

Severity:	Informational
Category:	Malware
Detection source:	Antivirus
Detection technology:	Client

Alert context

desktop-966uv3q

First activity: 09.27.2019 | 13:48:42
Last activity: 09.27.2019 | 13:48:42

Description

Malware and unwanted software are undesirable applications that perform annoying, disruptive, or harmful actions on affected machines. Some of these undesirable applications can replicate and spread from one machine to another. Others are able to receive commands from remote attackers and perform activities associated with cyber attacks.

This detection might indicate that the malware was stopped from delivering its payload. However, it is prudent to check the machine for signs

Recommended actions

Collect artifacts and determine scope
• Review the machine timeline for suspicious a
related artifacts (files, IPs/URLs)
• Look for the presence of relevant artifacts or
systems.

Show more

Alert process tree

Alert process tree is not available for this alert

This alert is related to 1 detection event not displayed here.
Last event time is 09.27.2019 | 13:48:42.
Click here to see all related events in the machine timeline.

Incident graph

'EICAR_Test_File' malware was detected

Open alert page | See in timeline | Link to another incident | ...

Manage alert

Status	Resolved
Classification	True alert
Determination	Malware

Alert details

Severity	Informational
Incident	EICAR Test File
Threat found	EICAR_Test_File
Category	Malware
Detection source	Antivirus
Generated on	Sep 27, 2019, 1:50:54 PM
First activity	Sep 27, 2019, 1:48:42 PM
Last activity	Sep 27, 2019, 1:48:42 PM
Assigned to	holger@M365-USECASES.DE
Alert description	Malware and unwanted software are undesirable applications that perform annoying, disruptive, or harmful actions on affected machines. Some of these undesirable applications can replicate and spread from one machine to another. Others are able to receive commands from remote attackers and perform ac...

Go to alert page to see full description

Automated investigation details

ID	'EICAR_Test_File' malware was detected
Status	Remediated
Duration	46:31 Minutes
Started	Sep 27, 2019, 1:50:56 PM
Ended	Sep 27, 2019, 2:37:27 PM

Comments and History | Actions and assistance | Consult a threat expert

EICAR Test File

Edit name

Status
Active

Assigned to
Unassigned

Severity
Informational

Classification
(Not set)
Set status and classification

Category
Malware

Alerts (1) | Machines (1) | Investigations (1) | Evidence (1) | Graph beta

Title	Severity	Status	Classification	Linked by	Category
'EICAR_Test_File' malware was detected	Informational	Resolved	True alert	Proximate time	Malware

Set classification

Incident status
Resolved

Classification
True alert

Determination
Security testing

Comment
Example - Remediation actions require approval

When resolving an incident, you also resolve all the linked active alerts.