Project Summary: Credential Extraction Simulation and Detection

Introduction

The project focused on simulating credential extraction attacks and enhancing detection mechanisms using Sysmon and Wazuh. The primary goal was to simulate real-world attack scenarios, ensure comprehensive event logging, and create custom detection rules to improve alert accuracy.

Objectives

1. Simulate credential extraction attacks using Mimikatz.
2. Ensure Sysmon effectively captures events related to these attacks.
3. Develop custom Wazuh rules to detect and alert on specific security events.
4. Enhance detection accuracy by utilizing detailed event fields.

Execution

Simulating Credential Extraction Attacks

- **Tool Used**: Mimikatz
- **Purpose**: To simulate credential extraction attacks typically used by malicious actors.
- **Process**: Executed Mimikatz in a controlled environment to extract credentials and generate security events.

Event Logging with Sysmon

- **Tool Used**: Sysmon (System Monitor)
- **Purpose**: To capture detailed events generated by the execution of Mimikatz.
- **Configuration**: Customized Sysmon configuration to log specific events related to credential extraction, ensuring comprehensive event capture.

Custom Detection Rules with Wazuh

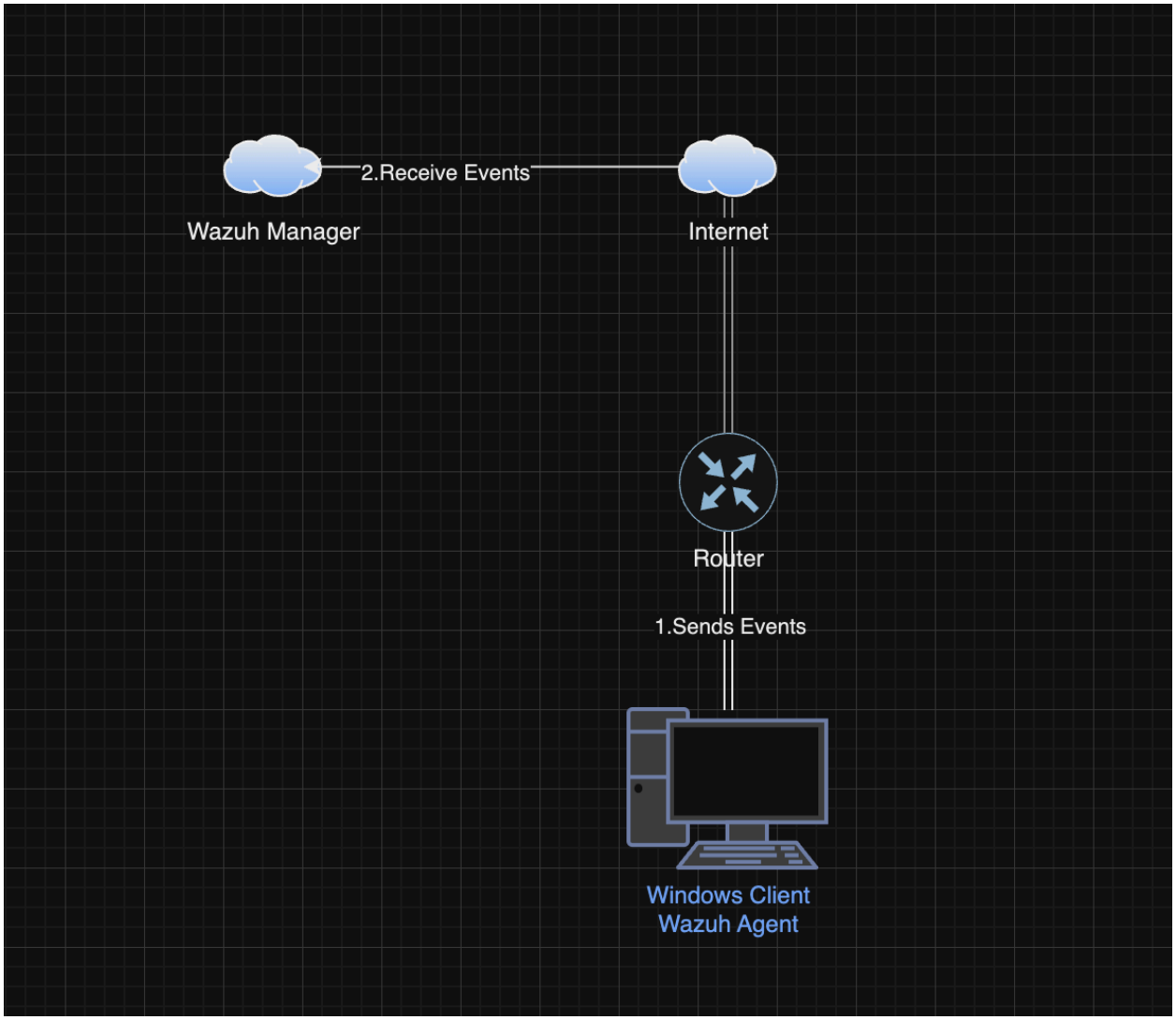
- **Tool Used**: Wazuh (an open-source security monitoring tool)
- **Purpose**: To detect and alert on the execution of Mimikatz and similar tools.
- **Process**:
    - Created custom Wazuh rules to monitor Sysmon logs.
    - Utilized specific event fields, such as "Original file name," to accurately detect the execution of Mimikatz.
    - Enhanced rule specificity to minimize false positives and improve detection accuracy.

