UNIVERSITY OF INFORMATION TECHNOLOGY
FACULTY OF COMPUTER NETWORK AND COMMUNICATION

REPORT
Subject: Digital Forensics
Semester II (2022 – 2023)

REGISTRY SPY AND OPEN EDR

Student 1: Võ Anh Kiệt - 20520605

Student 2: Nguyễn Bùi Kim Ngân - 20520648

Student 3: Nguyễn Bình Thục Trâm - 20520815

Class: NT334.N21.ANTN

University of Information Technology

Lecturer: Nguyễn Tấn Cầm

Hồ Chí Minh City, June 2023

UNIVERSITY OF INFORMATION TECHNOLOGY
FACULTY OF COMPUTER NETWORK AND COMMUNICATION

REPORT
Subject: Digital Forensics
Semester II (2022 – 2023)

REGISTRY SPY AND OPEN EDR

Student 1: Võ Anh Kiệt - 20520605

Student 2: Nguyễn Bùi Kim Ngân - 20520648

Student 3: Nguyễn Bình Thục Trâm - 20520815

Class: NT334.N21.ANTN

University of Information Technology

Lecturer: Nguyễn Tấn Cầm

Hồ Chí Minh City, June 2023

Acknowledgement

To begin, we would like to thank our advisor, PhD Nguyễn Tấn Cầm, for his direction and consistent monitoring, as well as for providing important project information and for their help in finishing the research.

My gratitude and appreciation also extend to our colleagues and lecturers who assisted us in the development of the project, as well as to those who have volunteered their time and skills to assist us.

Võ Anh Kiệt – 20520605 – ANTN.2020

Nguyễn Bùi Kim Ngân – 20520648 – ANTN.2020

Nguyễn Bình Thục Trâm – 20520815 – ANTN.2020

Contents

Part 1: Introduction

1.1. Overview Registry Spy

The management and organization of information have become crucial in today's digital environment, where enormous amounts of data are generated and saved. Utilizing registry technologies, which act as centralized repositories for storing and accessing critical information, is a key component of data management. These technologies are essential in a number of industries, including logistics, finance, and healthcare.

The Registry Tool Analysis is a comprehensive analysis of the features, advantages, and difficulties related to registry tools. An thorough review of these tools, their importance, and the effects they have on enterprises and organizations are all part of this in-depth report's goal.

The examination will delve into the fundamental ideas that underlie registry tools, illuminating how they support the effective management of data through hierarchical hierarchies and defined formats. Registry technologies provide unmatched simplicity and accessibility by collecting, organizing, and preserving crucial information in a single location, expediting crucial business operations.

The report will also examine the various industrial applications of registry tools. It will dig into the healthcare industry, where patient registries make it possible to gather and analyze data for epidemiological studies, medical research, and individualized patient care. Additionally, financial institutions use registry technologies extensively for customer relationship management, compliance monitoring, and fraud detection, offering an integrated method of managing client data.

Although registry technologies provide many advantages, the examination will also cover the difficulties that businesses encounter in setting up and maintaining them. This covers things like data security, privacy issues, scalability, and interoperability, which call for careful attention to guarantee registry systems perform at their best and maintain their integrity.

In the end, the goal of this Registry Tool Analysis is to provide businesses, decision-makers, and professionals with a thorough grasp of the function and potential of registry tools in contemporary data management. This paper will be an invaluable resource for anyone looking to harness the potential of registry technologies to improve their data management processes and boost operational efficiency by examining their capabilities, advantages, and limitations.

1.2. Overview EDR

The dynamic threat environment in the field of cybersecurity necessitates new strategies to safeguard digital assets. EDR, or endpoint detection and response, has become an essential part of the protection against sophisticated cyberthreats. Organizations can identify, look into, and react to dangerous actions at the endpoint level thanks to EDR technologies.

This piece tries to offer a comprehensive analysis of EDR, its features, and the importance it bears in protecting contemporary digital environments. The convergence of endpoint security, threat detection, and incident response will be the subject of this report, which will clarify the crucial part that EDR plays in reducing cyber risks.

The investigation will go into the underlying ideas of EDR, examining how it uses cutting-edge technologies like behavioral analytics, machine learning, and artificial intelligence to spot malware, flag suspicious activity, and react to security issues. EDR solutions give security teams real-time endpoint visibility, allowing them to proactively fight against sophisticated threats like fileless assaults, zero-day exploits, and advanced persistent threats (APTs).

The paper will also go through the primary attributes and functions of EDR solutions, such as continuous monitoring, forensic analysis, integration of threat intelligence, and automated reaction. EDR gives companies the ability to quickly recognize and neutralize threats, reducing the potential effect of cyber disasters. It does this by supplying granular visibility into endpoint actions and developing thorough defense systems.

The analysis will include the difficulties in installing and managing EDR solutions in addition to the advantages. This includes things like system complexity, resource needs, false positives, and making sure the system is compatible with the current security architecture. To make the most of their EDR initiatives, organizations must carefully assess these factors.

In the end, the purpose of this EDR research is to give decision-makers, security experts, and businesses a thorough knowledge of the value and potential of EDR in the face of changing cyberthreats. This research will be an invaluable resource for anyone looking to improve their cybersecurity posture and secure their digital assets through the deployment of effective EDR solutions by examining its functions, advantages, and problems.

1.3. Problem Statement

The potential of malware penetration is a huge concern in today's linked society, as digital gadgets are omnipresent and play a critical part in both our personal and professional life. Malicious software, also referred to as malware, is constantly evolving and adapting, coming up with new and creative ways to get past the security measures put in place by devices like computers, smartphones, tablets, and Internet of Things (IoT) devices.

The issue is that malware is becoming more sophisticated and diverse all the time. It may infect devices using a variety of attack routes, including phishing emails, compromised websites, software flaws, social engineering tricks, and illegal app downloads. Malware can cause chaos once it has gained access to a device by stealing confidential data, jeopardizing user privacy, engaging in unwanted actions, and even making the device unusable.

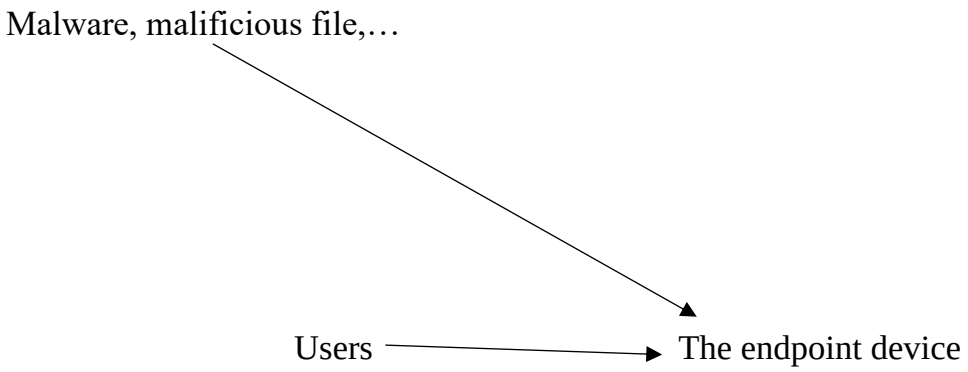
The effects of malware infestation are extensive and significant. Financial loss, identity theft, data breaches, system outages, and reputational harm are risks that both individuals and corporations must contend with. In addition, as technology develops and the Internet of Things connects more gadgets, there is an urgent

need to be concerned about the possibility of broad malware outbreaks and their potential cascade repercussions.

Malware infiltration must be addressed using a multifaceted strategy that includes strong cybersecurity controls, user education, proactive threat detection, and efficient incident response. Individuals, businesses, and security experts must maintain vigilance, regularly upgrade their defenses, and use security technologies that can identify and counter new malware threats.

