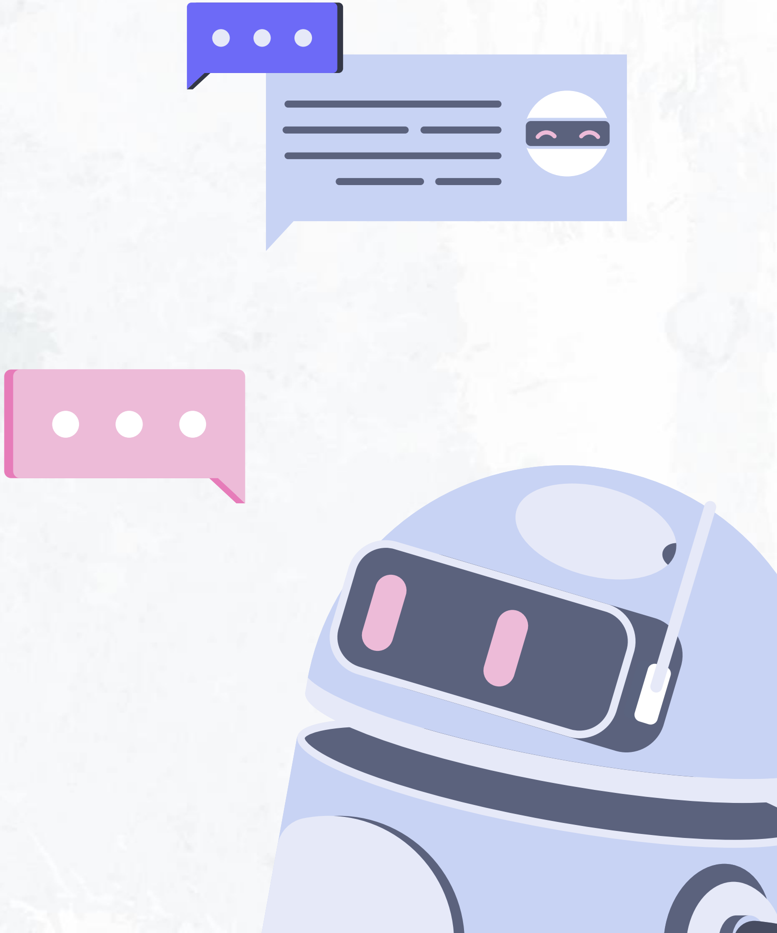
OpenEDR Registry Spy



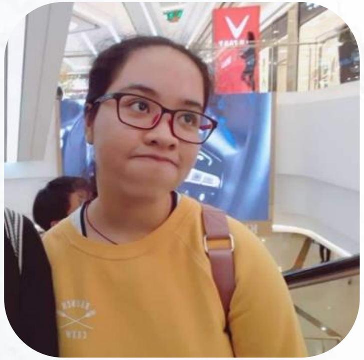
OUR TEAM

Nguyễn Bình Thục Trâm

20520815

Võ Anh Kiệt

20520605



Nguyễn Bùi Kim Ngân

20520648

Table of contents

01 → EDR - OpenEDR

02 → Registry Spy

01 →

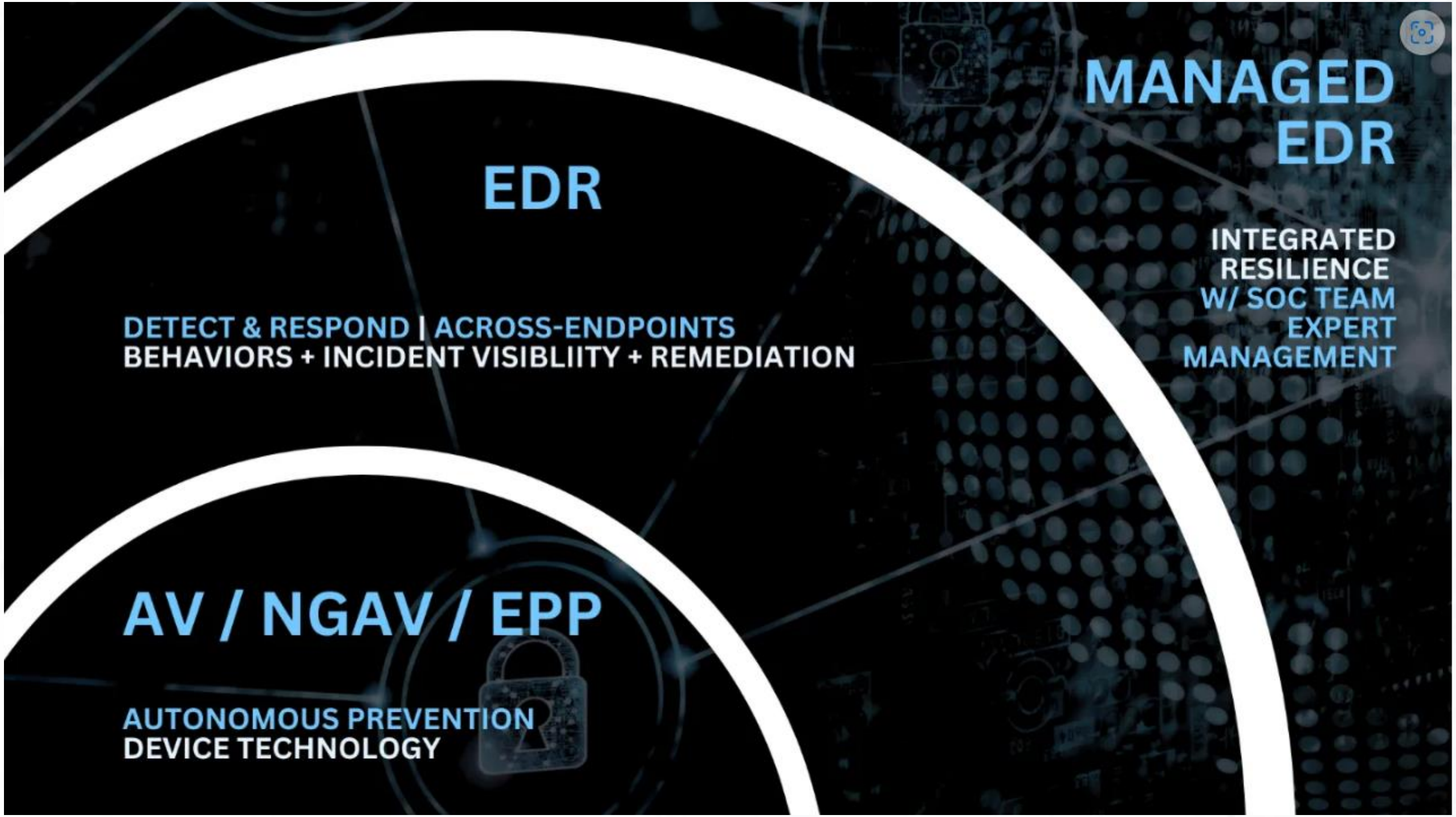
EDR – Endpoint Detect Respone OpenEDR

OpenEDR

Open EDR is a sophisticated, free, open-source endpoint detection and response solution. It provides analytic detection with Mitre ATT&CK visibility for event correlation and root cause analysis of adversarial threat activity and behaviors in real time.

This world-class endpoint telemetry platform is available to all cyber-security professionals, and every sized organization, to defend against threat actors and cyber criminals.

OpenEDR



MANAGED EDR

INTEGRATED RESILIENCE W/ SOC TEAM EXPERT MANAGEMENT

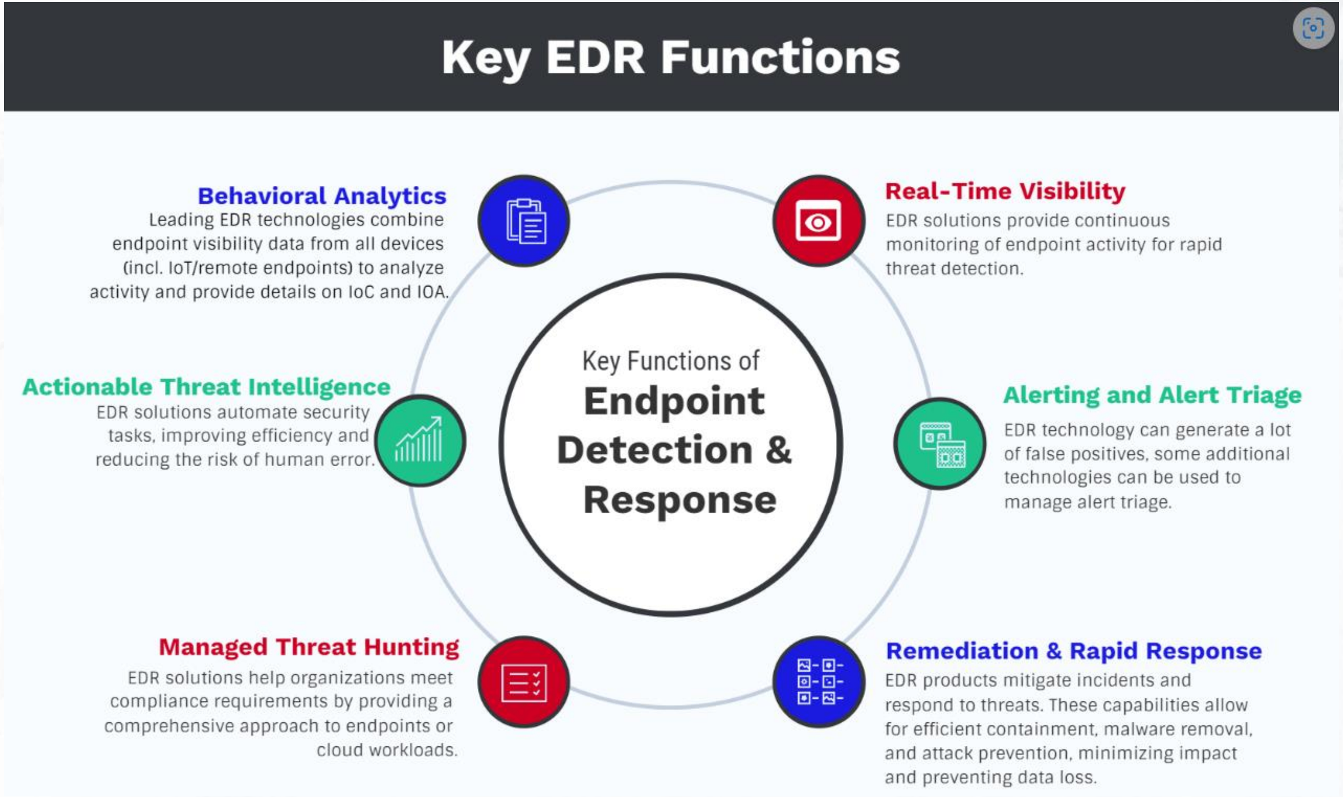
EDR

DETECT & RESPOND | ACROSS-ENDPOINTS
BEHAVIORS + INCIDENT VISIBLIITY + REMEDIATION

AV / NGAV / EPP

AUTONOMOUS PREVENTION
DEVICE TECHNOLOGY

OpenEDR



Key EDR Functions

Key Functions of **Endpoint Detection & Response**

Behavioral Analytics
Leading EDR technologies combine endpoint visibility data from all devices (incl. IoT/remote endpoints) to analyze activity and provide details on IoC and IOA.

Real-Time Visibility
EDR solutions provide continuous monitoring of endpoint activity for rapid threat detection.

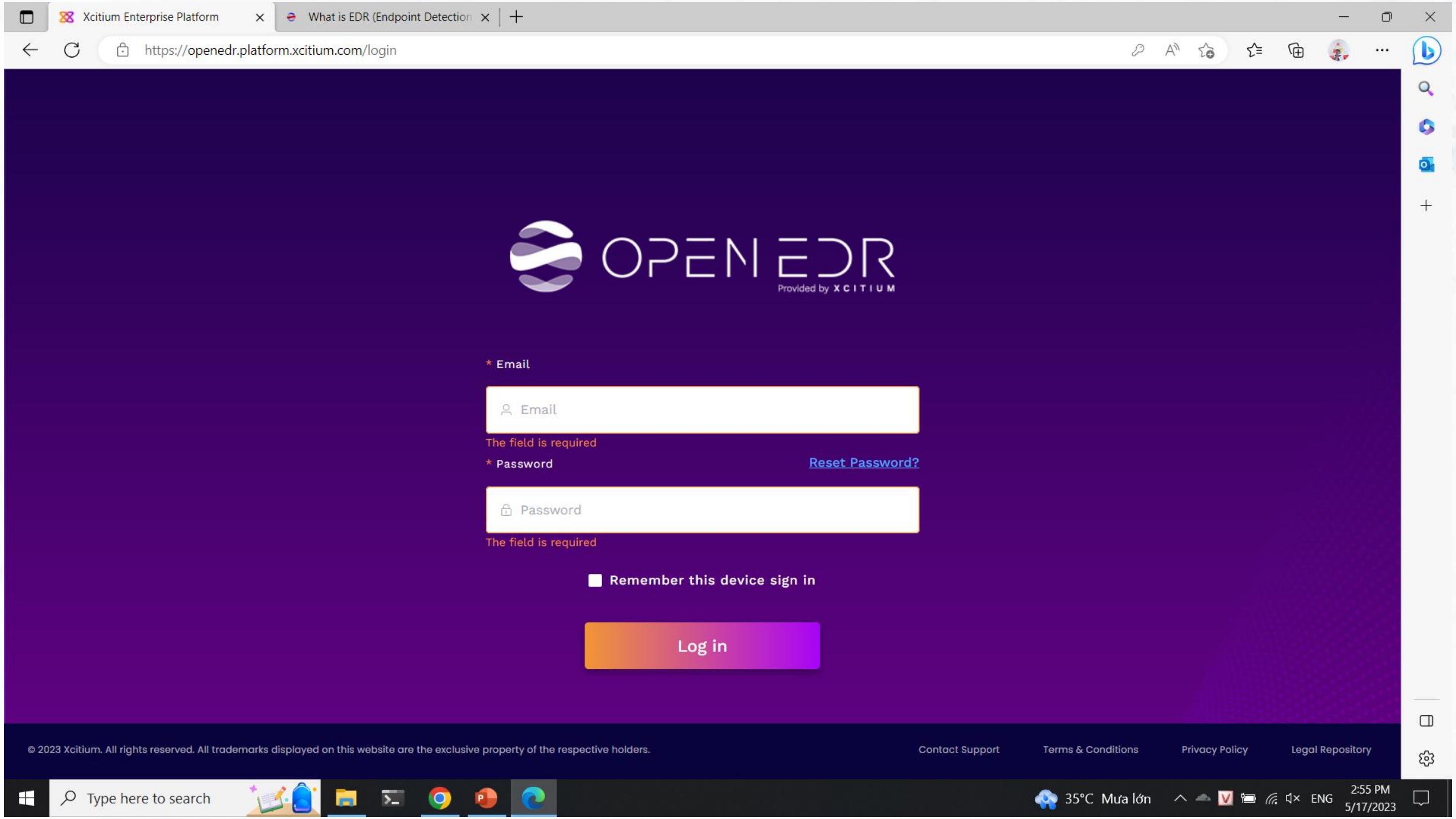
Actionable Threat Intelligence
EDR solutions automate security tasks, improving efficiency and reducing the risk of human error.

