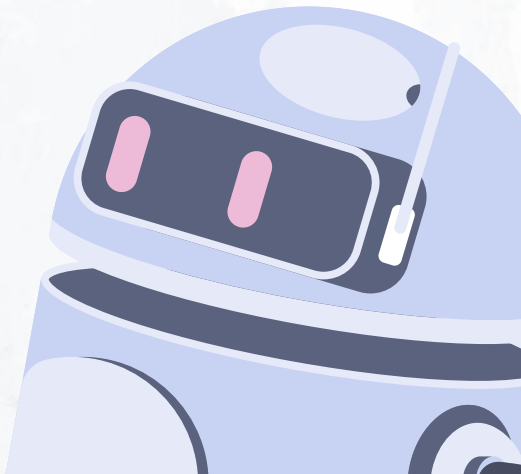


OpenEDR Registry Spy →

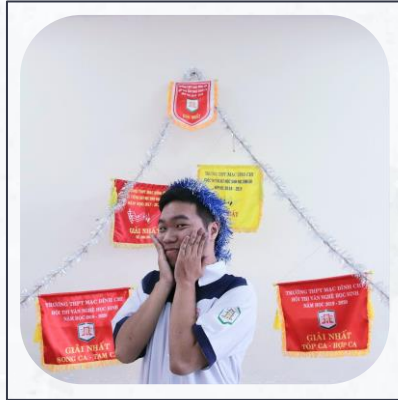


OUR TEAM



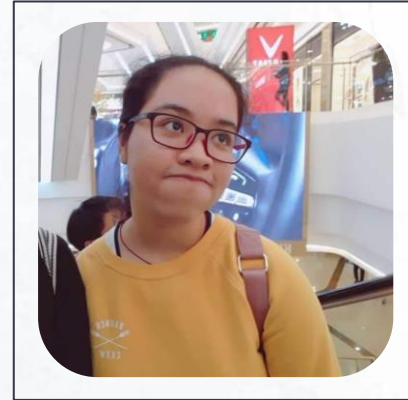
**Nguyễn Bình
Thực Trâm**

20520815



Võ Anh Kiệt

20520605



**Nguyễn Bùi
Kim Ngân**

20520648

Table of contents

01 → EDR - OpenEDR

02 → Registry Spy

01 →

EDR – Endpoint Detect Response
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.