The issue also gets more complicated as the lines between personal and professional gadget usage blur. The difficulty of securing a wide variety of devices, including employee-owned devices (Bring Your Own Device, or BYOD), is one that businesses must address because it increases the risks and potential weaknesses of corporate networks.

In conclusion, the issue of malware gaining access to devices is a persistent and constantly changing difficulty in today's digital environment. In order to protect themselves from malware infection and its effects on devices, people, companies, and the security community as a whole must always be on watch, react to new threats, and put strong security measures in place.



1.4. Scope

Deploy the EDR

Deploy the Registry Spy

Analysis the endpoint device

Detect malware

1.5. Objective

Using the EDR sponsor by OpenEDR to analysis the machine and detect malware.

Using the Registry spy to detect the DAT file

Part 2: Background

2.1. 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.

Features include:

- Windows, macOS, and Linux support
- Fast, on-the-fly parsing means no upfront overhead
- Open multiple hives at a time
- Searching
- Hex viewer
- Modification timestamps

2.2. EDR – 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.

Capability:

- Visibility and coverage: Open EDR solutions provide visibility into all activity and can cover both physical and virtualized environments.
- Detection: It provides an effective solution on detecting potential threats.
- Response: It reacts quickly and helps you contain and remediate incidents.
- Management and reporting: It is easy to manage and provide comprehensive reports that can help you improve your security posture.

There are many benefits of using Open EDR solutions, including:

- Improved Detection: It can help organizations to detect malicious activity that would otherwise go unnoticed. By collecting data from multiple sources and applying advanced analytics, Endpoint detection response software can provide visibility into suspicious activity and help security teams to immediately identify potential threats.
- Faster Investigation and Response: With all the data collected by an EDR solution in one place, security teams can quickly investigate incidents and take appropriate action to mitigate the threat. In addition, it often includes features such as automatic file quarantine that can help to contain an incident while it is being investigated.
- Damage from Attacks: By identifying attacks early and taking immediate action to block or contain them, EDR solutions can help organizations to reduce the damage caused by malicious actors. This can help organizations to minimize the impact of an attack and reduce the amount of time needed for recovery.
- Improved Compliance: It can also help organizations to meet compliance requirements, as many regulations require organizations to have effective security measures in place to protect data and systems. By deploying an EDR solution, organizations can demonstrate that they are taking appropriate steps to protect their systems from malicious activity.

Part 3: Requirement and Installation

3.1. Requirement

3.1.1. Registry Spy

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

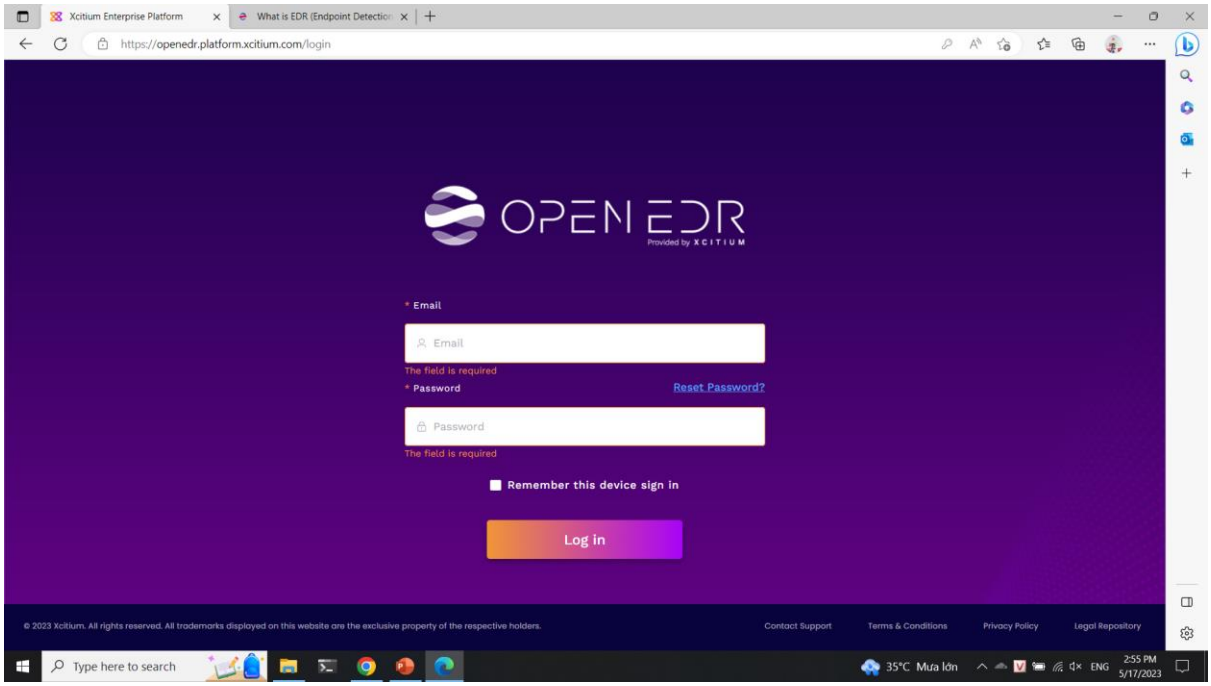
Operating System	Architecture	Compiler	
Windows 10 (1809 or later)	x86_64	MSVC 2022, MSVC 2019, MinGW 11.2	
Windows 11	x86_64	MSVC 2022, MSVC 2019, MinGW 11.2	
Windows on ARM	arm64	MSVC 2019/2022	Technology Preview

3.1.2. OpenEDR

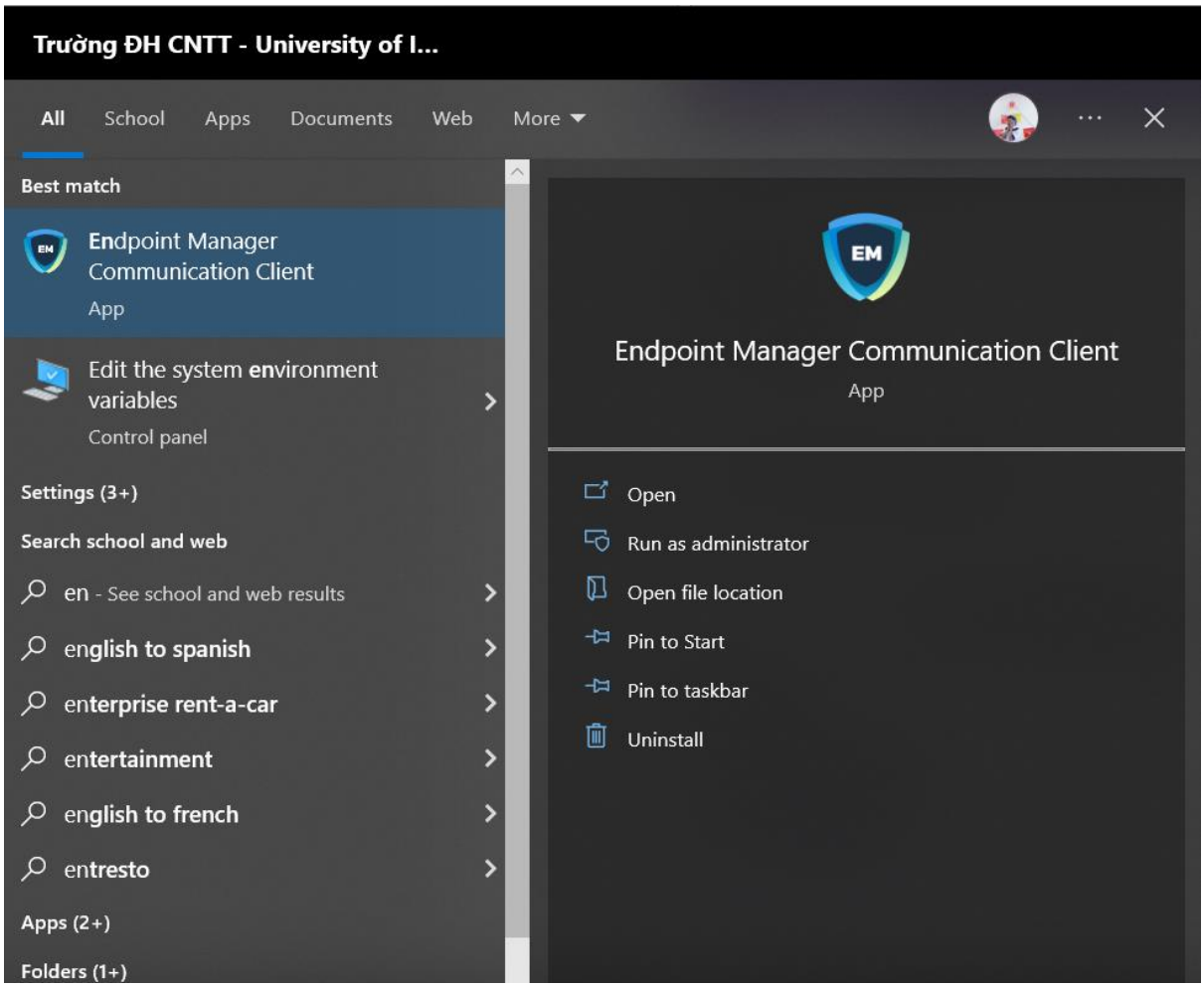
This system require:

- The main system to get the annoucement from agent
- The machine installed agent

The main system:



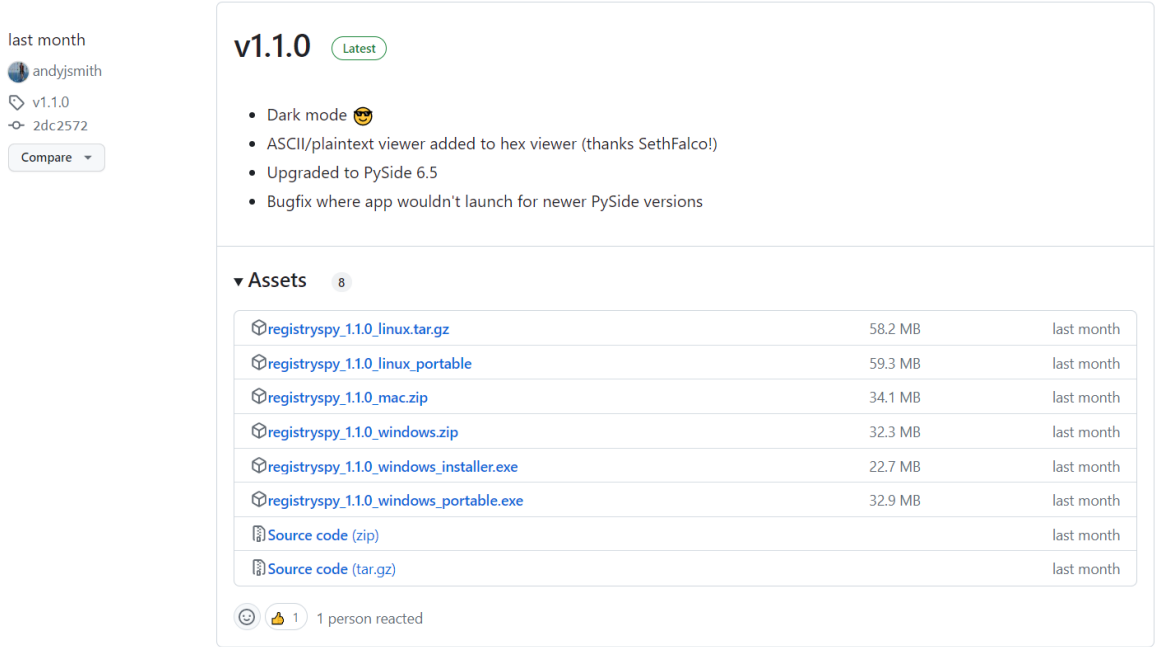
The machine with agent:



3.2. Installation

3.2.1. Registry spy

The newest version 1.1.0:



There are 2 method to install it:

Install with pip:

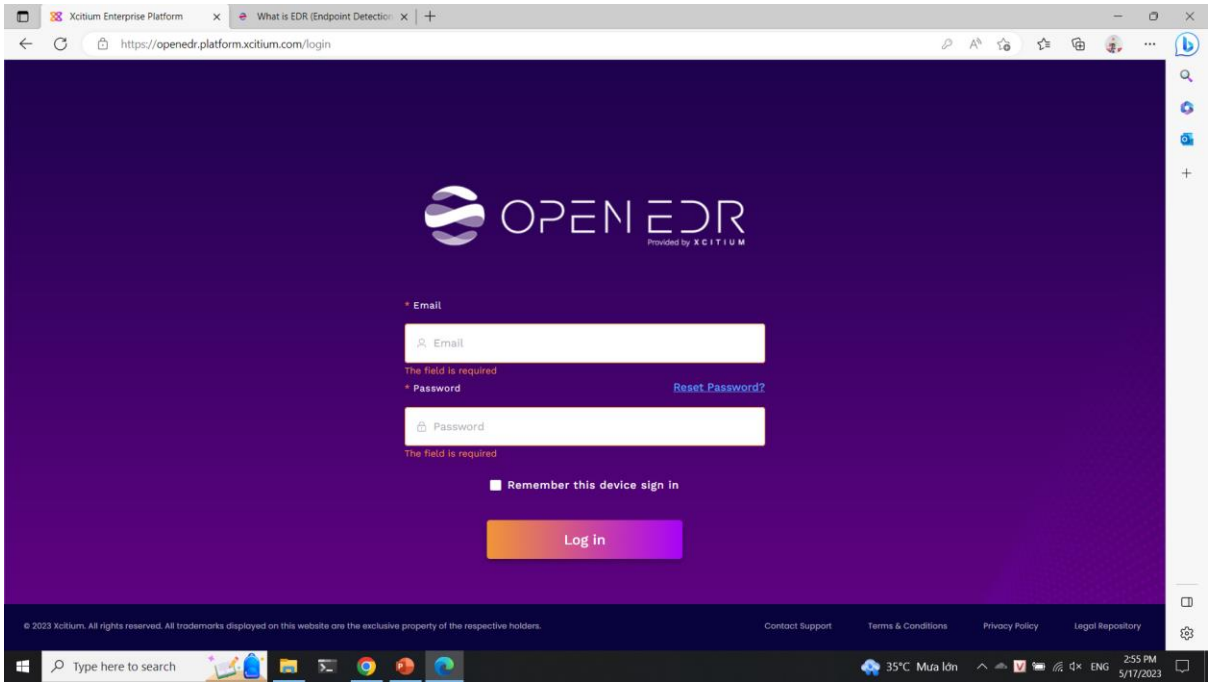
Pip → pip install registryspy → registryspy

Install manually:

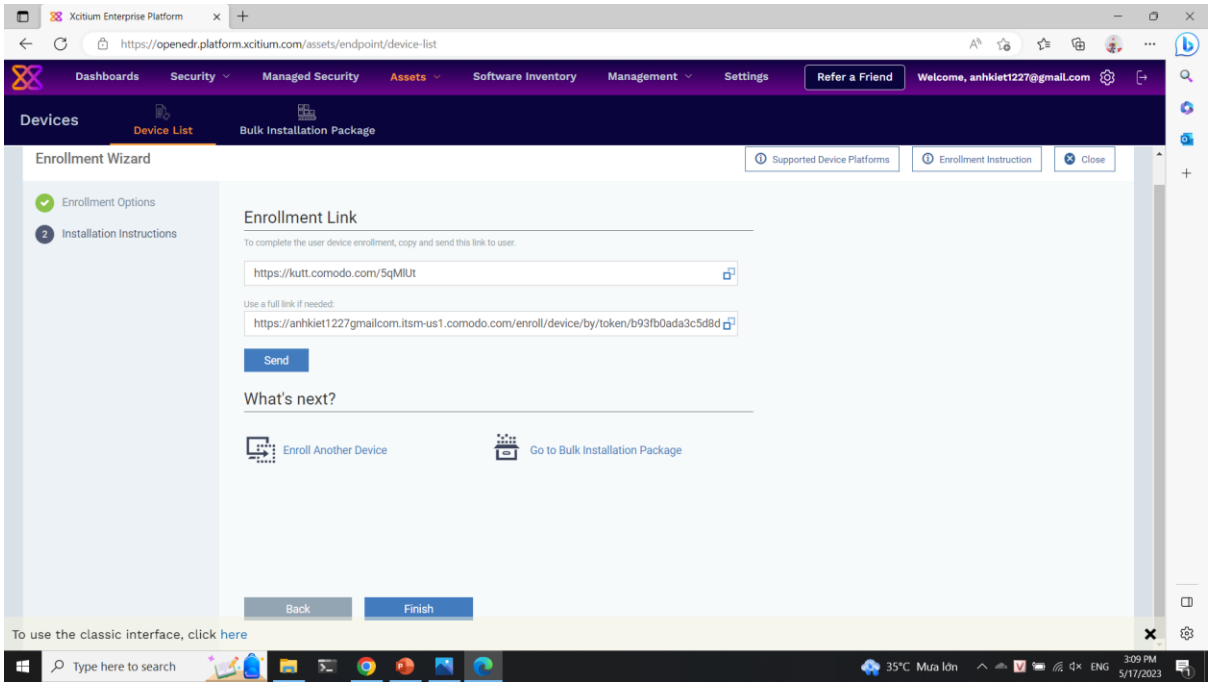
Clone the reposity/standalone → pip install –r requirements.txt → python setup.py install → registryspy

3.2.2. OpenEDR

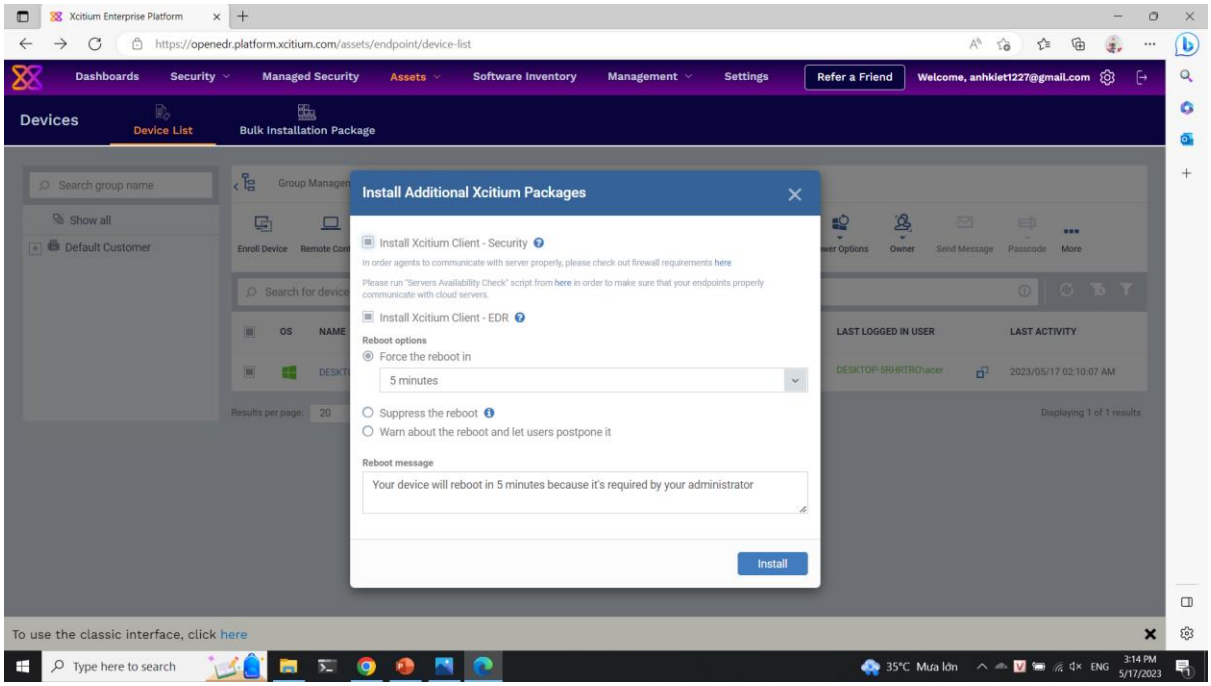
Register and install the main system:



Install the agent to the machine:



Install the packages:


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
Search group name
Show all
Default Customer
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
LAST LOGGED IN USER
LAST ACTIVITY
DESKTOP-5RHRTRO\acer
2023/05/17 02:10:07 AM
Displaying 1 of 1 results
To use the classic interface, click here
Type here to search
35°C Mưa lớn
ENG
3:14 PM
5/17/2023

Part 4: Implementation

4.1. Registry Spy

Check the information of the machine:

Computer name:

Name	Type	Data
ab ComputerName	REG_SZ	M57-CHARLIE

Firewall:

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

List application in Firewall list;

Name	Type	Data
ab %windir%\Network Diagn...	REG_SZ	%windir%\Network Diagnostic\xpnetdiag.exe:*:Enabled:@xpsp3res.dll,-20000
ab %windir%\system32\sess...	REG_SZ	%windir%\system32\sessmgr.exe:*:enabled:@xpsp2res.dll,-22019

Operation System:

Name	Type	Data
ab SubVersionNumber	REG_SZ	
ab CurrentBuild	REG_SZ	1.511.1 () (Obsolete data - do not use)
123 InstallDate	REG_DWORD	0x4af76f9b (1257729947)
ab ProductName	REG_SZ	Microsoft Windows XP
ab RegDone	REG_SZ	
ab RegisteredOrganization	REG_SZ	M57.biz
ab RegisteredOwner	REG_SZ	Charlie
ab SoftwareType	REG_SZ	SYSTEM
ab CurrentVersion	REG_SZ	5.1
ab CurrentBuildNumber	REG_SZ	2600
ab BuildLab	REG_SZ	2600.xpsp_sp3_gdr.090804-1435
ab CurrentType	REG_SZ	Multiprocessor Free
ab CSDVersion	REG_SZ	Service Pack 3
ab SystemRoot	REG_SZ	C:\WINDOWS
ab SourcePath	REG_SZ	D:\I386
ab PathName	REG_SZ	C:\WINDOWS
ab ProductId	REG_SZ	76487-027-5250835-22765
010 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...
010 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...