Alerting and Alert Triage
EDR technology can generate a lot of false positives, some additional technologies can be used to manage alert triage.

Managed Threat Hunting
EDR solutions help organizations meet compliance requirements by providing a comprehensive approach to endpoints or cloud workloads.

Remediation & Rapid Response
EDR products mitigate incidents and respond to threats. These capabilities allow for efficient containment, malware removal, and attack prevention, minimizing impact and preventing data loss.

Installation



https://openedr.platform.xcitium.com/login

* Email

Email

The field is required

* Password

Reset Password?

Password

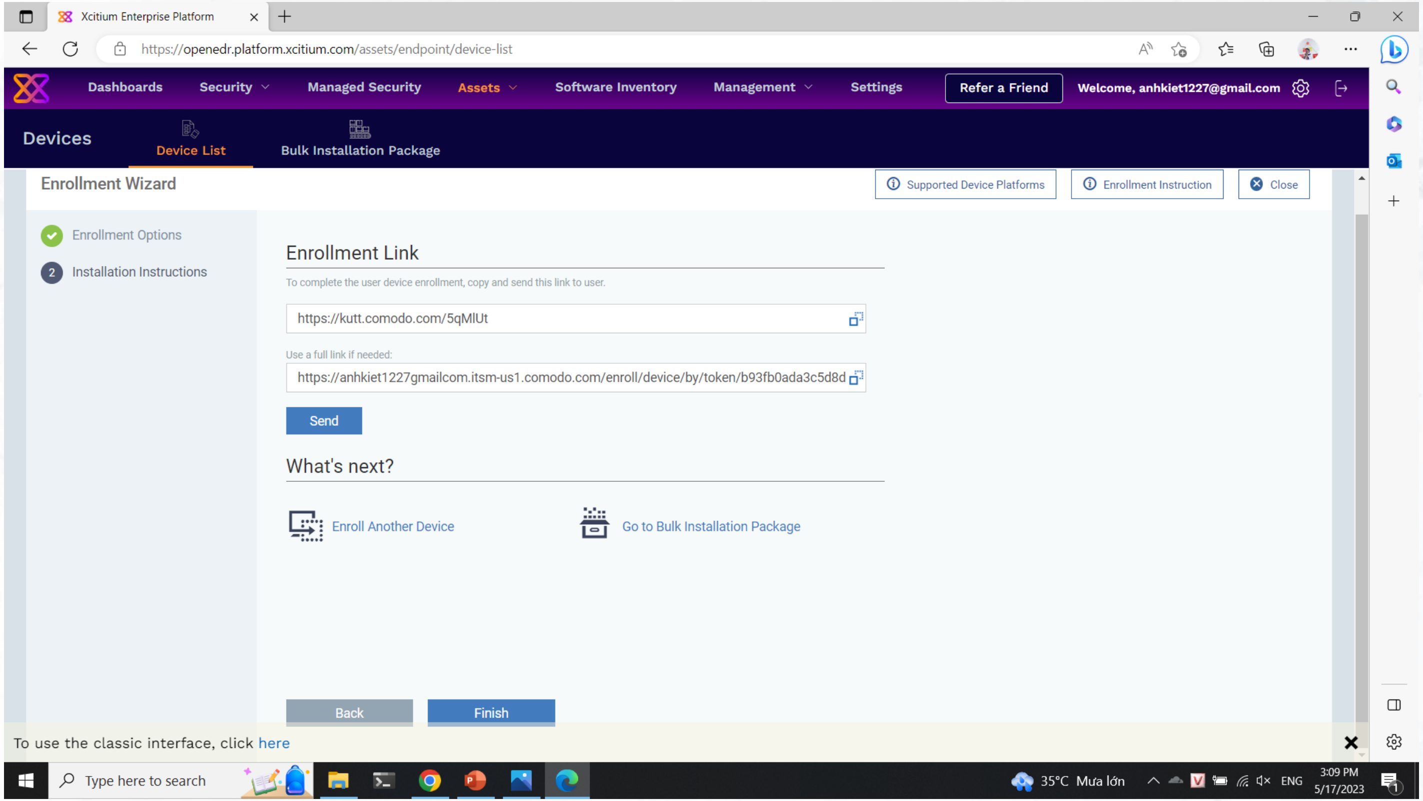
The field is required

□ Remember this device sign in

Log in

© 2023 Xcitium. All rights reserved. All trademarks displayed on this website are the exclusive property of the respective holders.

Installation Agent



Enrollment Wizard

- Enrollment Options
- 2 Installation Instructions

Enrollment Link

To complete the user device enrollment, copy and send this link to user.

https://kutt.comodo.com/5qMlUt

Use a full link if needed:

https://anhkiet1227gmailcom.itsm-us1.comodo.com/enroll/device/by/token/b93fb0ada3c5d8d

Send

What's next?

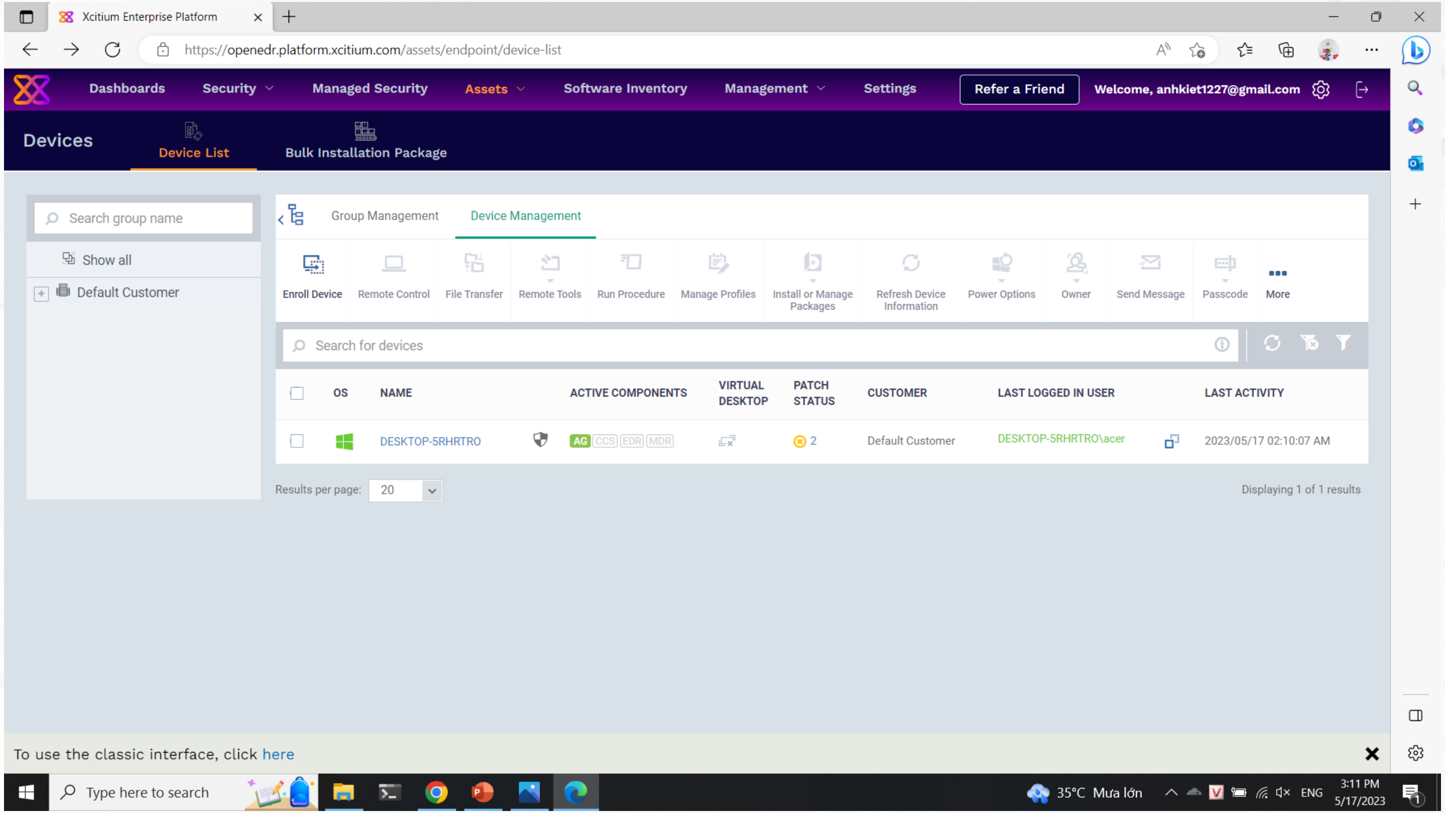
Enroll Another Device

Go to Bulk Installation Package

Back Finish

To use the classic interface, click here

Installation Agent



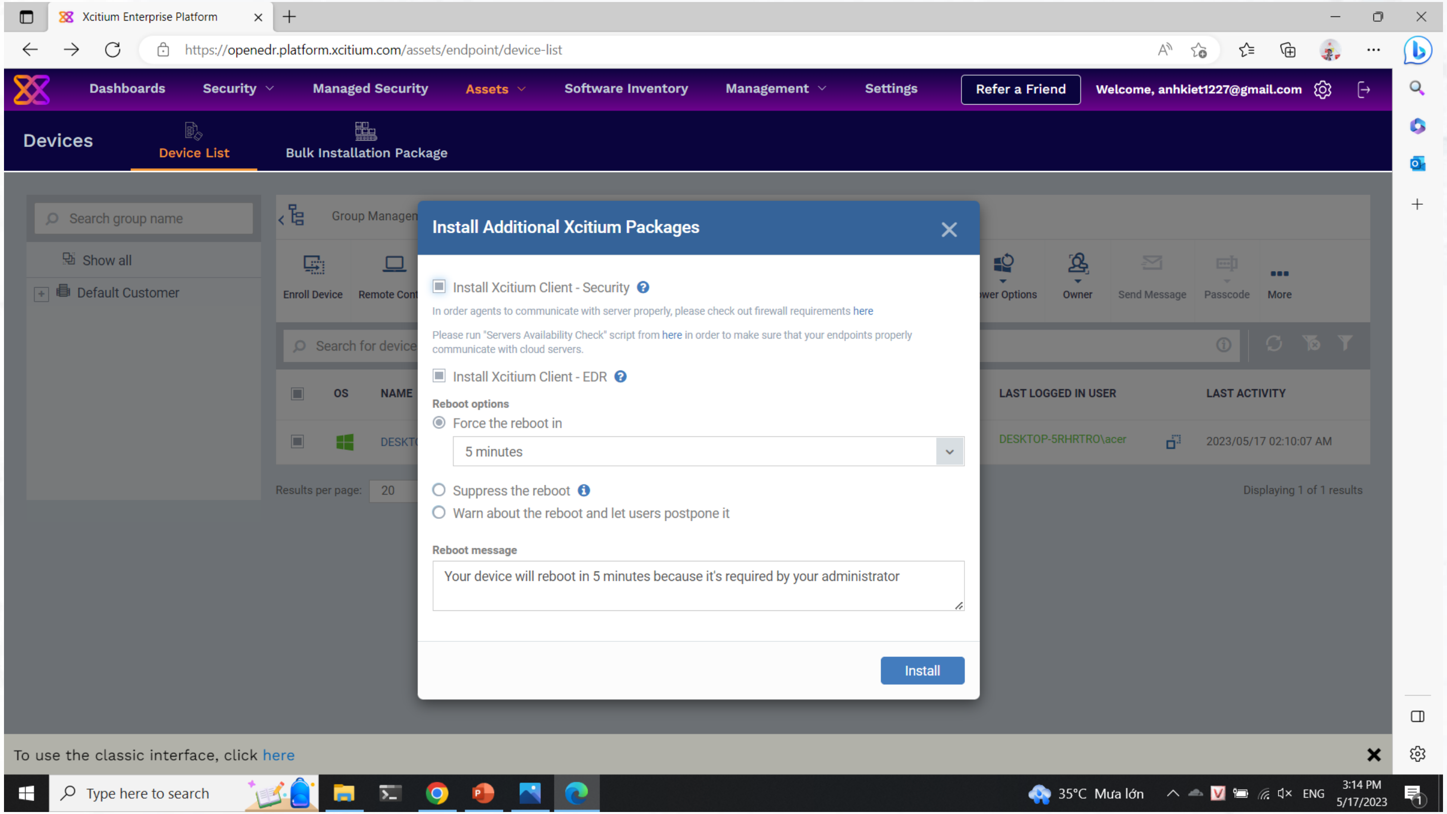
□	OS	NAME	ACTIVE COMPONENTS	VIRTUAL DESKTOP	PATCH STATUS	CUSTOMER	LAST LOGGED IN USER	LAST ACTIVITY
□		DESKTOP-5RHRTRO	AG CCS EDR MDR		2	Default Customer	DESKTOP-5RHRTRO\acer	2023/05/17 02:10:07 AM

Results per page: 20

Displaying 1 of 1 results

To use the classic interface, click here

Installation Packages



Install Additional Xcitium Packages

☐ Install Xcitium Client - Security

In order agents to communicate with server properly, please check out firewall requirements here

Please run "Servers Availability Check" script from here in order to make sure that your endpoints properly communicate with cloud servers.