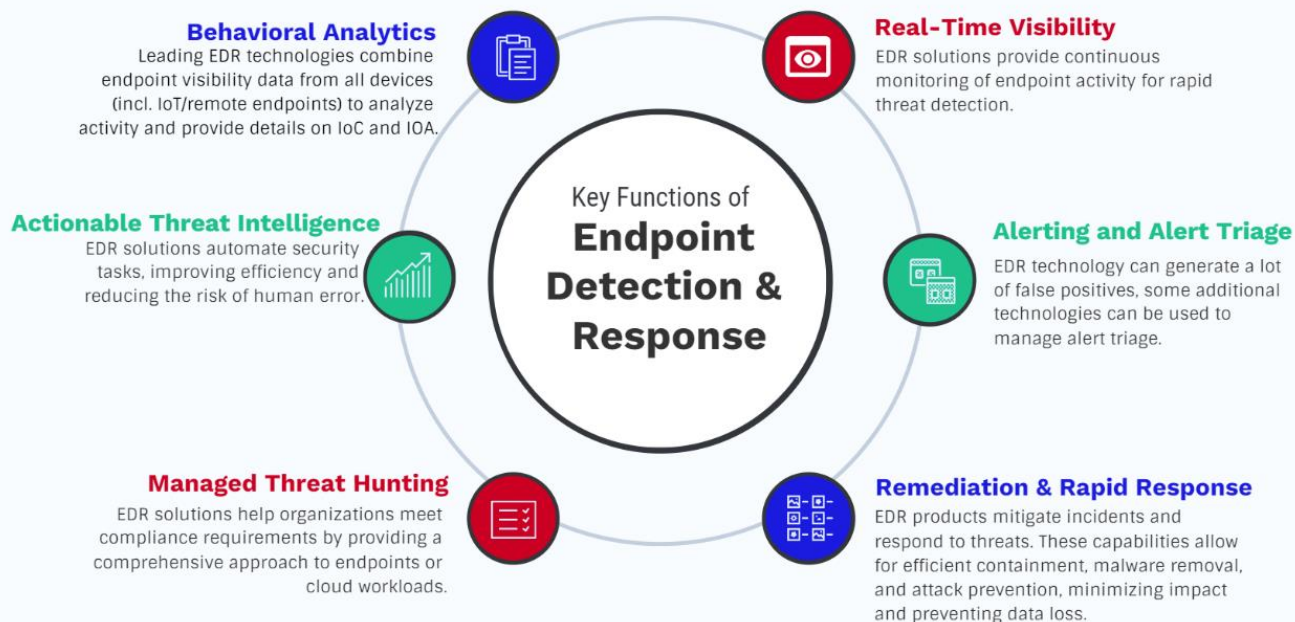


OpenEDR



OpenEDR

Key EDR Functions



Installation

The screenshot shows a web browser window with two tabs: "Xcitium Enterprise Platform" and "What is EDR (Endpoint Detection)". The address bar shows the URL "https://openedr.platform.xcitium.com/login". The page has a dark purple background with the "OPENEDR" logo and "Provided by XCITIUM" text. Below the logo are two input fields: "Email" and "Password", both with red error messages "The field is required". A "Reset Password?" link is next to the password field. There is a checkbox for "Remember this device sign in" and a "Log in" button. The footer contains copyright information and links for "Contact Support", "Terms & Conditions", "Privacy Policy", and "Legal Repository". The Windows taskbar at the bottom shows the search bar, task view, and several application icons, along with system information like temperature, weather, and time.

Xcitium Enterprise Platform x What is EDR (Endpoint Detection) x +

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

OPENEDR
Provided by XCITIUM

* 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.

Contact Support Terms & Conditions Privacy Policy Legal Repository

Type here to search

35°C Mưa lớn 2:55 PM 5/17/2023

Installation Agent

The screenshot shows the Xcitium Enterprise Platform web interface. The top navigation bar includes links for Dashboards, Security, Managed Security, Assets, Software Inventory, Management, and Settings. The user is logged in as 'anhkiet1227@gmail.com'. The main content area is titled 'Enrollment Wizard' and shows two steps: '1 Enrollment Options' (completed) and '2 Installation Instructions' (current step). The 'Enrollment Link' section provides a link to complete the user device enrollment: <https://kutt.comodo.com/5qMIUt>. Below this, a full link is provided: <https://anhkiet1227gmailcom.itsm-us1.comodo.com/enroll/device/by/token/b93fb0ada3c5d8d>. A 'Send' button is available. The 'What's next?' section offers two options: 'Enroll Another Device' and 'Go to Bulk Installation Package'. At the bottom, there are 'Back' and 'Finish' buttons. A footer note suggests using the classic interface via a link.

Xcitium Enterprise Platform

https://openedr.platform.xcitium.com/assets/endpoint/device-list

Dashboards Security Managed Security Assets Software Inventory Management Settings Refer a Friend Welcome, anhkiet1227@gmail.com

Devices Device List Bulk Installation Package

Enrollment Wizard

1 Enrollment Options

2 Installation Instructions

Enrollment Link

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

<https://kutt.comodo.com/5qMIUt>

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](#)

3:09 PM 5/17/2023

Installation Agent

The screenshot displays the Xcitium Enterprise Platform web interface. The browser address bar shows the URL `https://openedr.platform.xcitium.com/assets/endpoint/device-list`. The navigation bar includes links for Dashboards, Security, Managed Security, Assets, Software Inventory, Management, and Settings. The user is logged in as `anhkiet1227@gmail.com`.

The main section is titled "Devices" and contains two tabs: "Device List" (active) and "Bulk Installation Package". On the left, there is a sidebar with a search bar for group names and a list of groups, including "Default Customer".

The "Device Management" section features a toolbar with icons for various actions: Enroll Device, Remote Control, File Transfer, Remote Tools, Run Procedure, Manage Profiles, Install or Manage Packages, Refresh Device Information, Power Options, Owner, Send Message, Passcode, and More. Below the toolbar is a search bar for devices and a table of device information.