Results

- **Successful Simulation**: Executed Mimikatz attacks were successfully simulated and captured by Sysmon.
- **Effective Detection**: Custom Wazuh rules accurately detected the execution of Mimikatz, generating alerts with high precision.
- **Improved Monitoring**: The integration of detailed event logging and tailored alerting mechanisms significantly improved the security monitoring capabilities.

Conclusion

The project effectively demonstrated the importance of simulating real-world attacks to test and improve security detection mechanisms. By leveraging tools like Sysmon and Wazuh, the project successfully enhanced the ability to detect and respond to credential extraction attacks, contributing to a more robust cybersecurity posture.

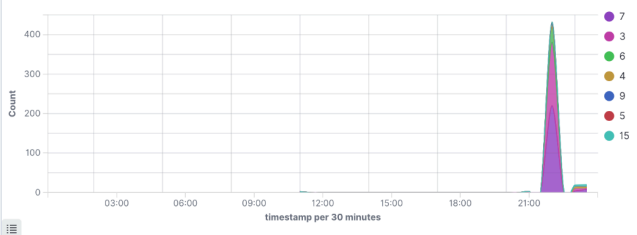


Search | DQL | Last 24 hours | Show dates | Refresh

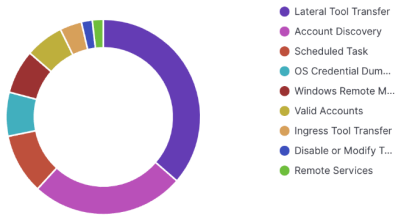
manager.name: waza | + Add filter

Total	Level 12 or above alerts	Authentication failure	Authentication success
489	9	0	7

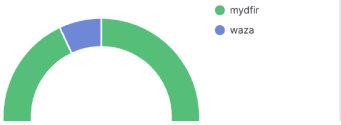
Alert level evolution



Top MITRE ATT&CKS



Top 5 agents



Alerts evolution - Top 5 agents

Security Alerts

Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Aug 4, 2024 @ 23:59:31.816	001	mydfir	T1003	Credential Access	Mimikatz Usage Detected	15	100002
Aug 4, 2024 @ 23:59:04.963	000	waza			Wazuh server started.	3	502
Aug 4, 2024 @ 23:58:53.186	000	waza			Host-based anomaly detection event (rootcheck).	7	510
Aug 4, 2024 @ 23:58:53.143	000	waza			Host-based anomaly detection event (rootcheck).	7	510
Aug 4, 2024 @ 23:58:32.506	001	mydfir	T1053.005	Execution, Persistence, Privilege Escalation	Process loaded taskschd.dll module. May be used to create delayed malware execution	4	92154
Aug 4, 2024 @ 23:53:25.827	000	waza			Wazuh server started.	3	502
Aug 4, 2024 @ 23:53:13.828	000	waza			Host-based anomaly detection event (rootcheck).	7	510
Aug 4, 2024 @ 23:53:13.803	000	waza			Host-based anomaly detection event (rootcheck).	7	510
Aug 4, 2024 @ 23:49:40.244	001	mydfir	T1003	Credential Access	Mimikatz Usage Detected	15	100002
Aug 4, 2024 @ 23:48:28.655	001	mydfir	T1053.005	Execution, Persistence, Privilege Escalation	Process loaded taskschd.dll module. May be used to create delayed malware execution	4	92154