☐ Install Xcitium Client - EDR

Reboot options

● Force the reboot in

5 minutes

○ Suppress the reboot

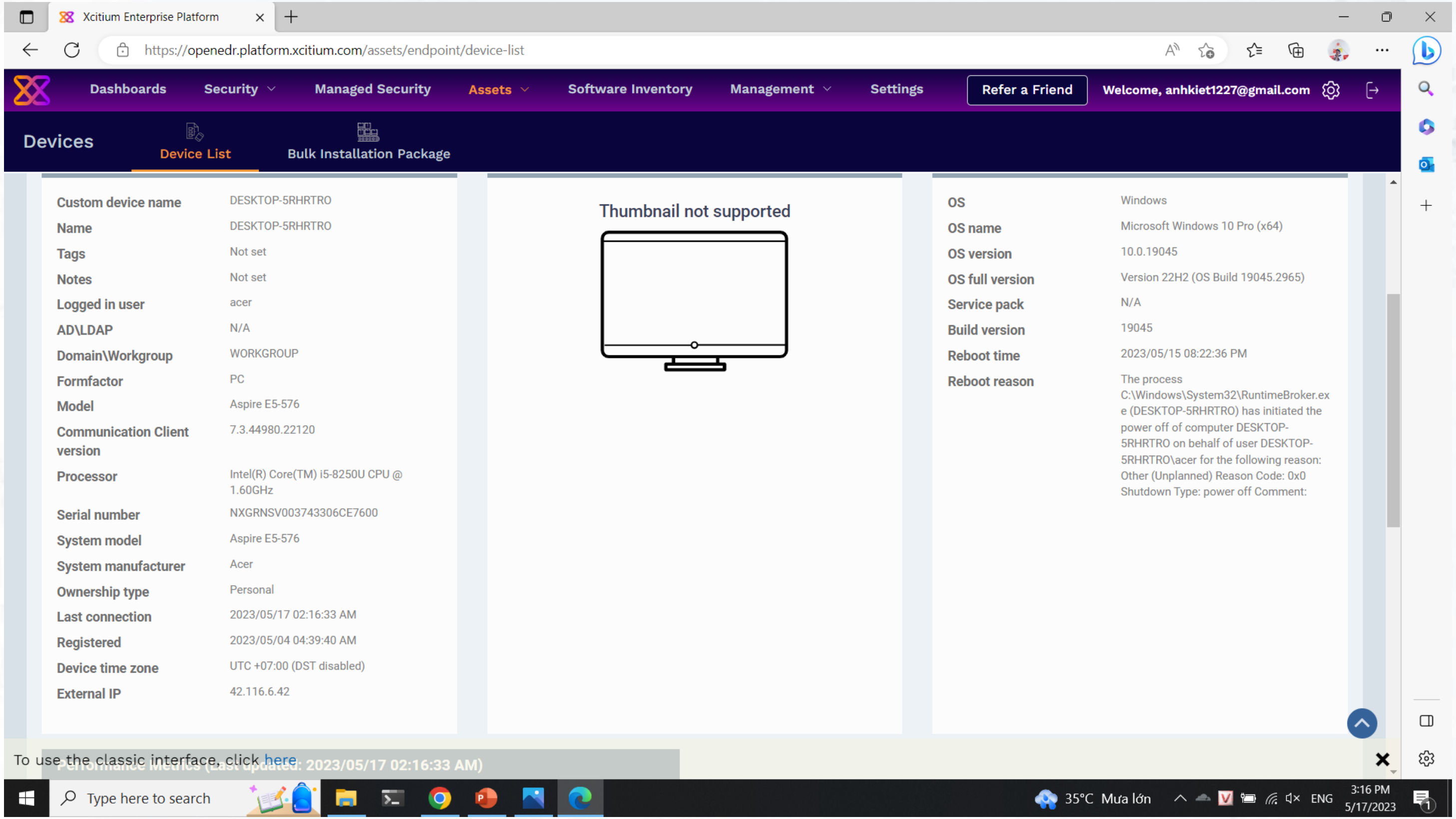
○ Warn about the reboot and let users postpone it

Reboot message

Your device will reboot in 5 minutes because it's required by your administrator

Install

Tool scanning



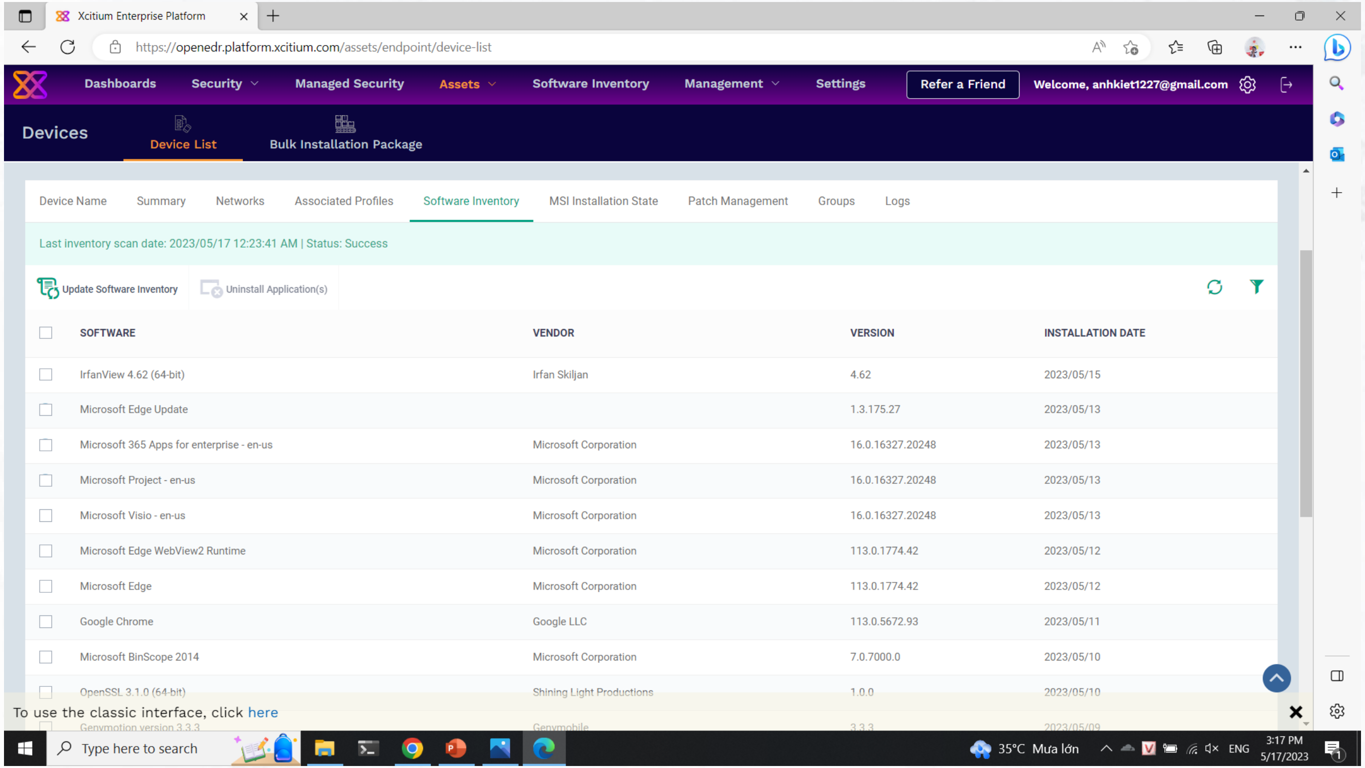
Custom device name	DESKTOP-5RHRTRO
Name	DESKTOP-5RHRTRO
Tags	Not set
Notes	Not set
Logged in user	acer
AD\LDAP	N/A
Domain\Workgroup	WORKGROUP
Formfactor	PC
Model	Aspire E5-576
Communication Client version	7.3.44980.22120
Processor	Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz
Serial number	NXGRNSV003743306CE7600
System model	Aspire E5-576
System manufacturer	Acer
Ownership type	Personal
Last connection	2023/05/17 02:16:33 AM
Registered	2023/05/04 04:39:40 AM
Device time zone	UTC +07:00 (DST disabled)
External IP	42.116.6.42

OS	Windows
OS name	Microsoft Windows 10 Pro (x64)
OS version	10.0.19045
OS full version	Version 22H2 (OS Build 19045.2965)
Service pack	N/A
Build version	19045
Reboot time	2023/05/15 08:22:36 PM
Reboot reason	The process C:\Windows\System32\RuntimeBroker.exe (DESKTOP-5RHRTRO) has initiated the power off of computer DESKTOP-5RHRTRO on behalf of user DESKTOP-5RHRTRO\acer for the following reason: Other (Unplanned) Reason Code: 0x0 Shutdown Type: power off Comment:

To use the classic interface, click here.

Performance Metrics (Last updated: 2023/05/17 02:16:33 AM)

Tool scanning

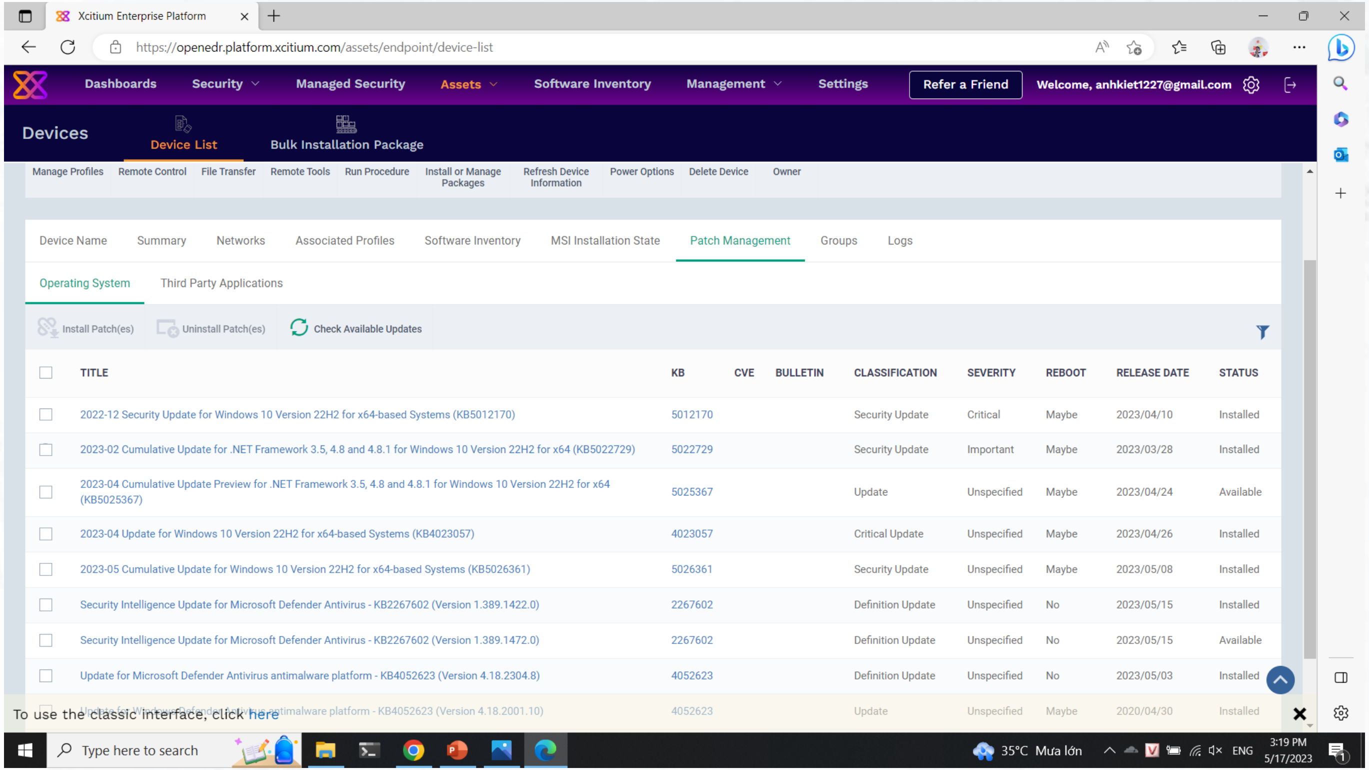


Last inventory scan date: 2023/05/17 12:23:41 AM | Status: Success

□	SOFTWARE	VENDOR	VERSION	INSTALLATION DATE
□	IrfanView 4.62 (64-bit)	Irfan Skiljan	4.62	2023/05/15
□	Microsoft Edge Update		1.3.175.27	2023/05/13
□	Microsoft 365 Apps for enterprise - en-us	Microsoft Corporation	16.0.16327.20248	2023/05/13
□	Microsoft Project - en-us	Microsoft Corporation	16.0.16327.20248	2023/05/13
□	Microsoft Visio - en-us	Microsoft Corporation	16.0.16327.20248	2023/05/13
□	Microsoft Edge WebView2 Runtime	Microsoft Corporation	113.0.1774.42	2023/05/12
□	Microsoft Edge	Microsoft Corporation	113.0.1774.42	2023/05/12
□	Google Chrome	Google LLC	113.0.5672.93	2023/05/11
□	Microsoft BinScope 2014	Microsoft Corporation	7.0.7000.0	2023/05/10
□	OpenSSL 3.1.0 (64-bit)	Shining Light Productions	1.0.0	2023/05/10
□	Genymotion version 3.3.3	Genymobile	3.3.3	2023/05/09