<input type="checkbox"/>	OS	NAME	ACTIVE COMPONENTS	VIRTUAL DESKTOP	PATCH STATUS	CUSTOMER	LAST LOGGED IN USER	LAST ACTIVITY
<input type="checkbox"/>	Windows	DESKTOP-5RHRTRO	AG CCS EDR MDR	Yes	2	Default Customer	DESKTOP-5RHRTRO\acer	2023/05/17 02:10:07 AM

At the bottom of the table, it indicates "Results per page: 20" and "Displaying 1 of 1 results". A footer note suggests using the classic interface via a link.

The Windows taskbar at the bottom shows the system clock as 3:11 PM on 5/17/2023, with a temperature of 35°C and weather conditions of "Mưa lớn" (Heavy Rain).

Installation Packages

The screenshot displays the Xcitium Enterprise Platform web interface. The top navigation bar includes links for Dashboards, Security, Managed Security, Assets, Software Inventory, Management, and Settings. The user is logged in as 'anhkiet1227@gmail.com'. The main content area is titled 'Devices' and shows a 'Device List' table with columns for OS and NAME. A modal dialog titled 'Install Additional Xcitium Packages' is open, allowing the user to install the Xcitium Client - Security and Xcitium Client - EDR. The dialog includes options for rebooting the device (Force the reboot in 5 minutes, Suppress the reboot, or Warn about the reboot) and a text area for a custom reboot message. The 'Install' button is at the bottom right of the dialog.

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

To use the classic interface, click [here](#)

Tool scanning

Xcitium Enterprise Platform

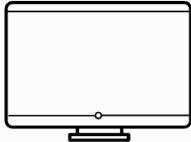
https://openedr.platform.xcitium.com/assets/endpoint/device-list

Dashboards Security Managed Security Assets Software Inventory Management Settings Refer a Friend Welcome, anhkiet1227@gmail.com

Devices Device List Bulk Installation Package

Custom device name	DESKTOP-SRHRTRO
Name	DESKTOP-SRHRTRO
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

Thumbnail not supported



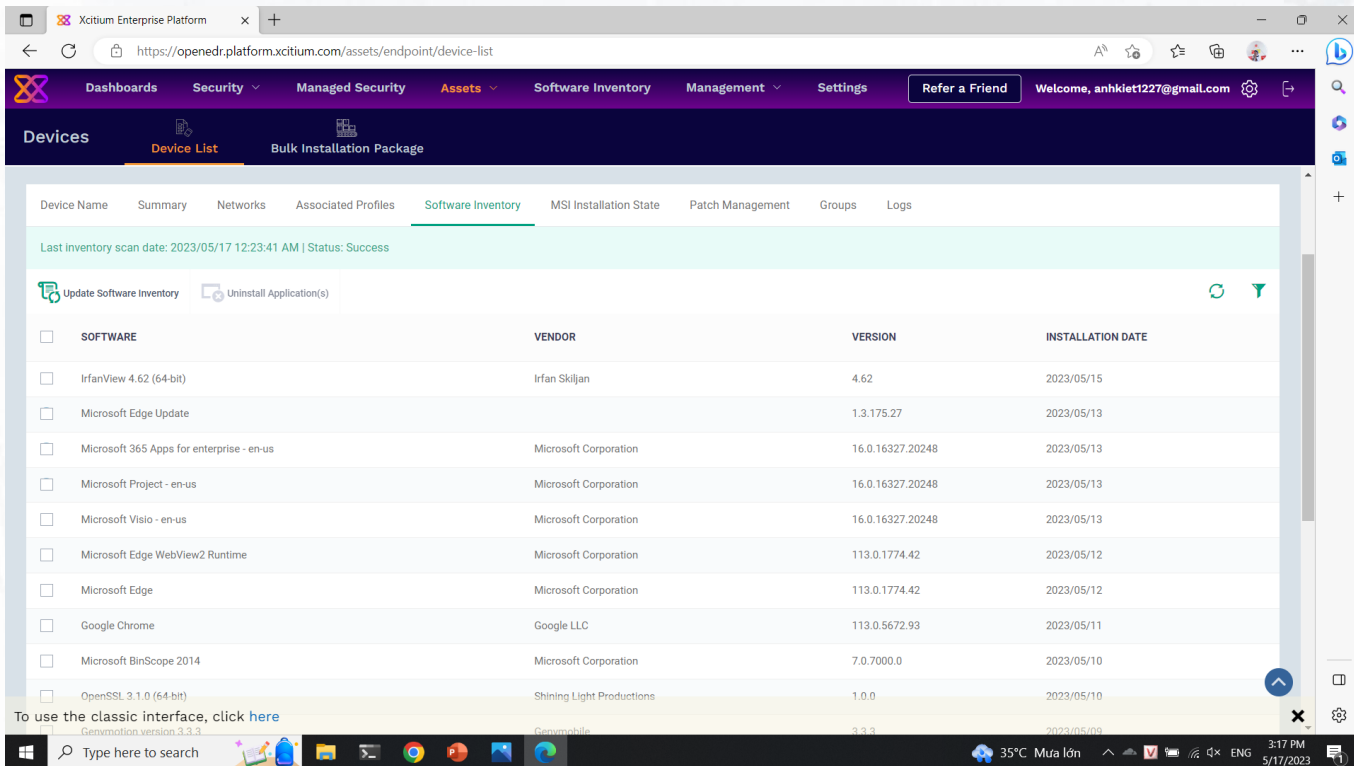
OS	Windows
OS name	Microsoft Windows 10 Pro (x64)
OS version	10.0.19045
OS full version	Version 22H2 (OS Build 19045.2965)
Service pack	N/A
Build version	19045
Reboot time	2023/05/15 08:22:36 PM
Reboot reason	The process C:\Windows\System32\RuntimeBroker.exe (DESKTOP-SRHRTRO) has initiated the power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