Enviroment:

Name	Type	Data
ab ComSpec	REG_EXPAND_SZ	%SystemRoot%\system32\cmd.exe
ab Path	REG_EXPAND_SZ	%SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\Wbem
ab windir	REG_EXPAND_SZ	%SystemRoot%
ab FP_NO_HOST_CHECK	REG_SZ	NO
ab OS	REG_SZ	Windows_NT
ab PROCESSOR_ARCHITECTU...	REG_SZ	x86
ab PROCESSOR_LEVEL	REG_SZ	15
ab PROCESSOR_IDENTIFIER	REG_SZ	x86 Family 15 Model 2 Stepping 9, GenuineIntel
ab PROCESSOR_REVISION	REG_SZ	0209
ab NUMBER_OF_PROCESSORS	REG_SZ	2
ab PATHEXT	REG_SZ	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
ab TEMP	REG_EXPAND_SZ	%SystemRoot%\TEMP
ab TMP	REG_EXPAND_SZ	%SystemRoot%\TEMP

Mount Device:

Name	Type	Data
\??\Volume{b32e3e4a-cc85-11de-9628-806d6172696f}	REG_BINARY	a9 ea a9 ea 00 7e 00 00 00 00 00 00
\DosDevices\C:	REG_BINARY	a9 ea a9 ea 00 7e 00 00 00 00 00 00
\??\Volume{ef9791c2-cc88-11de-a014-806d6172696f}	REG_BINARY	5c 00 3f 00 3f 00 5c 00 46 00 44 00 43 00 23 00 47 00 45 00 4e 00 45 00 52 00 49 00 43 00 5f 00 46 00 4c 00 4f 00 50 00...
\??\Volume{ef9791c3-cc88-11de-a014-806d6172696f}	REG_BINARY	5c 00 3f 00 3f 00 5c 00 49 00 44 00 45 00 23 00 43 00 64 00 52 00 6f 00 6d 00 4c 00 49 00 54 00 45 00 4f 00 4e 00 5f 00 ...
\??\Volume{ef9791c4-cc88-11de-a014-806d6172696f}	REG_BINARY	5c 00 3f 00 3f 00 5c 00 49 00 44 00 45 00 23 00 43 00 64 00 52 00 6f 00 6d 00 53 00 41 00 4d 00 53 00 55 00 4e 00 47 0...
\DosDevices\A:	REG_BINARY	5c 00 3f 00 3f 00 5c 00 46 00 44 00 43 00 23 00 47 00 45 00 4e 00 45 00 52 00 49 00 43 00 5f 00 46 00 4c 00 4f 00 50 00...
\DosDevices\D:	REG_BINARY	5c 00 3f 00 3f 00 5c 00 49 00 44 00 45 00 23 00 43 00 64 00 52 00 6f 00 6d 00 4c 00 49 00 54 00 45 00 4f 00 4e 00 5f 00 ...
\DosDevices\E:	REG_BINARY	5c 00 3f 00 3f 00 5c 00 49 00 44 00 45 00 23 00 43 00 64 00 52 00 6f 00 6d 00 53 00 41 00 4d 00 53 00 55 00 4e 00 47 0...

Time Zone:

Name	Type	Data
123 Bias	REG_DWORD	0x000001e0 (480)
ab StandardName	REG_SZ	Pacific Standard Time
123 StandardBias	REG_DWORD	0x00000000 (0)
StandardStart	REG_BINARY	00 00 0b 00 01 00 02 00 00 00 00 00 00 00 00 00
ab DaylightName	REG_SZ	Pacific Daylight Time
123 DaylightBias	REG_DWORD	0xffffffc4 (4294967236)
DaylightStart	REG_BINARY	00 00 03 00 02 00 02 00 00 00 00 00 00 00 00 00
123 ActiveTimeBias	REG_DWORD	0x000001e0 (480)

Network card:

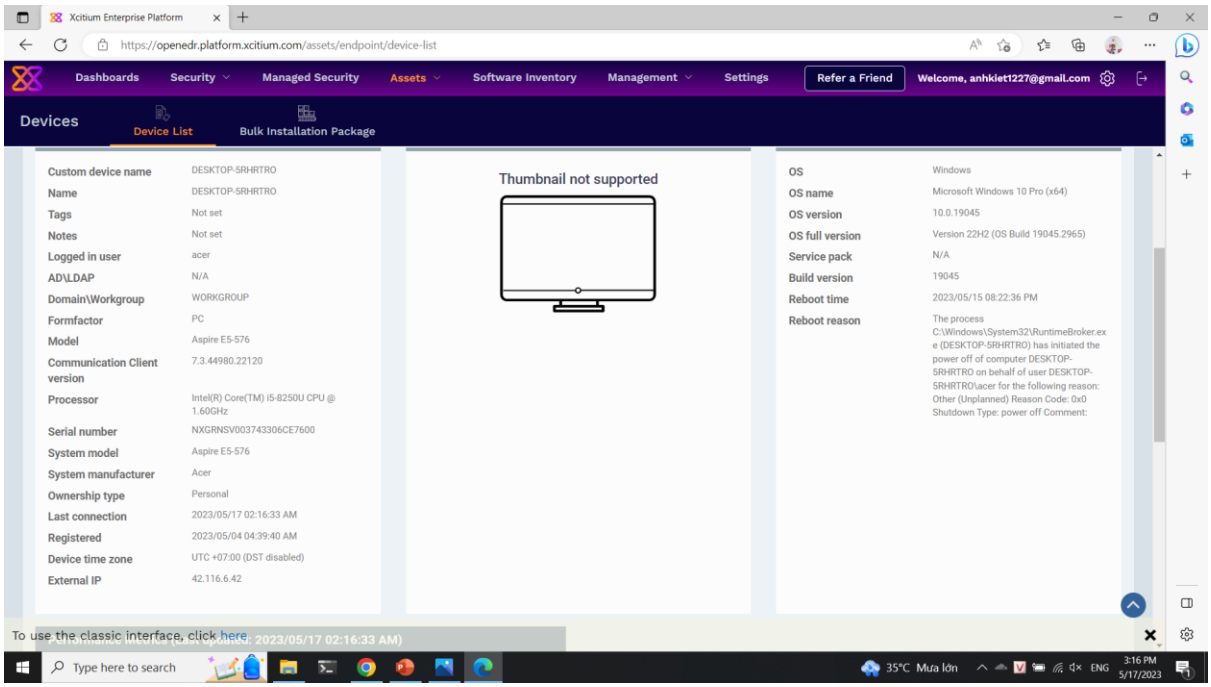
Name	Type	Data
ab ServiceName	REG_SZ	{B15FB27D-C44F-4540-AB9C-7C789450051B}
ab Description	REG_SZ	Intel(R) PRO/1000 MT Network Connection

Memory management:

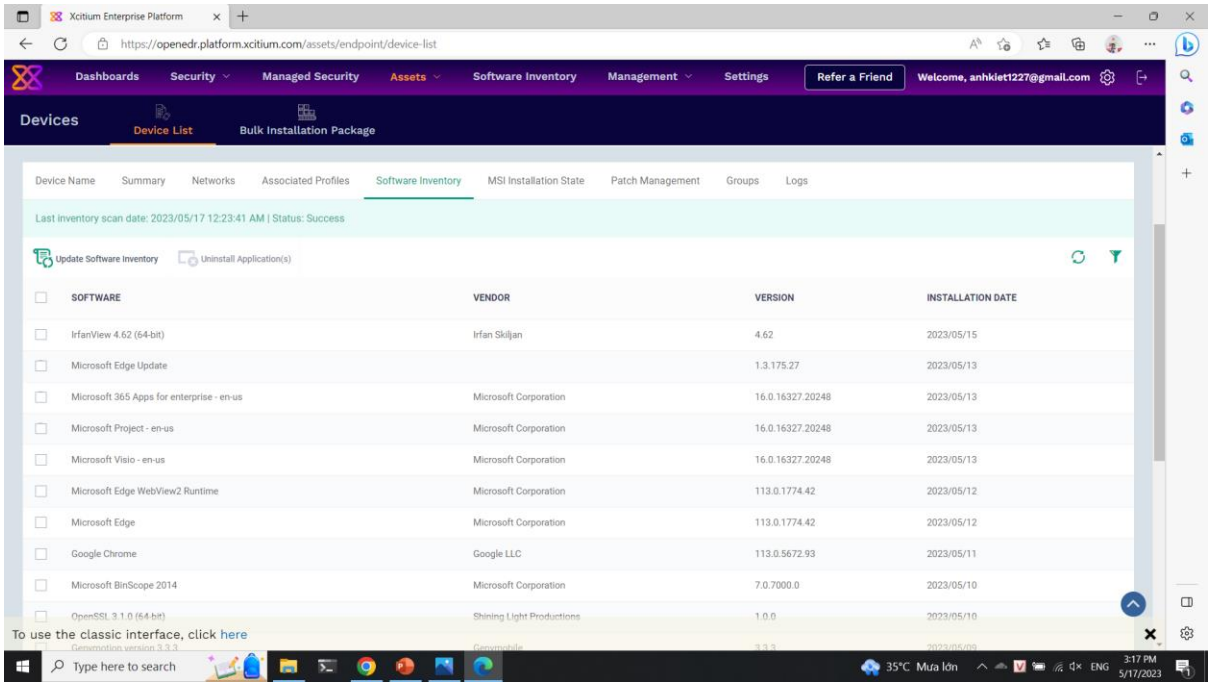
Name	Type	Data
ClearPageFileAtShutdown	REG_DWORD	0x00000000 (0)
DisablePagingExecutive	REG_DWORD	0x00000000 (0)
LargeSystemCache	REG_DWORD	0x00000000 (0)
NonPagedPoolQuota	REG_DWORD	0x00000000 (0)
NonPagedPoolSize	REG_DWORD	0x00000000 (0)
PagedPoolQuota	REG_DWORD	0x00000000 (0)
PagedPoolSize	REG_DWORD	0x00000000 (0)
SecondLevelDataCache	REG_DWORD	0x00000000 (0)
SystemPages	REG_DWORD	0x00033000 (208896)
PagingFiles	REG_MULTI_SZ	C:\pagefile.sys 2046 4092
PhysicalAddressExtension	REG_DWORD	0x00000000 (0)
SessionViewSize	REG_DWORD	0x00000030 (48)
SessionPoolSize	REG_DWORD	0x00000004 (4)

4.2. OpenEDR

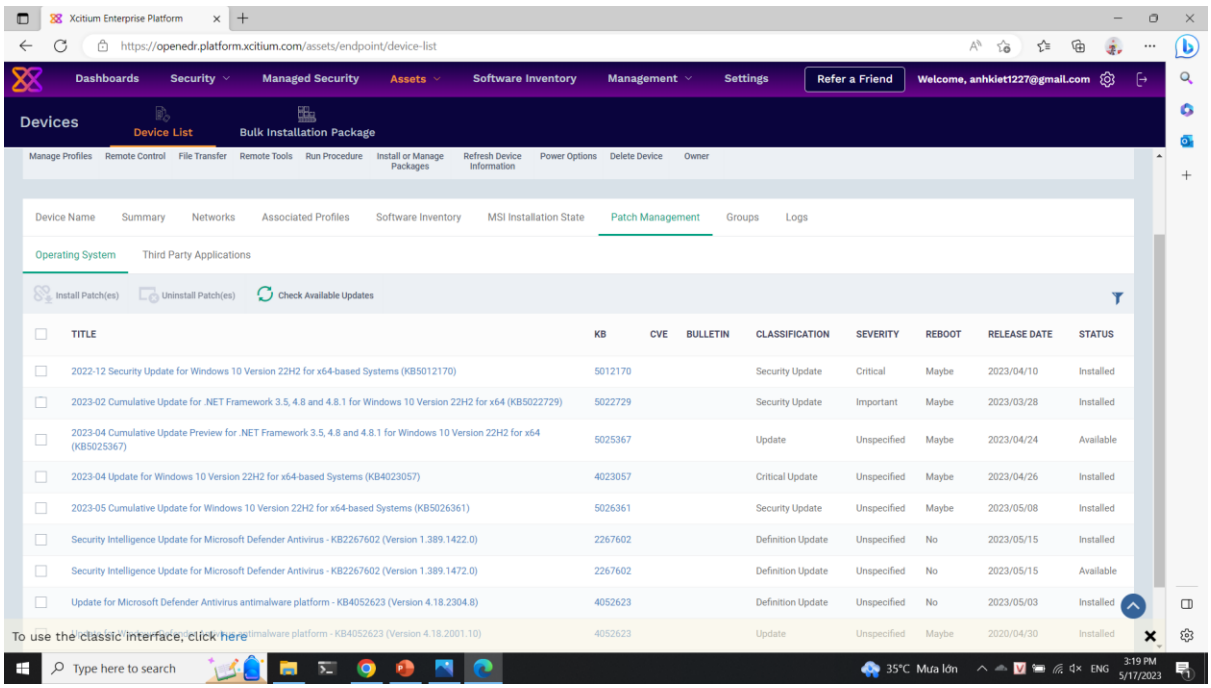
Scan the information of the endpoint:



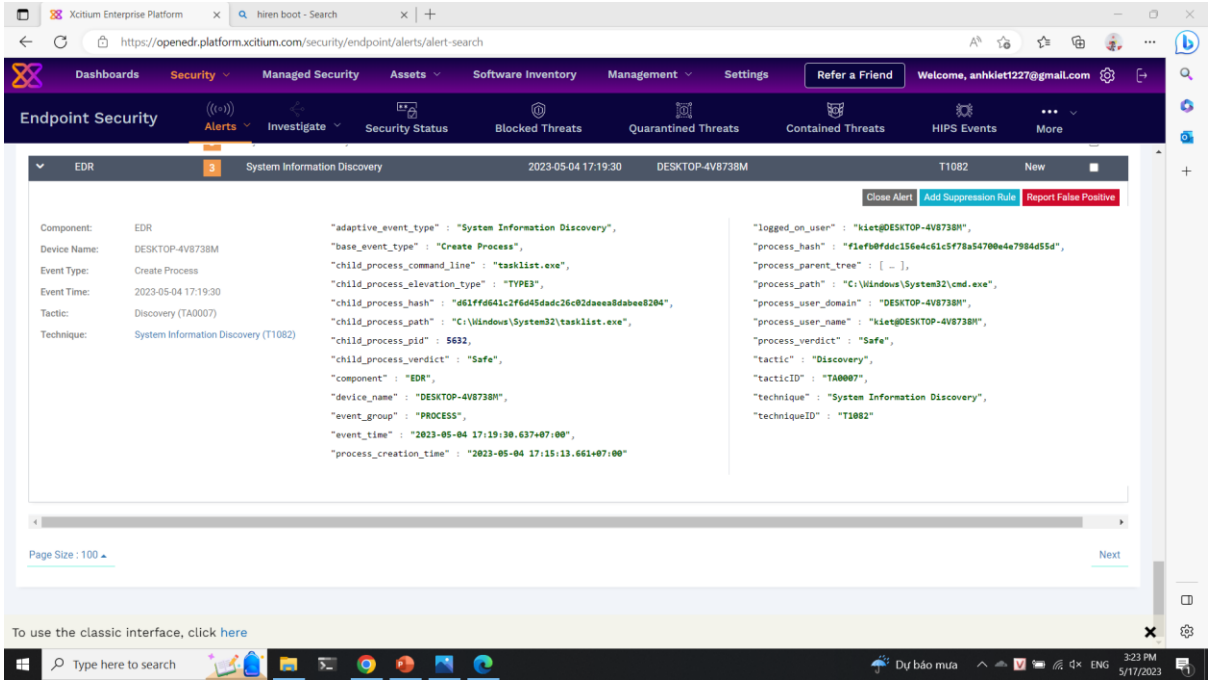
Scan the software of the endpoint:



Scan the patch of the endpoint:



Detect the process of the endpoint:



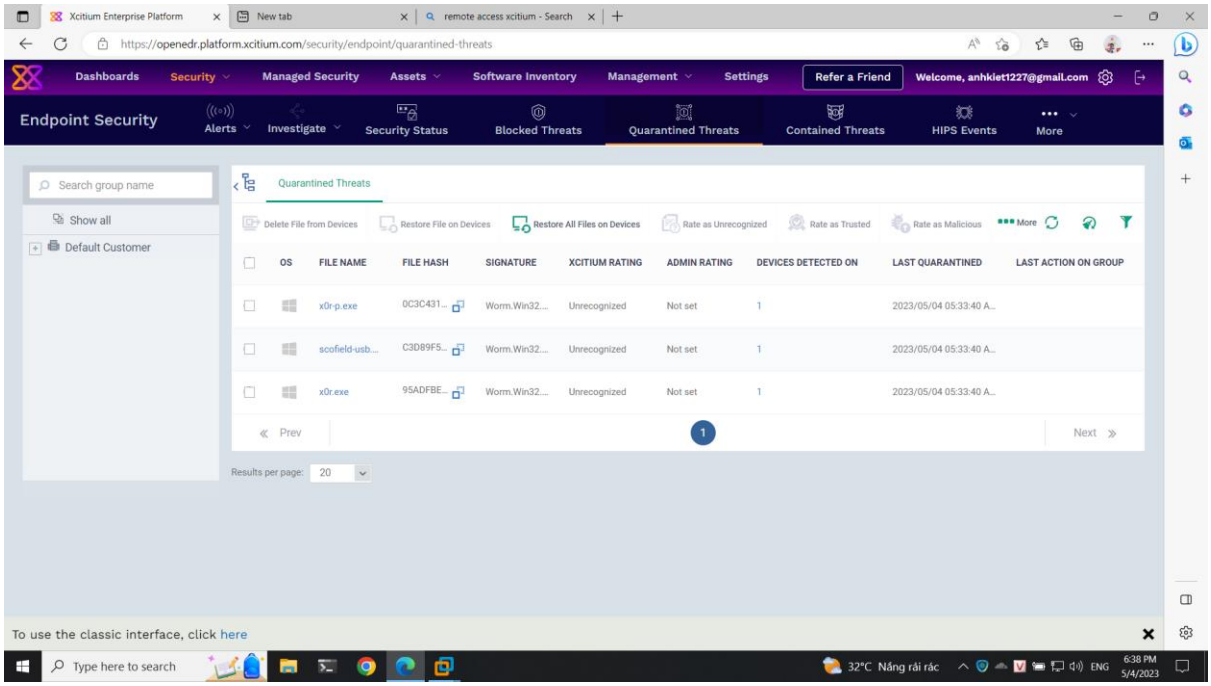
Process of detect and respone the malware of OpenEDR:

Detect the suspicious file → Quarantine → Detect → Delete → Find the same file again → Delete automaticly → Annoucement

>	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

Quarantine file:

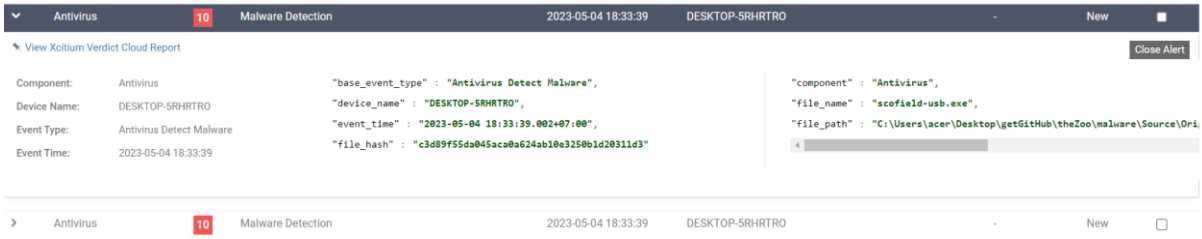
Quarantine room:



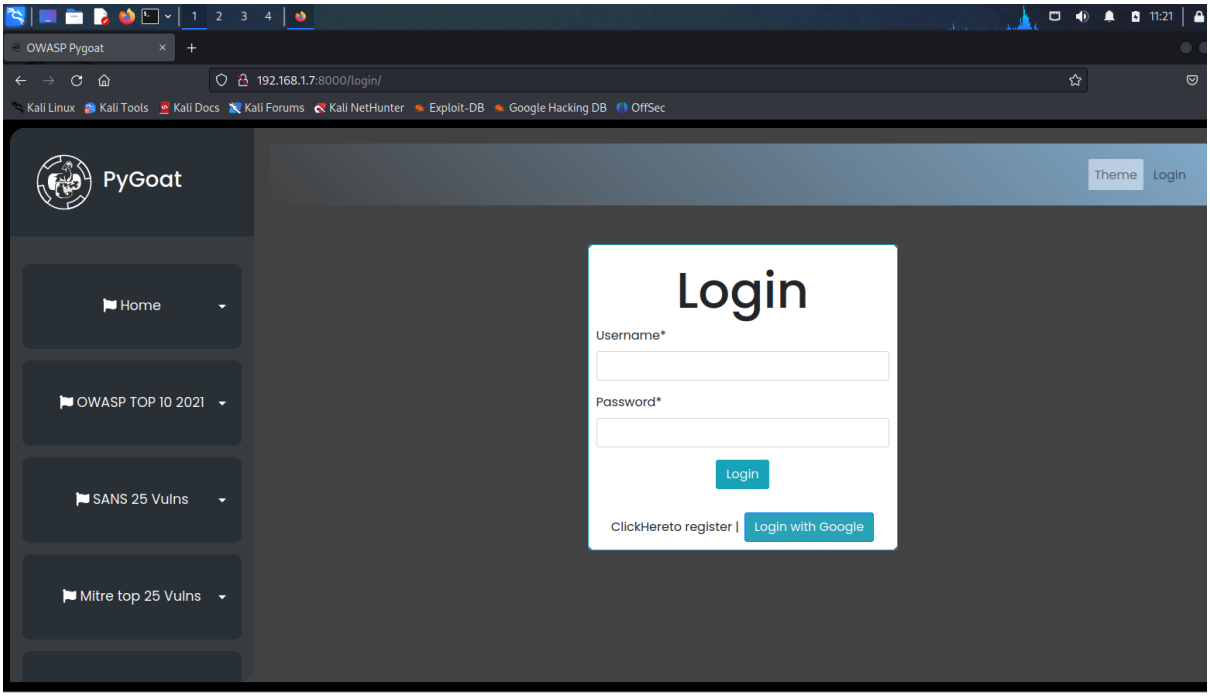
Detect malware:

Delete malware:

Delete malware automaticly (2nd times):



Top 10 OWASP:



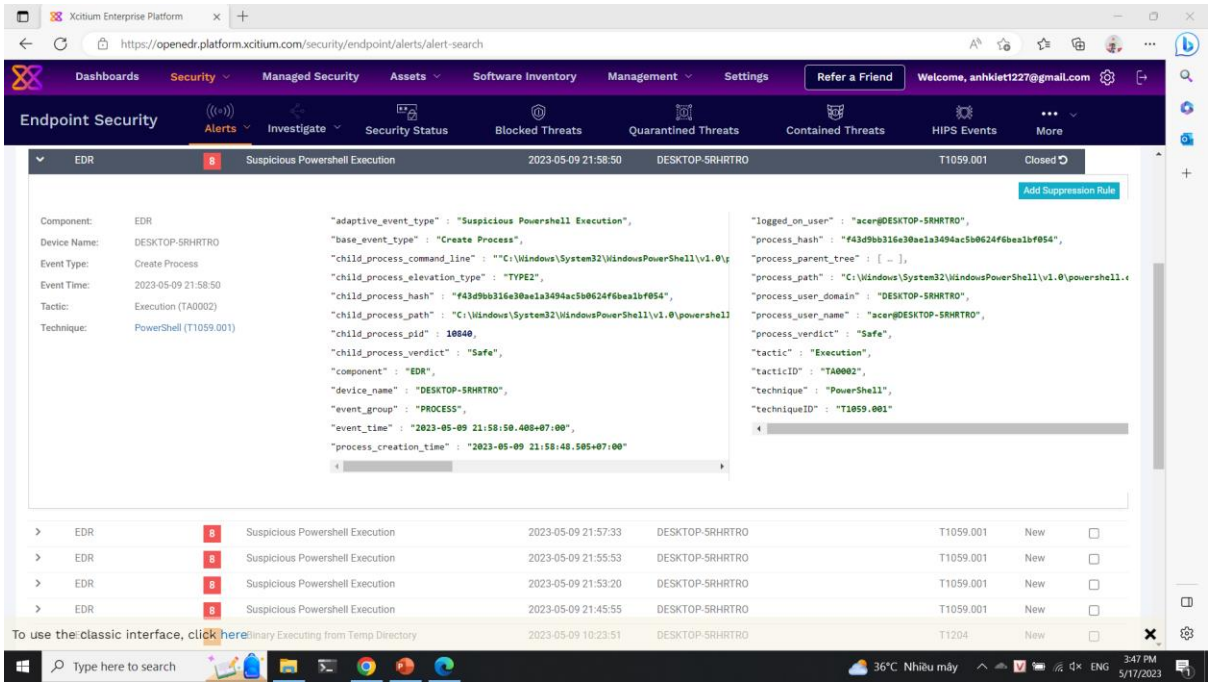
Pygoat - No announcement on OpenEDR:

```
None
None
None
None
admin
'or 1=1--
SELECT * FROM introduction_sql_lab_table WHERE id='admin'AND password='''or 1=1--'
admin
```

Webgoat - No announcement on OpenEDR:

```
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)
```

Weakness – detect and ban wrong process:


Xcitium Enterprise Platform
https://openedr.platform.xcitium.com/security/endpoint/alerts/alert-search
Dashboards
Security
Managed Security
Assets
Software Inventory
Management
Settings
Refer a Friend
Welcome, anhkiet1227@gmail.com
Endpoint Security
Alerts
Investigate
Security Status
Blocked Threats
Quarantined Threats
Contained Threats
HIPS Events
More
EDR
Suspicious Powershell Execution
2023-05-09 21:58:50
DESKTOP-5RHRTRO
T1059.001
Closed
Add Suppression Rule
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.
"process_user_domain" : "DESKTOP-5RHRTRO",
"process_user_name" : "acer@DESKTOP-5RHRTRO",
"process_verdict" : "Safe",
"tactic" : "Execution",
"tacticID" : "TA0002",
"technique" : "PowerShell",
"techniqueID" : "T1059.001"
EDR Suspicious Powershell Execution 2023-05-09 21:57:33 DESKTOP-5RHRTRO T1059.001 New
EDR Suspicious Powershell Execution 2023-05-09 21:55:53 DESKTOP-5RHRTRO T1059.001 New
EDR Suspicious Powershell Execution 2023-05-09 21:53:20 DESKTOP-5RHRTRO T1059.001 New
EDR Suspicious Powershell Execution 2023-05-09 21:45:55 DESKTOP-5RHRTRO T1059.001 New
To use the classic interface, click here
Binary Executing from Temp Directory 2023-05-09 10:23:51 DESKTOP-5RHRTRO T1204 New
Type here to search
36°C Nhiều mây
ENG
3:47 PM
5/17/2023

Part 5: Conclusion and Future Work

5.1. Conclusion

In conclusion, the registry tool and Endpoint Detection and Response (EDR) play vital roles in enhancing the security and overall management of computer systems. The registry, as a core component of the operation system, acts as a centralized database that stores essential configuration settings and options. By utilizing the registry tool effectively, administrators and users can modify settings, troubleshoot issues, and optimize system performance.

EDR, on the other hand, provides advanced threat detection, prevention, and response capabilities to safeguard endpoints against malicious activities. It continuously monitors and analyzes system events, network traffic, and user behavior to identify and respond to potential threats promptly. EDR solutions offer real-time visibility into endpoint activities, enabling security teams to detect and mitigate sophisticated attacks, such as fileless malware, advanced persistent threats, and zero-day exploits.

When used in conjunction, the registry tool and EDR form a robust defense mechanism against cyber threats. The registry tool allows for fine-grained control over system settings, ensuring secure configurations that align with organizational security policies. EDR solutions provide additional layers of defense by actively monitoring the system, detecting anomalies, and responding swiftly to potential threats, minimizing the risk of data breaches, system compromise, and unauthorized access.

Moreover, the integration of the registry tool and EDR enhances incident response capabilities. In the event of a security incident, the registry tool can be leveraged to analyze system changes, track suspicious registry modifications, and restore critical settings. EDR solutions, with their comprehensive visibility and incident investigation capabilities, provide valuable insights into the attack vector, its impact, and potential lateral movement within the network. This information empowers security teams to conduct thorough forensic

investigations, facilitate timely incident response, and implement appropriate remediation measures.

In conclusion, the effective utilization of the registry tool and EDR strengthens the security posture of computer systems by enabling secure configurations, proactive threat detection, and efficient incident response. As the threat landscape continues to evolve, organizations must embrace these tools, alongside other security measures, to safeguard their digital assets and maintain a resilient cybersecurity posture. By prioritizing the implementation and integration of the registry tool and EDR, organizations can enhance their ability to mitigate risks, detect and respond to threats, and protect sensitive information, ultimately safeguarding the integrity and availability of their systems.

5.2. Future work

In the future, there are several areas that can be explored and expanded upon regarding the registry tool and Endpoint Detection and Response (EDR) to further enhance their effectiveness and impact on computer system security. Here are some potential avenues for future work:

- Advanced Registry Analysis
- Registry Integrity Monitoring
- Enhanced Registry Remediation
- Integration with Threat Intelligence
- Registry Auditing and Compliance
- Cross-Platform Support

In conclusion, the future work of the project surrounding the registry tool and EDR presents exciting opportunities for further research and development. By focusing on advanced analysis techniques, integrity monitoring, automated remediation, threat intelligence integration, auditing, compliance, and cross-platform support, we can continue to enhance the security posture of computer systems, detect and respond to emerging threats effectively, and ensure the resilience and protection of critical assets in the face of evolving cyber risks.

Reference

OpenEDR: What is EDR (Endpoint Detection & Response)? Open source EDR® (openedr.com)

Registry Spy: GitHub - andyjsmith/Registry-Spy: Cross-platform registry browser for raw Windows registry files