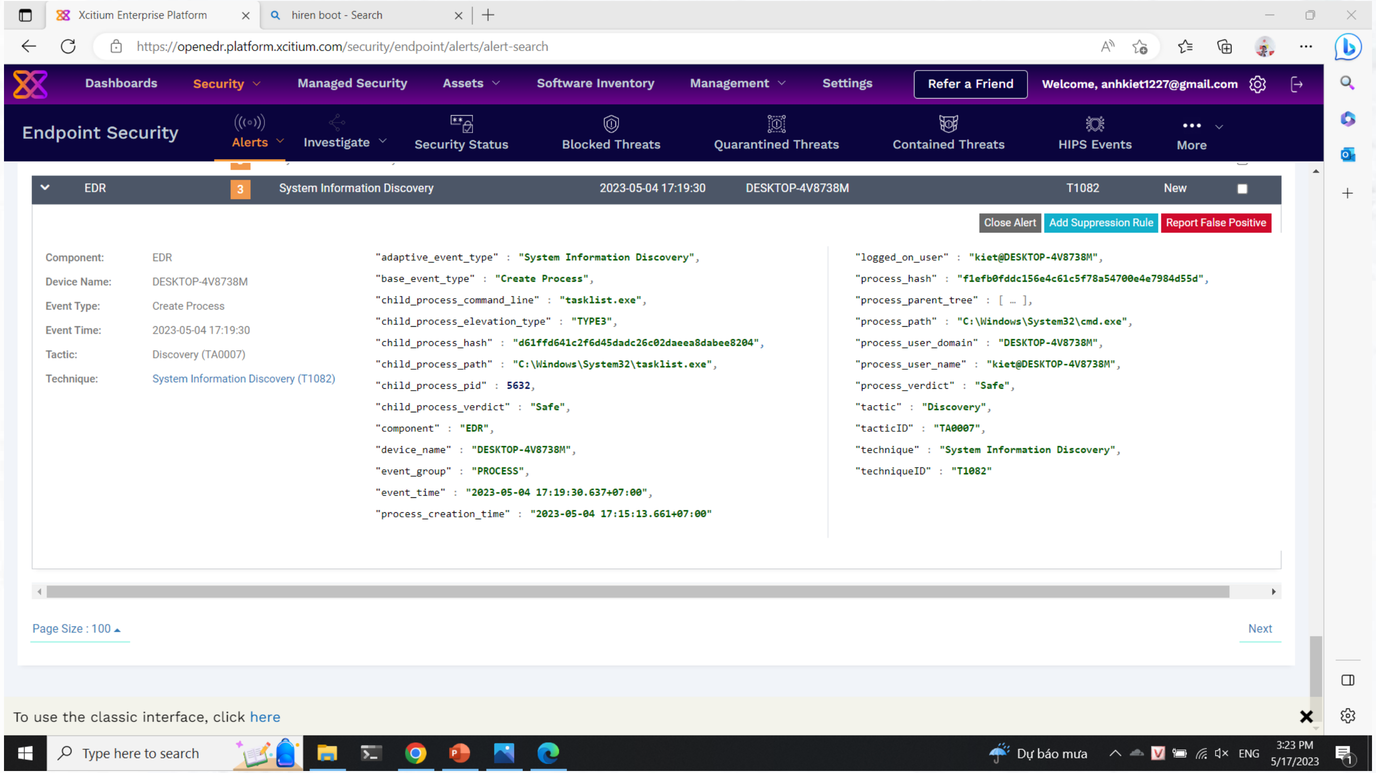
To use the classic interface, click here

Tool scanning



☐	TITLE	KB	CVE	BULLETIN	CLASSIFICATION	SEVERITY	REBOOT	RELEASE DATE	STATUS
☐	2022-12 Security Update for Windows 10 Version 22H2 for x64-based Systems (KB5012170)	5012170			Security Update	Critical	Maybe	2023/04/10	Installed
☐	2023-02 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 22H2 for x64 (KB5022729)	5022729			Security Update	Important	Maybe	2023/03/28	Installed
☐	2023-04 Cumulative Update Preview for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 22H2 for x64 (KB5025367)	5025367			Update	Unspecified	Maybe	2023/04/24	Available
☐	2023-04 Update for Windows 10 Version 22H2 for x64-based Systems (KB4023057)	4023057			Critical Update	Unspecified	Maybe	2023/04/26	Installed
☐	2023-05 Cumulative Update for Windows 10 Version 22H2 for x64-based Systems (KB5026361)	5026361			Security Update	Unspecified	Maybe	2023/05/08	Installed
☐	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.389.1422.0)	2267602			Definition Update	Unspecified	No	2023/05/15	Installed
☐	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.389.1472.0)	2267602			Definition Update	Unspecified	No	2023/05/15	Available
☐	Update for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.2304.8)	4052623			Definition Update	Unspecified	No	2023/05/03	Installed
☐	Update for Windows Defender Antivirus antimalware platform - KB4052623 (Version 4.18.2001.10)	4052623			Update	Unspecified	Maybe	2020/04/30	Installed

Tool scanning



EDR	3	System Information Discovery	2023-05-04 17:19:30	DESKTOP-4V8738M	T1082	New	□

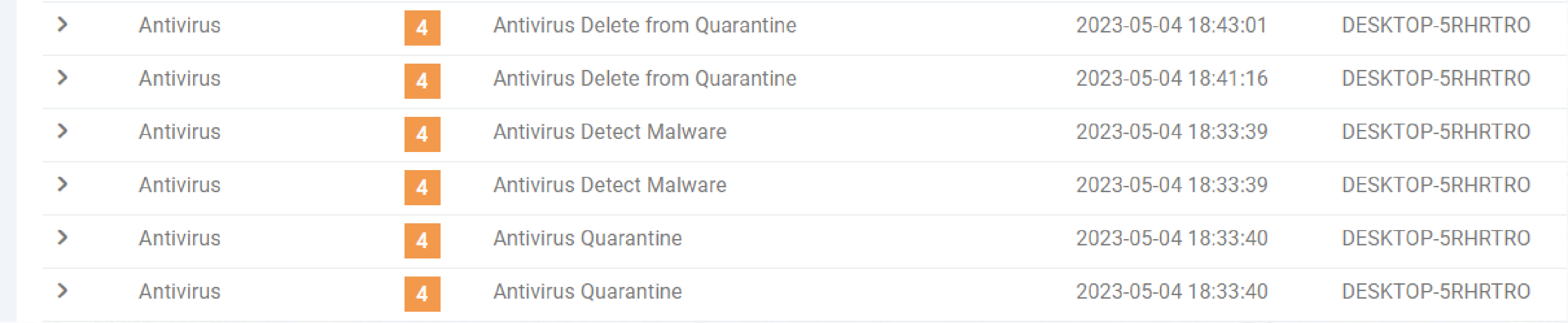
Component:	EDR
Device Name:	DESKTOP-4V8738M
Event Type:	Create Process
Event Time:	2023-05-04 17:19:30
Tactic:	Discovery (TA0007)
Technique:	System Information Discovery (T1082)

```
"adaptive_event_type" : "System Information Discovery",
"base_event_type" : "Create Process",
"child_process_command_line" : "tasklist.exe",
"child_process_elevation_type" : "TYPE3",
"child_process_hash" : "d61ffd641c2f6d45dadc26c02daeea8dabee8204",
"child_process_path" : "C:\Windows\System32\tasklist.exe",
"child_process_pid" : 5632,
"child_process_verdict" : "Safe",
"component" : "EDR",
"device_name" : "DESKTOP-4V8738M",
"event_group" : "PROCESS",
"event_time" : "2023-05-04 17:19:30.637+07:00",
"process_creation_time" : "2023-05-04 17:15:13.661+07:00"
```

```
"logged_on_user" : "kiet@DESKTOP-4V8738M",
"process_hash" : "f1efb0fddc156e4c61c5f78a54700e4e7984d55d",
"process_parent_tree" : [ … ],
"process_path" : "C:\Windows\System32\cmd.exe",
"process_user_domain" : "DESKTOP-4V8738M",
"process_user_name" : "kiet@DESKTOP-4V8738M",
"process_verdict" : "Safe",
"tactic" : "Discovery",
"tacticID" : "TA0007",
"technique" : "System Information Discovery",
"techniqueID" : "T1082"
```

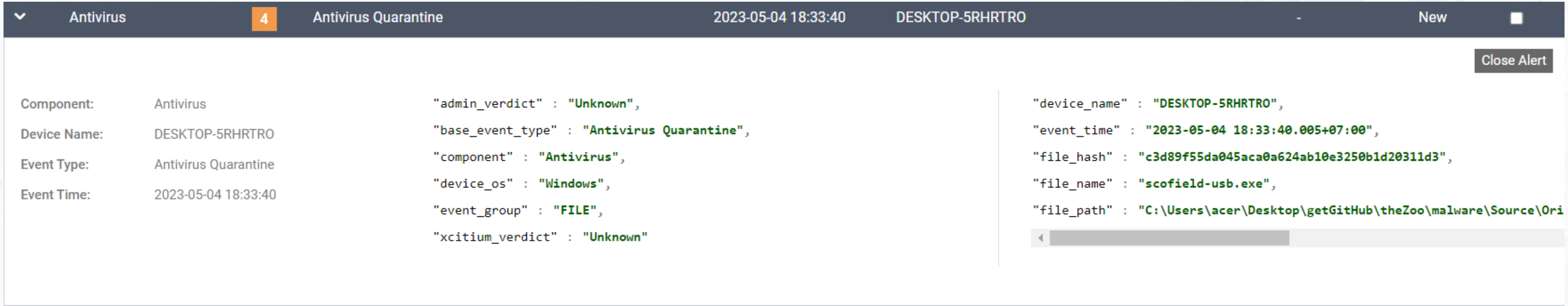
To use the classic interface, click here

Malware



›	Antivirus	4	Antivirus Delete from Quarantine	2023-05-04 18:43:01	DESKTOP-5RHRTRO
›	Antivirus	4	Antivirus Delete from Quarantine	2023-05-04 18:41:16	DESKTOP-5RHRTRO
›	Antivirus	4	Antivirus Detect Malware	2023-05-04 18:33:39	DESKTOP-5RHRTRO
›	Antivirus	4	Antivirus Detect Malware	2023-05-04 18:33:39	DESKTOP-5RHRTRO
›	Antivirus	4	Antivirus Quarantine	2023-05-04 18:33:40	DESKTOP-5RHRTRO
›	Antivirus	4	Antivirus Quarantine	2023-05-04 18:33:40	DESKTOP-5RHRTRO