To use the classic interface, click [here](#). 2023/05/17 02:16:33 AM

Type here to search

35°C Mưa lớn 3:16 PM 5/17/2023





Tool scanning



The screenshot displays the Xcitium Enterprise Platform web interface. The top navigation bar includes links for Dashboards, Security, Managed Security, Assets, Software Inventory, Management, and Settings. The user is logged in as 'Welcome, anhkiet227@gmail.com'. The main content area is titled 'Devices' and shows the 'Device List' tab. A sub-tab 'Software Inventory' is active, displaying a table of installed software on a device. The table has columns for Software, Vendor, Version, and Installation Date. The last inventory scan date is 2023/05/17 12:23:41 AM, with a status of Success. Below the table, there are buttons for 'Update Software Inventory' and 'Uninstall Application(s)'. The Windows taskbar at the bottom shows the time as 3:17 PM on 5/17/2023, with a temperature of 35°C and weather 'Mưa lớn'.

Device Name Summary Networks Associated Profiles **Software Inventory** MSI Installation State Patch Management Groups Logs

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

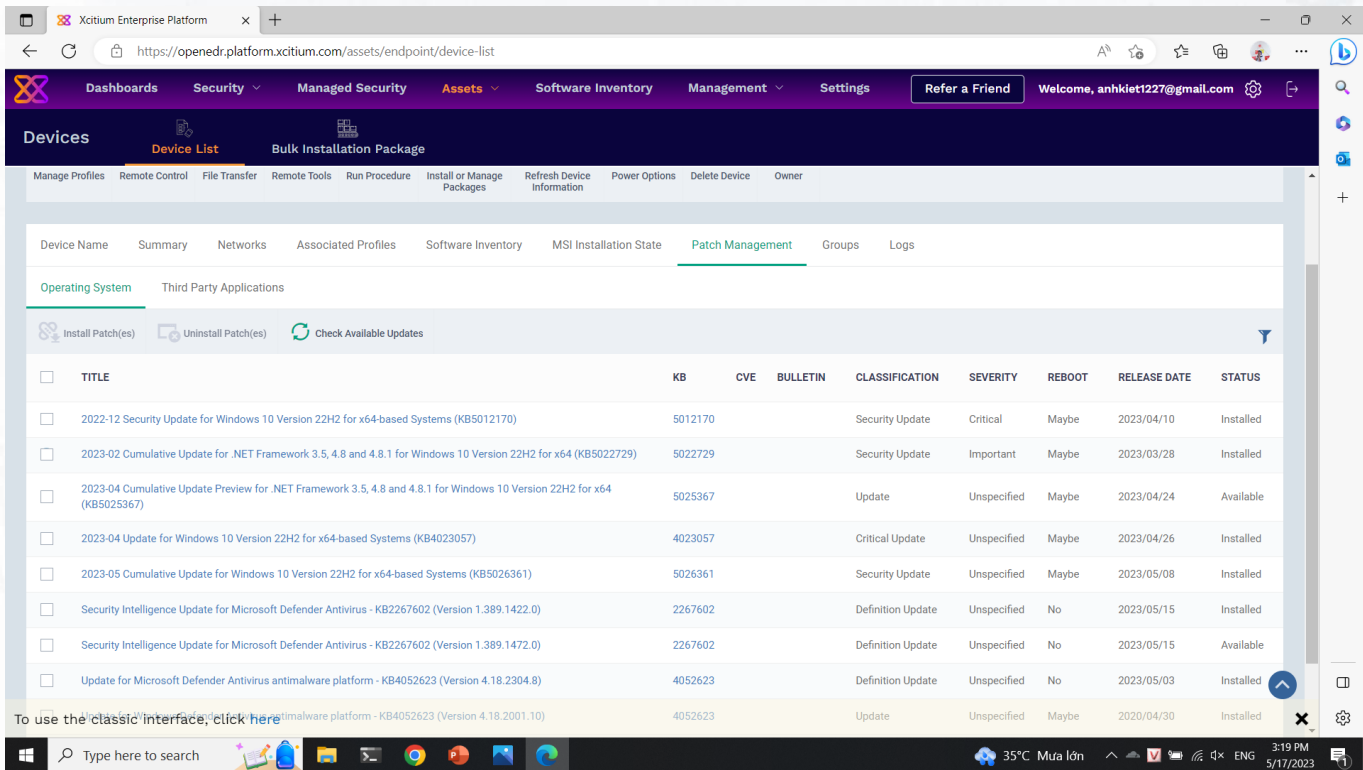
 Update Software Inventory  Uninstall Application(s)  

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

To use the classic interface, click [here](#)

35°C Mưa lớn 3:17 PM 5/17/2023

Tool scanning



The screenshot displays the Xcitium Enterprise Platform interface. The top navigation bar includes links for Dashboards, Security, Managed Security, Assets, Software Inventory, Management, and Settings. The user is logged in as anhkiet1227@gmail.com. The main section is titled 'Devices' and shows the 'Device List' tab. Below this, there are tabs for 'Operating System' and 'Third Party Applications'. The 'Patch Management' tab is active, showing a list of updates. The table lists various updates, including Windows 10 Security Updates, .NET Framework updates, and Microsoft Defender Antivirus updates. The table columns include Title, KB, CVE, Bulletin, Classification, Severity, Reboot, Release Date, and Status.