Malware



Antivirus 4 Antivirus Quarantine 2023-05-04 18:33:40 DESKTOP-5RHRTRO - New □

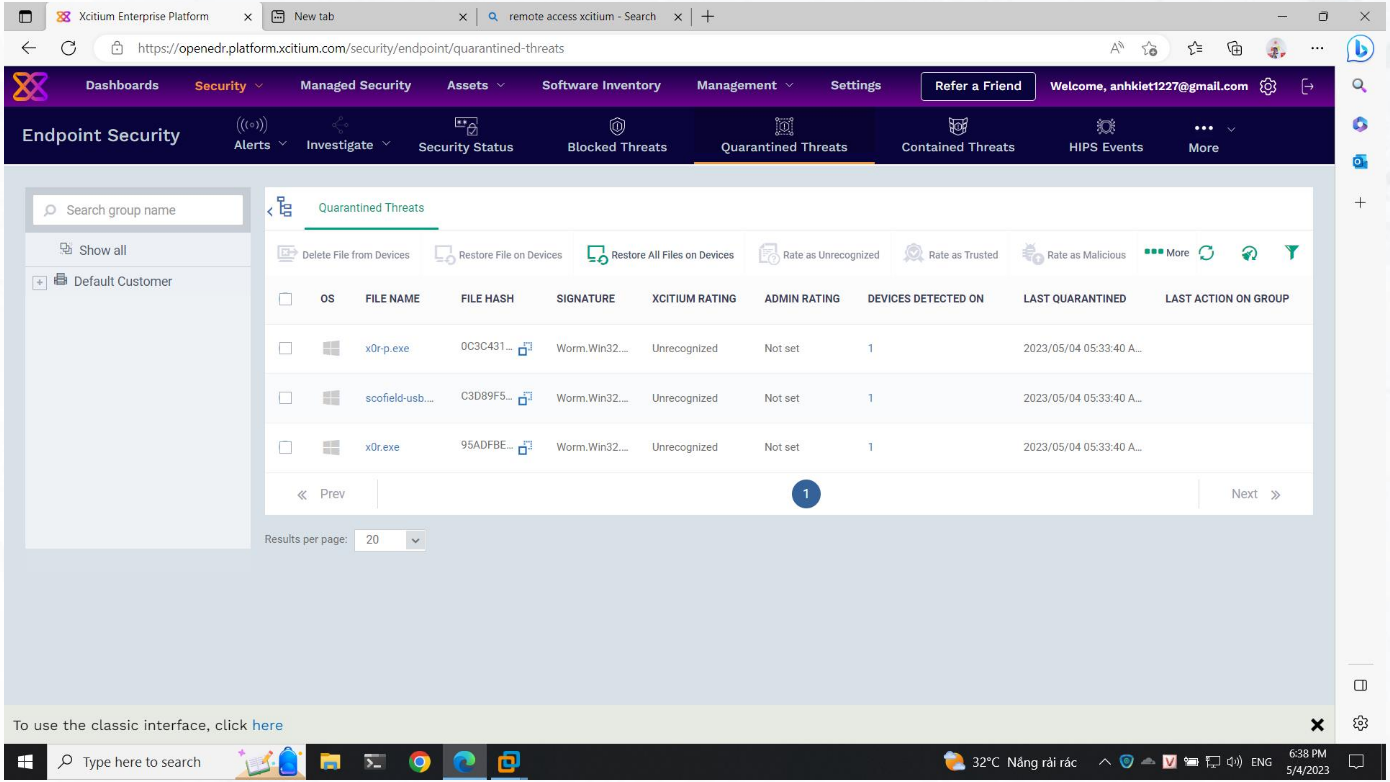
Close Alert

Component:	Antivirus
Device Name:	DESKTOP-5RHRTRO
Event Type:	Antivirus Quarantine
Event Time:	2023-05-04 18:33:40

```
"admin_verdict" : "Unknown",
"base_event_type" : "Antivirus Quarantine",
"component" : "Antivirus",
"device_os" : "Windows",
"event_group" : "FILE",
"xcitium_verdict" : "Unknown"
```

```
"device_name" : "DESKTOP-5RHRTRO",
"event_time" : "2023-05-04 18:33:40.005+07:00",
"file_hash" : "c3d89f55da045aca0a624ab10e3250b1d20311d3",
"file_name" : "scofield-usb.exe",
"file_path" : "C:\Users\acer\Desktop\getGitHub\theZoo\malware\Source\Ori
```

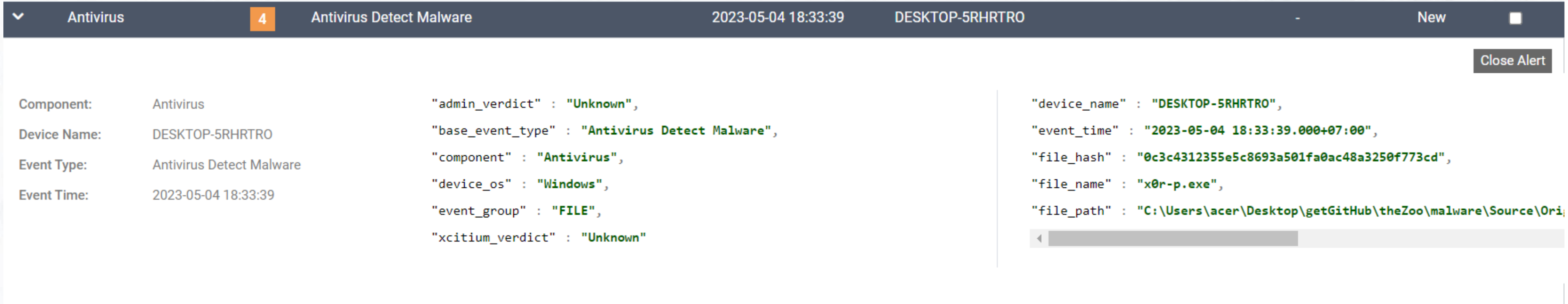
Malware



□	OS	FILE NAME	FILE HASH	SIGNATURE	XCITIUM RATING	ADMIN RATING	DEVICES DETECTED ON	LAST QUARANTINED	LAST ACTION ON GROUP
□		x0r-p.exe	0C3C431...	Worm.Win32....	Unrecognized	Not set	1	2023/05/04 05:33:40 A...	
□		scofield-usb....	C3D89F5...	Worm.Win32....	Unrecognized	Not set	1	2023/05/04 05:33:40 A...	
□		x0r.exe	95ADFBE...	Worm.Win32....	Unrecognized	Not set	1	2023/05/04 05:33:40 A...	

To use the classic interface, click here

Malware



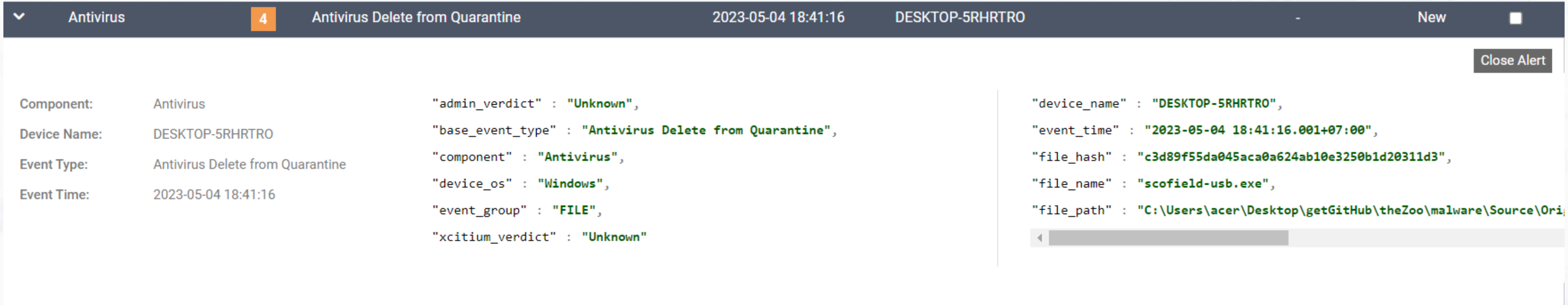
⌄	Antivirus	4	Antivirus Detect Malware	2023-05-04 18:33:39	DESKTOP-5RHRTRO	-	New □

Component:	Antivirus
Device Name:	DESKTOP-5RHRTRO
Event Type:	Antivirus Detect Malware
Event Time:	2023-05-04 18:33:39

```
"admin_verdict" : "Unknown",
"base_event_type" : "Antivirus Detect Malware",
"component" : "Antivirus",
"device_os" : "Windows",
"event_group" : "FILE",
"xcitium_verdict" : "Unknown"
```

```
"device_name" : "DESKTOP-5RHRTRO",
"event_time" : "2023-05-04 18:33:39.000+07:00",
"file_hash" : "0c3c4312355e5c8693a501fa0ac48a3250f773cd",
"file_name" : "x0r-p.exe",
"file_path" : "C:\Users\acer\Desktop\getGitHub\theZoo\malware\Source\Ori
```

Malware

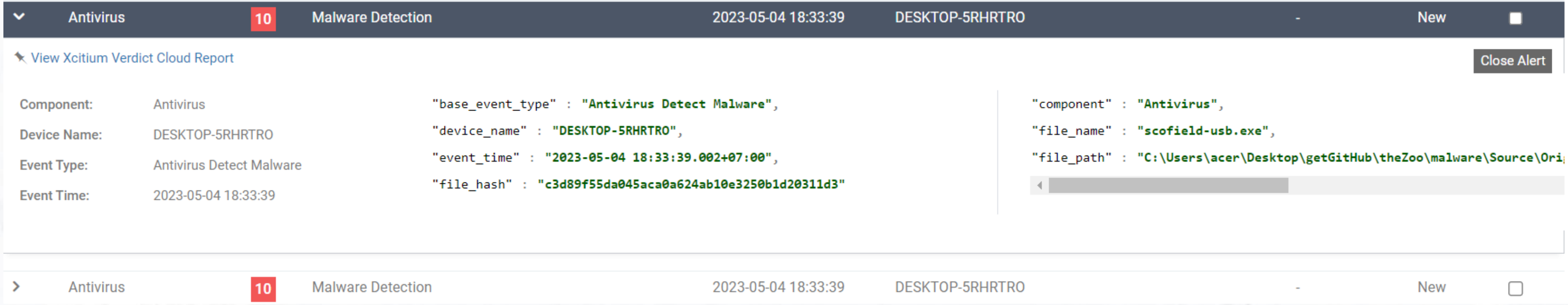


Component:	Antivirus
Device Name:	DESKTOP-5RHRTRO
Event Type:	Antivirus Delete from Quarantine
Event Time:	2023-05-04 18:41:16

```
"admin_verdict" : "Unknown",
"base_event_type" : "Antivirus Delete from Quarantine",
"component" : "Antivirus",
"device_os" : "Windows",
"event_group" : "FILE",
"xcitium_verdict" : "Unknown"
```

```
"device_name" : "DESKTOP-5RHRTRO",
"event_time" : "2023-05-04 18:41:16.001+07:00",
"file_hash" : "c3d89f55da045aca0a624ab10e3250b1d20311d3",
"file_name" : "scofield-usb.exe",
"file_path" : "C:\Users\acer\Desktop\getGitHub\theZoo\malware\Source\Ori
```

Malware



⌄	Antivirus	10	Malware Detection	2023-05-04 18:33:39	DESKTOP-5RHRTRO	-	New	☐

View Xcitium Verdict Cloud Report

Close Alert

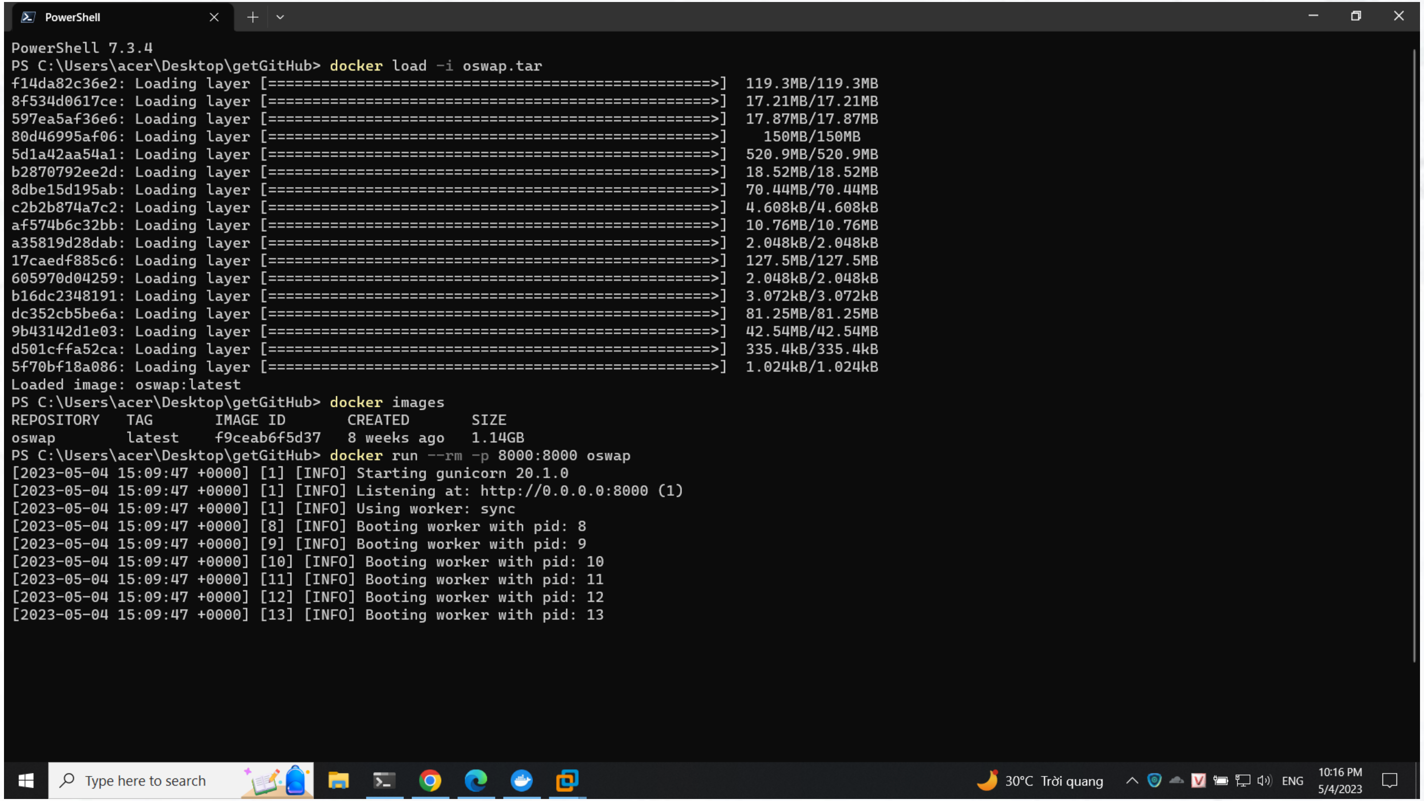
Component:	Antivirus
Device Name:	DESKTOP-5RHRTRO
Event Type:	Antivirus Detect Malware
Event Time:	2023-05-04 18:33:39

```
"base_event_type" : "Antivirus Detect Malware",
"device_name" : "DESKTOP-5RHRTRO",
"event_time" : "2023-05-04 18:33:39.002+07:00",
"file_hash" : "c3d89f55da045aca0a624ab10e3250b1d20311d3"
```

```
"component" : "Antivirus",
"file_name" : "scofield-usb.exe",
"file_path" : "C:\Users\acer\Desktop\getGitHub\theZoo\malware\Source\Ori
```