	TITLE	KB	CVE	BULLETIN	CLASSIFICATION	SEVERITY	REBOOT	RELEASE DATE	STATUS
<input type="checkbox"/>	2022-12 Security Update for Windows 10 Version 22H2 for x64-based Systems (KB5012170)	5012170			Security Update	Critical	Maybe	2023/04/10	Installed
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	2023-04 Update for Windows 10 Version 22H2 for x64-based Systems (KB4023057)	4023057			Critical Update	Unspecified	Maybe	2023/04/26	Installed
<input type="checkbox"/>	2023-05 Cumulative Update for Windows 10 Version 22H2 for x64-based Systems (KB5026361)	5026361			Security Update	Unspecified	Maybe	2023/05/08	Installed
<input type="checkbox"/>	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.389.1422.0)	2267602			Definition Update	Unspecified	No	2023/05/15	Installed
<input type="checkbox"/>	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.389.1472.0)	2267602			Definition Update	Unspecified	No	2023/05/15	Available
<input type="checkbox"/>	Update for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.2304.8)	4052623			Definition Update	Unspecified	No	2023/05/03	Installed
<input type="checkbox"/>	Update for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.2001.10)	4052623			Update	Unspecified	Maybe	2020/04/30	Installed

To use the classic interface, [click here](#)

Tool scanning

The screenshot displays the Xcitiem Enterprise Platform interface. The browser address bar shows the URL <https://openedr.platform.xcitiem.com/security/endpoint/alerts/alert-search>. The platform's navigation bar includes sections for Dashboards, Security, Managed Security, Assets, Software Inventory, Management, and Settings. The main navigation bar highlights Endpoint Security, with sub-sections for Alerts, Investigate, Security Status, Blocked Threats, Quarantined Threats, Contained Threats, HIPS Events, and More.