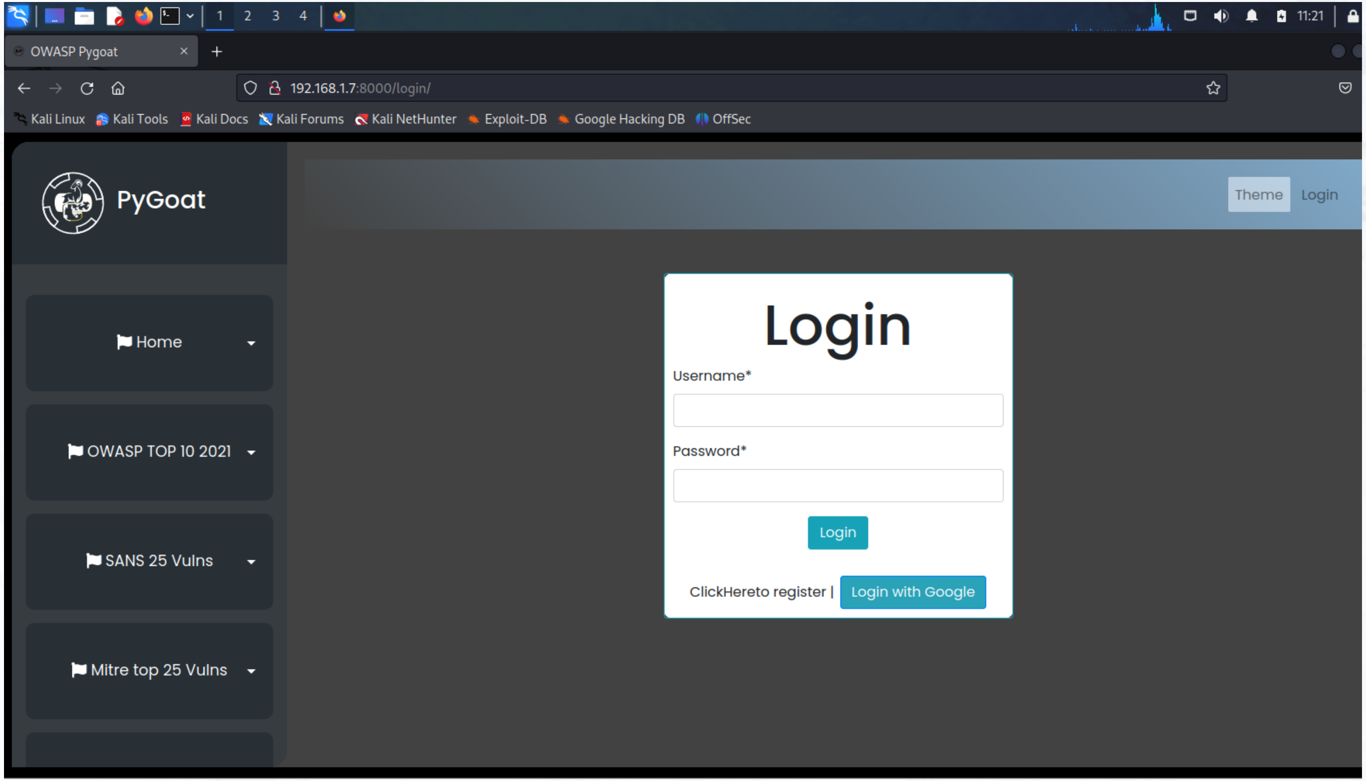
›	Antivirus	10	Malware Detection	2023-05-04 18:33:39	DESKTOP-5RHRTRO	-	New	☐

PyGoat – Top 10 OWASP



```
PowerShell 7.3.4
PS C:\Users\acer\Desktop\getGitHub> docker load -i oswap.tar
f14da82c36e2: Loading layer [=================================================>]  119.3MB/119.3MB
8f534d0617ce: Loading layer [=================================================>]  17.21MB/17.21MB
597ea5af36e6: Loading layer [=================================================>]  17.87MB/17.87MB
80d46995af06: Loading layer [=================================================>]    150MB/150MB
5d1a42aa54a1: Loading layer [=================================================>]  520.9MB/520.9MB
b2870792ee2d: Loading layer [=================================================>]  18.52MB/18.52MB
8dbe15d195ab: Loading layer [=================================================>]  70.44MB/70.44MB
c2b2b874a7c2: Loading layer [=================================================>]  4.608kB/4.608kB
af574b6c32bb: Loading layer [=================================================>]  10.76MB/10.76MB
a35819d28dab: Loading layer [=================================================>]  2.048kB/2.048kB
17caedf885c6: Loading layer [=================================================>]  127.5MB/127.5MB
605970d04259: Loading layer [=================================================>]  2.048kB/2.048kB
b16dc2348191: Loading layer [=================================================>]  3.072kB/3.072kB
dc352cb5be6a: Loading layer [=================================================>]  81.25MB/81.25MB
9b43142d1e03: Loading layer [=================================================>]  42.54MB/42.54MB
d501cffa52ca: Loading layer [=================================================>]  335.4kB/335.4kB
5f70bf18a086: Loading layer [=================================================>]  1.024kB/1.024kB
Loaded image: oswap:latest
PS C:\Users\acer\Desktop\getGitHub> docker images
REPOSITORY   TAG       IMAGE ID       CREATED       SIZE
oswap        latest    f9ceab6f5d37   8 weeks ago   1.14GB
PS C:\Users\acer\Desktop\getGitHub> docker run --rm -p 8000:8000 oswap
[2023-05-04 15:09:47 +0000] [1] [INFO] Starting gunicorn 20.1.0
[2023-05-04 15:09:47 +0000] [1] [INFO] Listening at: http://0.0.0.0:8000 (1)
[2023-05-04 15:09:47 +0000] [1] [INFO] Using worker: sync
[2023-05-04 15:09:47 +0000] [8] [INFO] Booting worker with pid: 8
[2023-05-04 15:09:47 +0000] [9] [INFO] Booting worker with pid: 9
[2023-05-04 15:09:47 +0000] [10] [INFO] Booting worker with pid: 10
[2023-05-04 15:09:47 +0000] [11] [INFO] Booting worker with pid: 11
[2023-05-04 15:09:47 +0000] [12] [INFO] Booting worker with pid: 12
[2023-05-04 15:09:47 +0000] [13] [INFO] Booting worker with pid: 13
```

PyGoat – Top 10 OWASP



Login

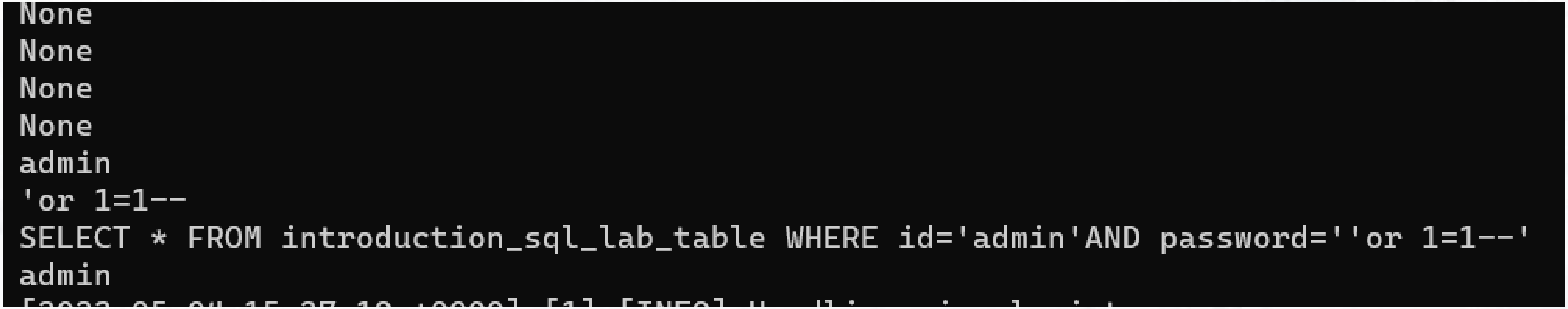
Username*

Password*

Login

ClickHereto register | Login with Google

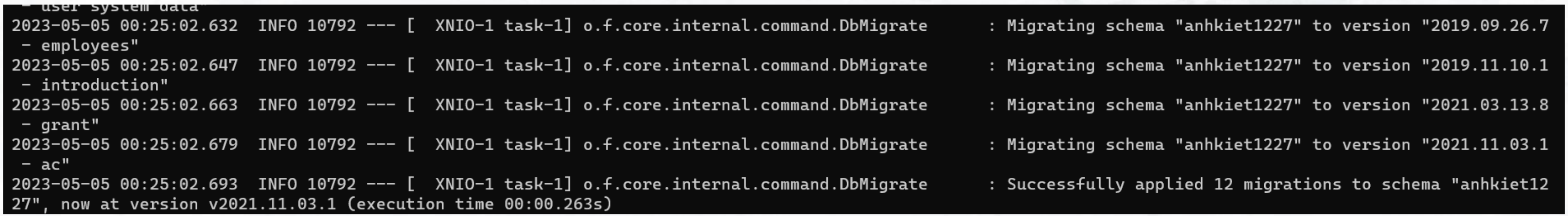
PyGoat – Top 10 OWASP



```
None
None
None
None
admin
'or 1=1--
SELECT * FROM introduction_sql_lab_table WHERE id='admin'AND password=''or 1=1--'
admin
[2023-05-04 15:37:19 +0000] [1] [INFO] Handling signal: int
```

No announcement on OpenEDR

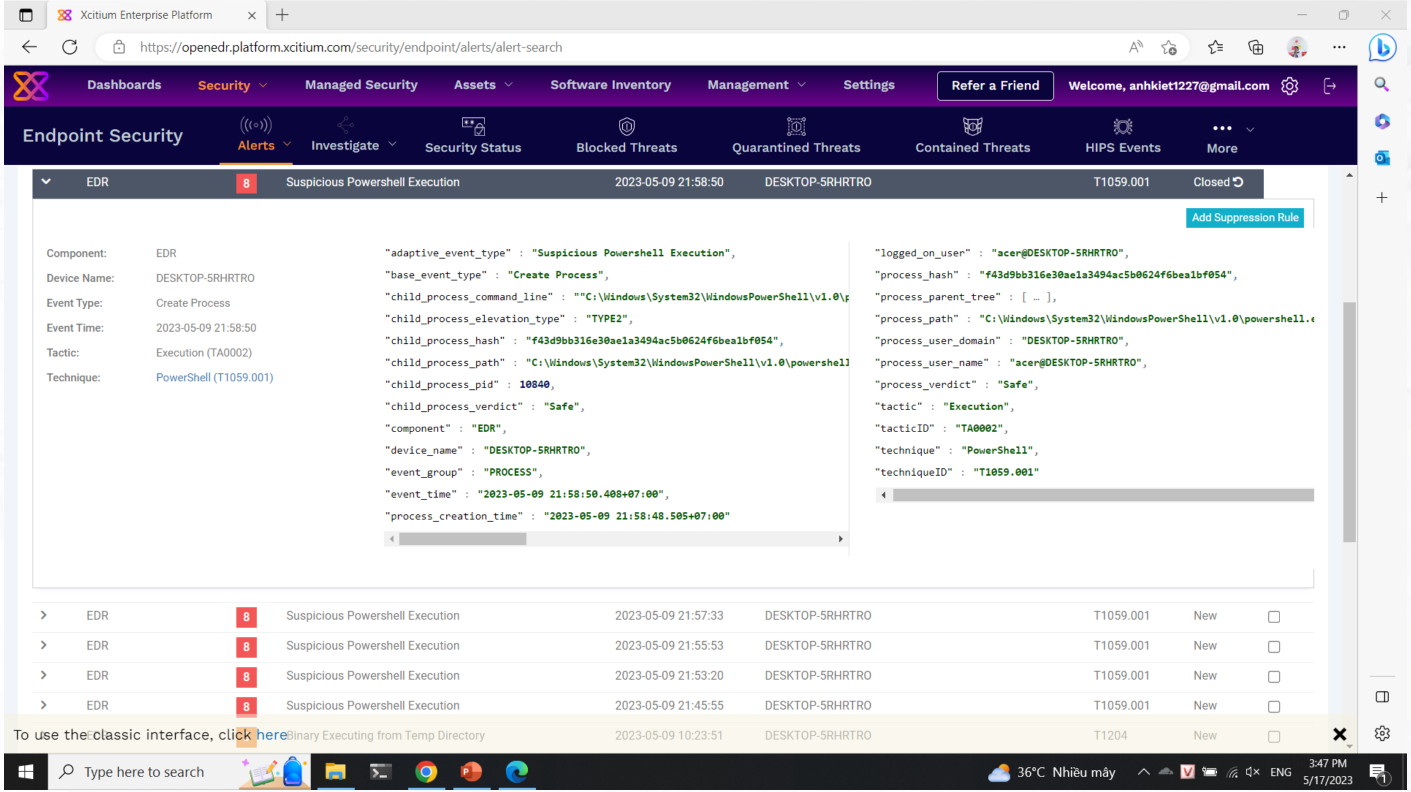
WebGoat – Top 10 OWASP



```
 - user system data"
2023-05-05 00:25:02.632  INFO 10792 --- [  XNIO-1 task-1] o.f.core.internal.command.DbMigrate      : Migrating schema "anhkiet1227" to version "2019.09.26.7
 - employees"
2023-05-05 00:25:02.647  INFO 10792 --- [  XNIO-1 task-1] o.f.core.internal.command.DbMigrate      : Migrating schema "anhkiet1227" to version "2019.11.10.1
 - introduction"
2023-05-05 00:25:02.663  INFO 10792 --- [  XNIO-1 task-1] o.f.core.internal.command.DbMigrate      : Migrating schema "anhkiet1227" to version "2021.03.13.8
 - grant"
2023-05-05 00:25:02.679  INFO 10792 --- [  XNIO-1 task-1] o.f.core.internal.command.DbMigrate      : Migrating schema "anhkiet1227" to version "2021.11.03.1
 - ac"
2023-05-05 00:25:02.693  INFO 10792 --- [  XNIO-1 task-1] o.f.core.internal.command.DbMigrate      : Successfully applied 12 migrations to schema "anhkiet12
27", now at version v2021.11.03.1 (execution time 00:00.263s)
```