The alert details for 'System Information Discovery' are shown, including the following fields:

- 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)

The alert details are displayed in a JSON format:

```
{  "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": "d61ff641c2f6d45dad26c02daeea8dabee8204",  "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": "filefb0fddc156e4c61c5f78a54700e4e7984d55d",  "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"}
```

At the bottom of the interface, a message states: "To use the classic interface, click [here](#)". The Windows taskbar at the bottom shows the time as 3:23 PM on 5/17/2023.

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-5RHRTR0

-

New

■

Close Alert

Component: Antivirus

Device Name: DESKTOP-5RHRTR0

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-5RHRTR0",

"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

The screenshot displays the Xciti Enterprise Platform interface, specifically the 'Quarantined Threats' section. The interface features a top navigation bar with various tabs like Dashboards, Security, Managed Security, Assets, Software Inventory, Management, and Settings. The 'Security' tab is active, and the 'Quarantined Threats' sub-tab is selected. On the left, there is a sidebar with a search bar and a list of groups, including 'Default Customer'. The main area shows a table of quarantined threats with columns for OS, File Name, File Hash, Signature, Xciti Rating, Admin Rating, Devices Detected On, Last Quarantined, and Last Action on Group. Three threats are listed: x0r-p.exe, scofield-usb..., and x0r.exe, all identified as 'Worm.Win32...' and 'Unrecognized'. The interface also includes action buttons like 'Delete File from Devices', 'Restore File on Devices', and 'Restore All Files on Devices'. At the bottom, there is a footer with a link to the classic interface and a system tray showing the date and time.

Search group name

Show all

Default Customer

Quarantined Threats

Delete File from Devices Restore File on Devices Restore All Files on Devices Rate as Unrecognized Rate as Trusted Rate as Malicious More

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

« Prev 1 Next »

Results per page: 20

To use the classic interface, click [here](#)

Type here to search

32°C Nắng rải rác 6:38 PM 5/4/2023

Malware

▼

Antivirus

4

Antivirus Detect Malware

2023-05-04 18:33:39

DESKTOP-5RHRTRO

-

New

■

Close Alert

Component:

Device Name:

Event Type:

Event Time:

Antivirus

DESKTOP-5RHRTRO

Antivirus Detect Malware

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

▼

Antivirus

4

Antivirus Delete from Quarantine

2023-05-04 18:41:16

DESKTOP-5RHRTRO

-

New

■

Close Alert

Component:

Antivirus

"admin_verdict" : "Unknown",

Device Name:

DESKTOP-5RHRTRO

"base_event_type" : "Antivirus Delete from Quarantine",

Event Type:

Antivirus Delete from Quarantine

"component" : "Antivirus",

Event Time:

2023-05-04 18:41:16

"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" : "scotfield-usb.exe",

"file_path" : "C:\Users\acer\Desktop\getGitHub\theZoo\malware\Source\Ori,

◀

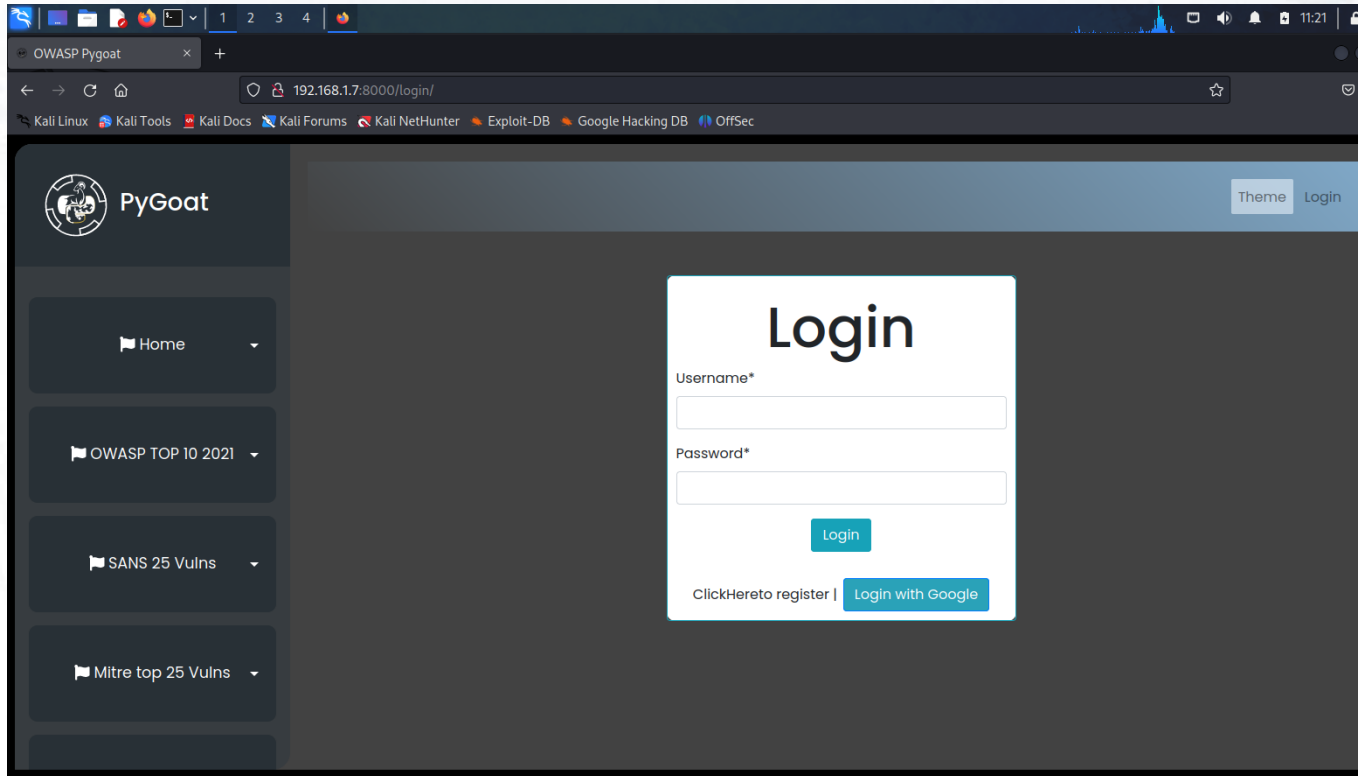
Malware

▼	Antivirus	10	Malware Detection	2023-05-04 18:33:39	DESKTOP-5RHRTR0	-	New	■
View Xcitium Verdict Cloud Report								Close Alert
Component:	Antivirus	"base_event_type" : "Antivirus Detect Malware",			"component" : "Antivirus",			
Device Name:	DESKTOP-5RHRTR0	"device_name" : "DESKTOP-5RHRTR0",			"file_name" : "scofield-usb.exe",			
Event Type:	Antivirus Detect Malware	"event_time" : "2023-05-04 18:33:39.002+07:00",			"file_path" : "C:\\Users\\acer\\Desktop\\getGitHub\\theZoo\\malware\\Source\\Ori			
Event Time:	2023-05-04 18:33:39	"file_hash" : "c3d89f55da045aca0a624ab10e3250b1d20311d3"			<div><div></div></div>			
>	Antivirus	10	Malware Detection	2023-05-04 18:33:39	DESKTOP-5RHRTR0	-	New	□

PyGoat – Top 10 OWASP

```
PowerShell
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



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
[2022-05-04 15:27:10:10000] [1] [INFO] User login successful
```

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

Xcitium Enterprise Platform

https://openedr.platform.xcitium.com/security/endpoint/alerts/alert-search

Endpoint Security

Alerts | Investigate | Security Status | Blocked Threats | Quarantined Threats | Contained Threats | HIPS Events | More

EDR | 8 | Suspicious Powershell Execution | 2023-05-09 21:58:50 | DESKTOP-SRHRTR0 | T1059.001 | Closed