No announcement on OpenEDR

Weakness



EDR	8	Suspicious Powershell Execution	2023-05-09 21:58:50	DESKTOP-5RHRTRO	T1059.001	Closed

Component:	EDR
Device Name:	DESKTOP-5RHRTRO
Event Type:	Create Process
Event Time:	2023-05-09 21:58:50
Tactic:	Execution (TA0002)
Technique:	PowerShell (T1059.001)

```
"adaptive_event_type" : "Suspicious Powershell Execution",
"base_event_type" : "Create Process",
"child_process_command_line" : ""C:\Windows\System32\WindowsPowerShell\v1.0\p
"child_process_elevation_type" : "TYPE2",
"child_process_hash" : "f43d9bb316e30ae1a3494ac5b0624f6bea1bf054",
"child_process_path" : "C:\Windows\System32\WindowsPowerShell\v1.0\powershell
"child_process_pid" : 10840,
"child_process_verdict" : "Safe",
"component" : "EDR",
"device_name" : "DESKTOP-5RHRTRO",
"event_group" : "PROCESS",
"event_time" : "2023-05-09 21:58:50.408+07:00",
"process_creation_time" : "2023-05-09 21:58:48.505+07:00"
```

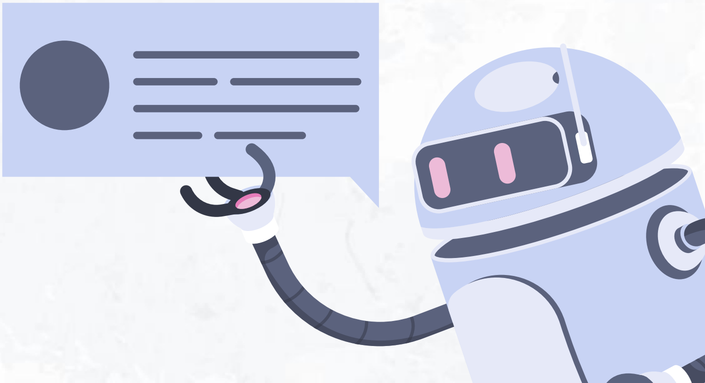
```
"logged_on_user" : "acer@DESKTOP-5RHRTRO",
"process_hash" : "f43d9bb316e30ae1a3494ac5b0624f6bea1bf054",
"process_parent_tree" : [ … ],
"process_path" : "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.e
"process_user_domain" : "DESKTOP-5RHRTRO",
"process_user_name" : "acer@DESKTOP-5RHRTRO",
"process_verdict" : "Safe",
"tactic" : "Execution",
"tacticID" : "TA0002",
"technique" : "PowerShell",
"techniqueID" : "T1059.001"
```

EDR	8	Suspicious Powershell Execution	2023-05-09 21:57:33	DESKTOP-5RHRTRO	T1059.001	New	□
EDR	8	Suspicious Powershell Execution	2023-05-09 21:55:53	DESKTOP-5RHRTRO	T1059.001	New	□
EDR	8	Suspicious Powershell Execution	2023-05-09 21:53:20	DESKTOP-5RHRTRO	T1059.001	New	□
EDR	8	Suspicious Powershell Execution	2023-05-09 21:45:55	DESKTOP-5RHRTRO	T1059.001	New	□
EDR		Binary Executing from Temp Directory	2023-05-09 10:23:51	DESKTOP-5RHRTRO	T1204	New	□

To use the classic interface, click here

02 →

Registry Spy



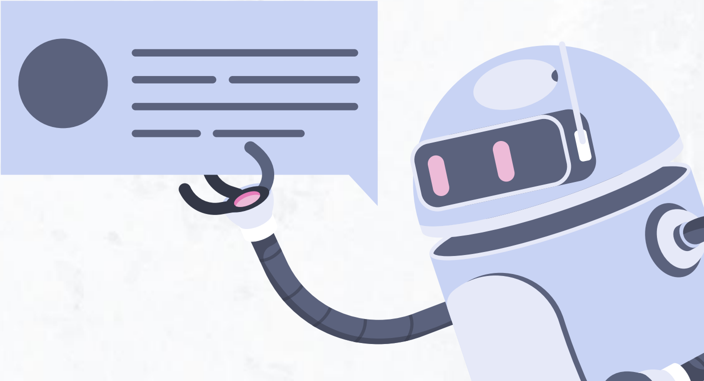
Registry Spy

Registry Spy is a free, open-source cross-platform Windows Registry viewer. It is a fast, modern, and versatile explorer for raw registry files.

Requirement installation

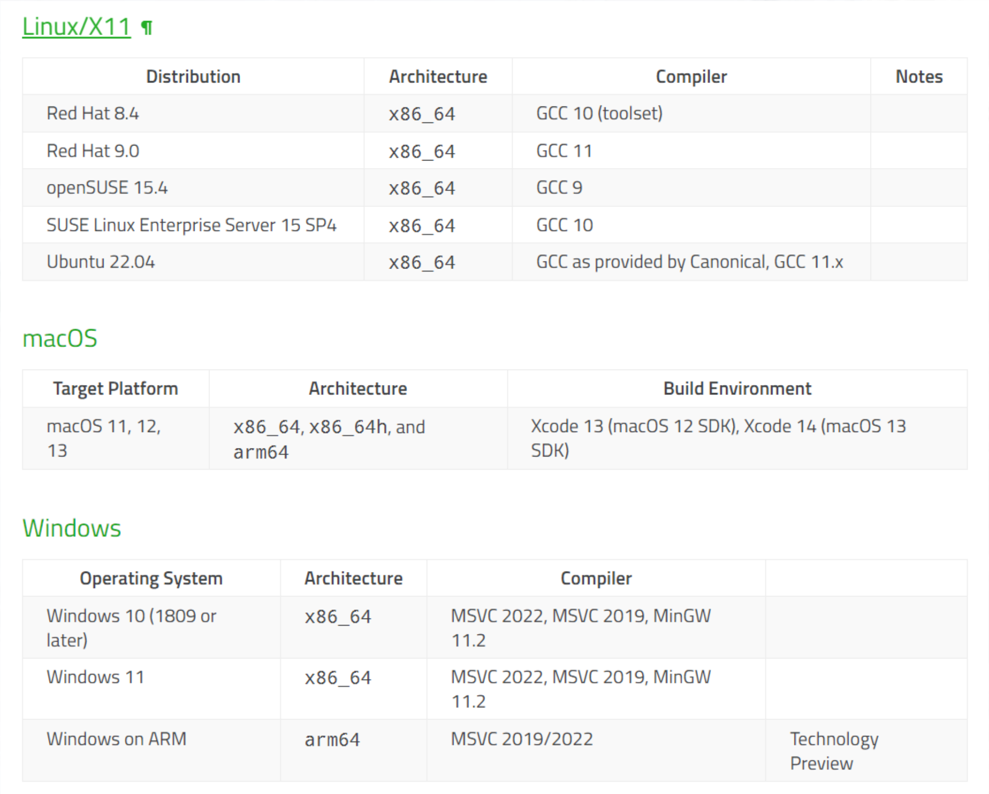
(-) Python >= 3.8 →

Python is a high-level, general-purpose programming language. Its design philosophy emphasizes code readability with the use of significant indentation via the off-side rule.



Requirement installation

(-) Operation System →



Linux/X11 ¶

Distribution	Architecture	Compiler	Notes
Red Hat 8.4	x86_64	GCC 10 (toolset)	
Red Hat 9.0	x86_64	GCC 11	
openSUSE 15.4	x86_64	GCC 9	
SUSE Linux Enterprise Server 15 SP4	x86_64	GCC 10	
Ubuntu 22.04	x86_64	GCC as provided by Canonical, GCC 11.x	

macOS

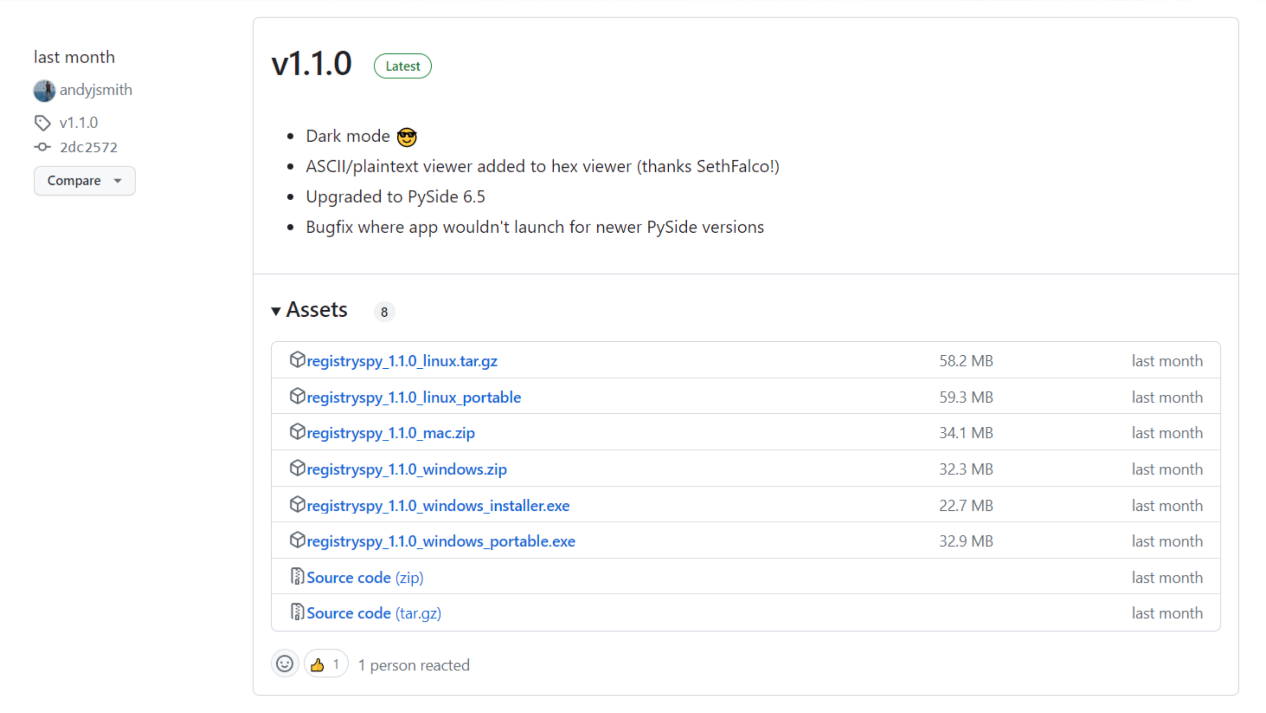
Target Platform	Architecture	Build Environment
macOS 11, 12, 13	x86_64, x86_64h, and arm64	Xcode 13 (macOS 12 SDK), Xcode 14 (macOS 13 SDK)

Windows

Operating System	Architecture	Compiler	
Windows 10 (1809 or later)	x86_64	MSVC 2022, MSVC 2019, MinGW 11.2	
Windows 11	x86_64	MSVC 2022, MSVC 2019, MinGW 11.2	
Windows on ARM	arm64	MSVC 2019/2022	Technology Preview

Installation

(-) Version →



last month

andyjsmith

v1.1.0

2dc2572

v1.1.0

- Dark mode 😎
- ASCII/plaintext viewer added to hex viewer (thanks SethFalco!)
- Upgraded to PySide 6.5
- Bugfix where app wouldn't launch for newer PySide versions

▾ Assets 8

registryspy_1.1.0_linux.tar.gz	58.2 MB	last month
registryspy_1.1.0_linux_portable	59.3 MB	last month
registryspy_1.1.0_mac.zip	34.1 MB	last month
registryspy_1.1.0_windows.zip	32.3 MB	last month
registryspy_1.1.0_windows_installer.exe	22.7 MB	last month
registryspy_1.1.0_windows_portable.exe	32.9 MB	last month
Source code (zip)		last month
Source code (tar.gz)		last month

👍 1 1 person reacted

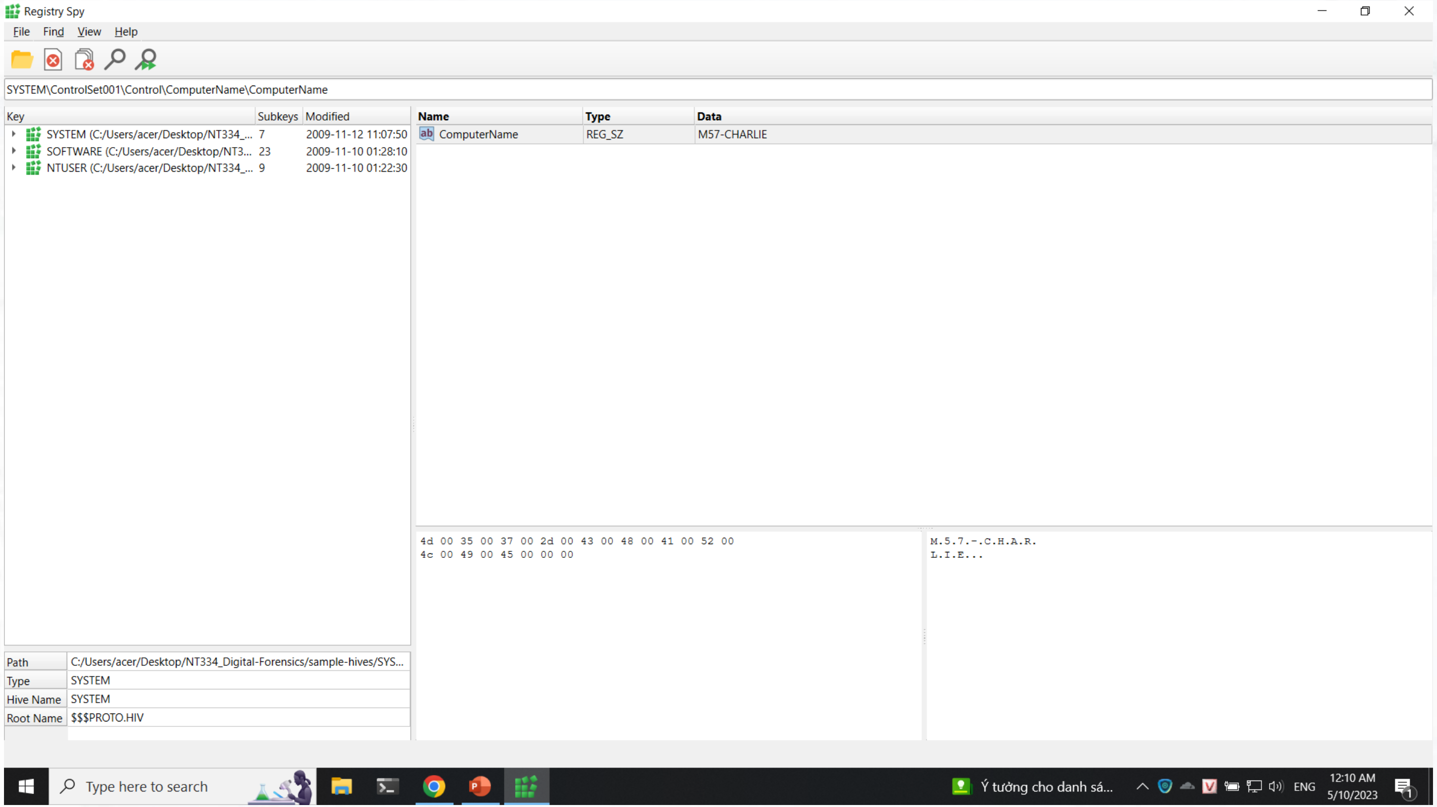
Installation

(-) Pip → pip install registryspy → registryspy

(-) Manual → pip install –r requirements.txt →
python setup.py install → registryspy

(-) Standalone → pip install –r requirements.txt →
python registryspy.py

Implemetation



SYSTEM\ControlSet001\Control\ComputerName\ComputerName

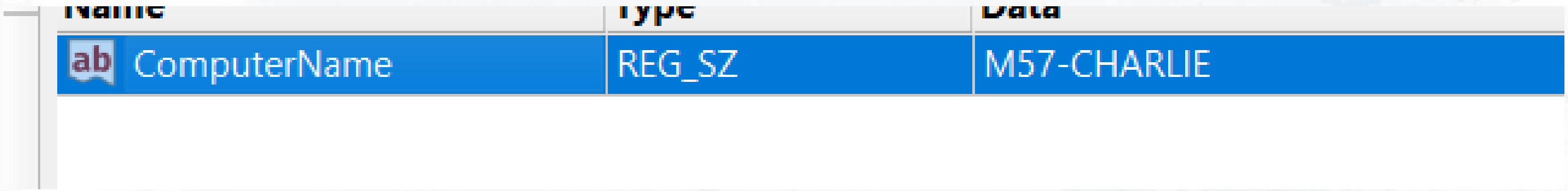
Key	Subkeys	Modified
SYSTEM (C:/Users/acer/Desktop/NT334_...	7	2009-11-12 11:07:50
SOFTWARE (C:/Users/acer/Desktop/NT3...	23	2009-11-10 01:28:10
NTUSER (C:/Users/acer/Desktop/NT334_...	9	2009-11-10 01:22:30

Name	Type	Data
ComputerName	REG_SZ	M57-CHARLIE

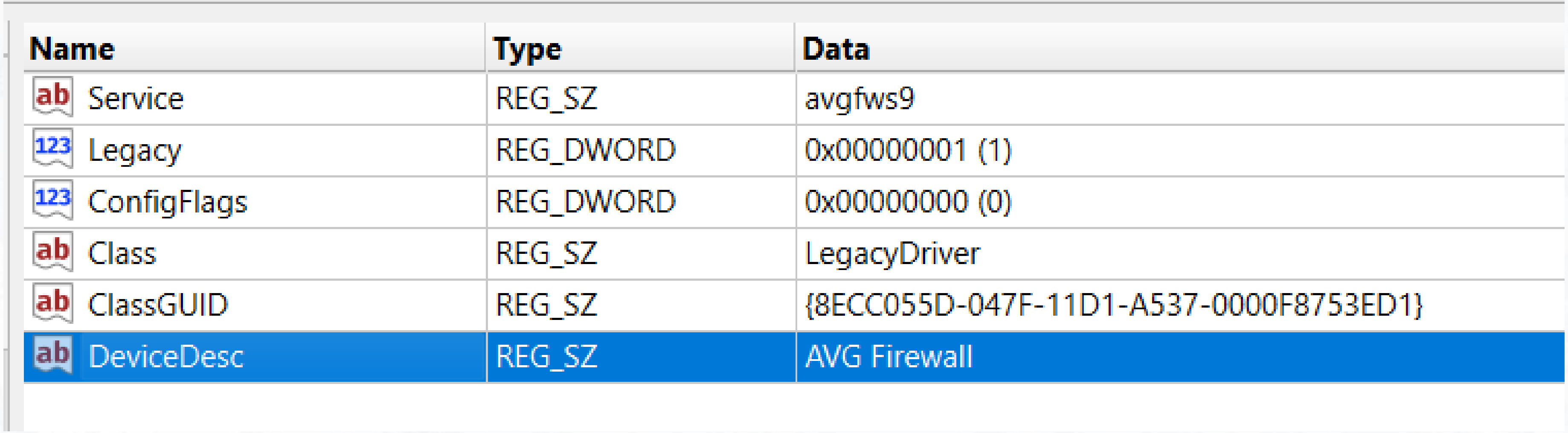
```
4d 00 35 00 37 00 2d 00 43 00 48 00 41 00 52 00    M.5.7.-.C.H.A.R.
4c 00 49 00 45 00 00 00                            L.I.E...
```

Path	C:/Users/acer/Desktop/NT334_Digital-Forensics/sample-hives/SYS...
Type	SYSTEM
Hive Name	SYSTEM
Root Name	$$$PROTO.HIV

Implemetation

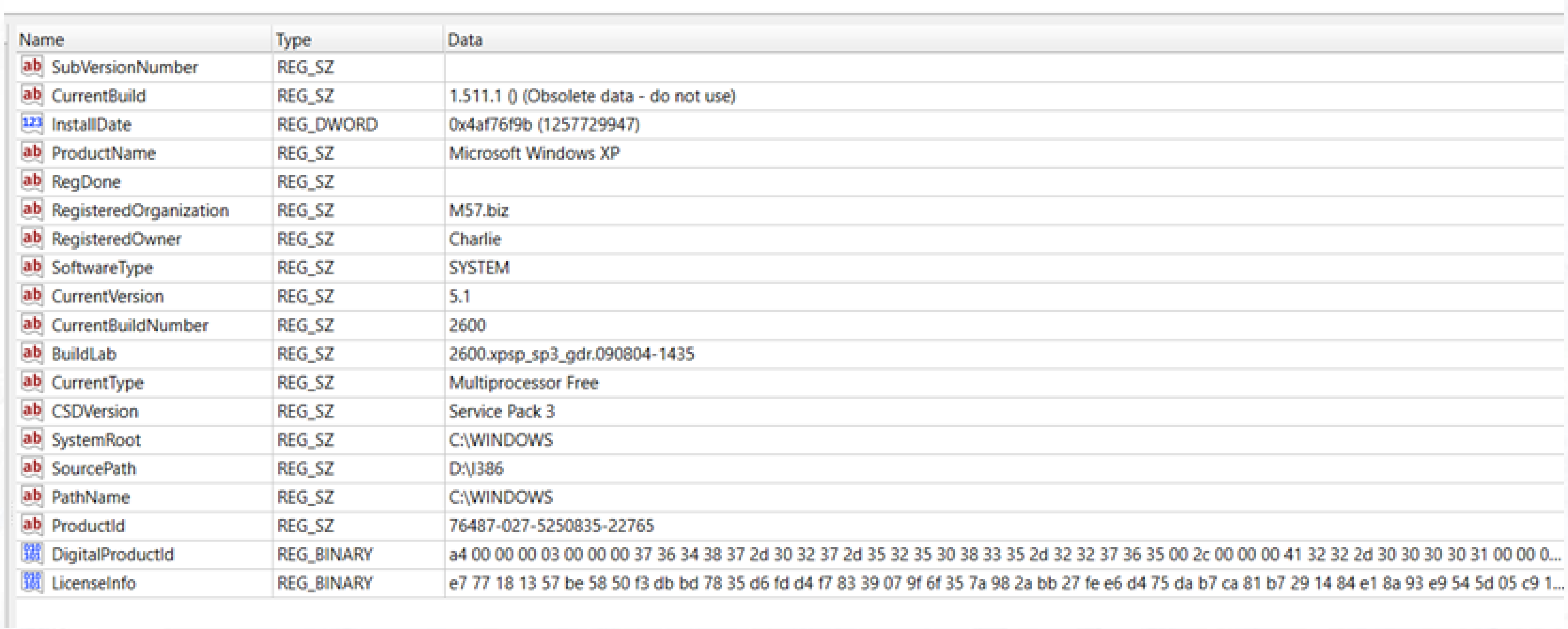


Name	Type	Data
ComputerName	REG_SZ	M57-CHARLIE



Name	Type	Data
Service	REG_SZ	avgfws9
Legacy	REG_DWORD	0x00000001 (1)
ConfigFlags	REG_DWORD	0x00000000 (0)
Class	REG_SZ	LegacyDriver
ClassGUID	REG_SZ	{8ECC055D-047F-11D1-A537-0000F8753ED1}
DeviceDesc	REG_SZ	AVG Firewall

Implemetation



Name	Type	Data
SubVersionNumber	REG_SZ	
CurrentBuild	REG_SZ	1.511.1 () (Obsolete data - do not use)
InstallDate	REG_DWORD	0x4af76f9b (1257729947)
ProductName	REG_SZ	Microsoft Windows XP
RegDone	REG_SZ	
RegisteredOrganization	REG_SZ	M57.biz
RegisteredOwner	REG_SZ	Charlie
SoftwareType	REG_SZ	SYSTEM
CurrentVersion	REG_SZ	5.1
CurrentBuildNumber	REG_SZ	2600
BuildLab	REG_SZ	2600.xpsp_sp3_gdr.090804-1435
CurrentType	REG_SZ	Multiprocessor Free
CSDVersion	REG_SZ	Service Pack 3
SystemRoot	REG_SZ	C:\WINDOWS
SourcePath	REG_SZ	D:\I386
PathName	REG_SZ	C:\WINDOWS
ProductId	REG_SZ	76487-027-5250835-22765
DigitalProductId	REG_BINARY	a4 00 00 00 03 00 00 00 37 36 34 38 37 2d 30 32 37 2d 35 32 35 30 38 33 35 2d 32 32 37 36 35 00 2c 00 00 00 41 32 32 2d 30 30 30 30 31 00 00 0...
LicenseInfo	REG_BINARY	e7 77 18 13 57 be 58 50 f3 db bd 78 35 d6 fd d4 f7 83 39 07 9f 6f 35 7a 98 2a bb 27 fe e6 d4 75 da b7 ca 81 b7 29 14 84 e1 8a 93 e9 54 5d 05 c9 1...

Resources

- What is EDR (Endpoint Detection & Response)? Open source EDR® (openedr.com)
- GitHub - andyjsmith/Registry-Spy: Cross-platform registry browser for raw Windows registry files

Thanks! →

Any questions?

CREDITS: This presentation template was created by **Slidesgo** and includes icons by **Flaticon**, infographics & images by **Freepik** and content by **Eliana Delacour**

Please, keep this slide as attribution