[Add Suppression Rule](#)

Component: EDR
Device Name: DESKTOP-SRHRTR0
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\\powershell.exe",
"child_process_elevation_type": "TYPE2",
"child_process_hash": "f43d9bb316e30ae1a3494ac5b0624f6bea1bf054",
"child_process_path": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",
"child_process_pid": 10840,
"child_process_verdict": "Safe",
"component": "EDR",
"device_name": "DESKTOP-SRHRTR0",
"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-SRHRTR0",
"process_hash": "f43d9bb316e30ae1a3494ac5b0624f6bea1bf054",
"process_parent_tree": [ ... ],
"process_path": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",
"process_user_domain": "DESKTOP-SRHRTR0",
"process_user_name": "acer@DESKTOP-SRHRTR0",
"process_verdict": "Safe",
"tactic": "Execution",
"tacticID": "TA0002",
"technique": "PowerShell",
"techniqueID": "T1059.001"
```

>	EDR	8	Suspicious Powershell Execution	2023-05-09 21:57:33	DESKTOP-SRHRTR0	T1059.001	New	<input type="checkbox"/>
>	EDR	8	Suspicious Powershell Execution	2023-05-09 21:55:53	DESKTOP-SRHRTR0	T1059.001	New	<input type="checkbox"/>
>	EDR	8	Suspicious Powershell Execution	2023-05-09 21:53:20	DESKTOP-SRHRTR0	T1059.001	New	<input type="checkbox"/>
>	EDR	8	Suspicious Powershell Execution	2023-05-09 21:45:55	DESKTOP-SRHRTR0	T1059.001	New	<input type="checkbox"/>

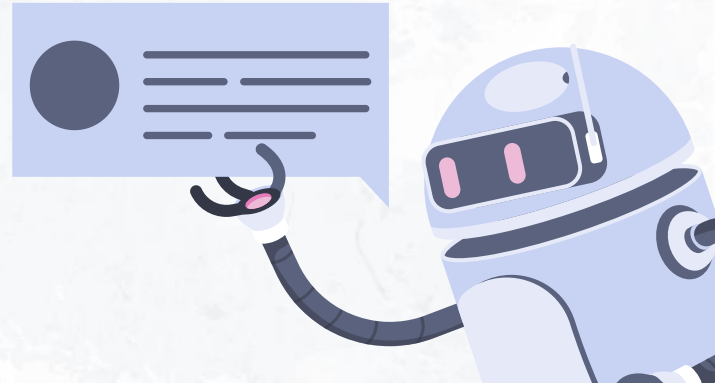
To use the classic interface, [click here](#)

Binary Executing from Temp Directory	2023-05-09 10:23:51	DESKTOP-SRHRTR0	T1204	New	<input type="checkbox"/>
--------------------------------------	---------------------	-----------------	-------	-----	--------------------------

Windows | Type here to search | 36°C Nhiều mây | 3:47 PM 5/17/2023

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 \longrightarrow

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

 andysmith

 v1.1.0









 2dc2572

Compare ▾

v1.1.0 Latest

- 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







The screenshot displays the Registry Spy application window. The title bar reads "Registry Spy". The menu bar includes "File", "Find", "View", and "Help". Below the menu bar is a toolbar with icons for file operations and search. The main window shows the path "SYSTEM\ControlSet001\Control\ComputerName\ComputerName". A table lists registry keys with columns for "Key", "Subkeys", "Modified", "Name", "Type", and "Data". The "ComputerName" key is selected, showing its type as "REG_SZ" and data as "M57-CHARLIE". At the bottom, a metadata section shows the path, type, hive name, and root name.

Key	Subkeys	Modified	Name	Type	Data
SYSTEM (C:/Users/acer/Desktop/NT334_...	7	2009-11-12 11:07:50	ComputerName	REG_SZ	M57-CHARLIE
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			




















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.xsp3_sp3_gdr.090804-1435
 CurrentType	REG_SZ	Multiprocessor Free
 CSDVersion	REG_SZ	Service Pack 3
 SystemRoot	REG_SZ	C:\WINDOWS
 SourcePath	REG_SZ	D:\J386
 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 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 - andysmith/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