Rows per page: 10 < 1 2 3 4 5 ... 49 >

Mimikatz Usage Detected

View alerts of this Rule

Information

ID	Level	File	Path
100002	15	local_rules.xml	etc/rules

Groups
local, syslog, sshd

Details

If_group	Win.Eventdata.OriginalFileName
sysmon_event1	pattern: (?i)mimikatz\.exe, type: pcre2

Compliance

Related rules

ID	Description	Groups	Compliance	Level	File
100001	sshd: authentication failed from IP 1.1.1.1.	authentication_failed, local, syslog, sshd	PCI_DSS	5	local_rules.xml
100002	Mimikatz Usage Detected	local, syslog, sshd	MITRE	15	local_rules.xml

Rows per page: 10

1

Security Alerts

Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Aug 4, 2024 @ 22:58:37.020	001	mydfir	T1003	Credential Access	Mimikatz Usage Detected	15	100002
Aug 4, 2024 @ 22:58:23.158	001	mydfir	T1105	Command and Control	Executable file dropped in folder commonly used by malware	15	92213

Private IPv4 address: 172

File Home Share View | Manage Application Tools | x64

This PC › Downloads › mimikatz_trunk › x64

Search x64

Name	Date modified	Type	Size
awesome	8/5/2024 5:26 AM	Application	1,324 KB
mimidrv.sys	8/5/2024 5:26 AM	System file	37 KB
mimilib.dll	8/5/2024 5:26 AM	Application exten...	37 KB
mimispool.dll	8/5/2024 5:26 AM	Application exten...	11 KB

Quick access
Desktop
Documents
Downloads
Pictures
ossec-agent
This PC
Network

4 items | 1 item | 5 items

mimikatz 2.2.0 x64 (oe.eo)

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> cd C:\Users\Administrator\Downloads\mimikatz_trunk\x64
PS C:\Users\Administrator\Downloads\mimikatz_trunk\x64> .\awesome.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz #
```

Search | DQL | Last 24 hours | Show dates | Refresh

+ Add filter

wazuh-archives-**

Search field names

Filter by type 0

Selected fields

_source

Available fields

_index
@timestamp
agent.id
agent.ip
agent.name
data.file
data.title
data.win.eventdata.creationUtcTime
data.win.eventdata.image
data.win.eventdata.processGuid
data.win.eventdata.processId
data.win.eventdata.ruleName
data.win.eventdata.targetFilename
data.win.eventdata.user
data.win.eventdata.utcTime
data.win.system.channel
data.win.system.computer

126 hits

Aug 3, 2024 @ 22:36:17.743 - Aug 4, 2024 @ 22:36:17.743 Auto

Time	_source
Aug 4, 2024 @ 22:36:12.455	predecoder.hostname: waza predecoder.program_name: opensearch-dashboards predecoder.timestamp: Aug 5 05:36:10 agent.name: waza agent.id: 000 manager.name: waza full_log: Aug 5 05:36:10 waza opensearch-dashboards[57473]: {"type":"response","@timestamp":"2024-08-05T05:36:10Z","tags":[],"pid":57473,"method":"get","statusCode":200,"req":{"url":"/47502/bundles/plugin/discover/discover.chunk.3.js","method":"get","headers":{"host":"143.110.234.22","connection":"keep-alive","sec-ch-ua":"\"Not/A)Brand\";v=\"8\", \"Chromium\";v=\"126\", \"Google Chrome\";v=\"126\"","dnt":"1","sec-ch-ua-mobile":"?
Aug 4, 2024 @ 22:36:12.455	predecoder.hostname: waza predecoder.program_name: opensearch-dashboards predecoder.timestamp: Aug 5 05:36:10 agent.name: waza agent.id: 000 manager.name: waza full_log: Aug 5 05:36:10 waza opensearch-dashboards[57473]: {"type":"response","@timestamp":"2024-08-05T05:36:10Z","tags":[],"pid":57473,"method":"get","statusCode":200,"req":{"url":"/47502/bundles/plugin/discover/discover.chunk.1.js","method":"get","headers":{"host":"143.110.234.22","connection":"keep-alive","sec-ch-ua":"\"Not/A)Brand\";v=\"8\", \"Chromium\";v=\"126\", \"Google Chrome\";v=\"126\"","dnt":"1","sec-ch-ua-mobile":"?
Aug 4, 2024 @ 22:36:12.455	predecoder.hostname: waza predecoder.program_name: opensearch-dashboards predecoder.timestamp: Aug 5 05:36:10 agent.name: waza agent.id: 000 manager.name: waza full_log: Aug 5 05:36:10 waza opensearch-dashboards[57473]: {"type":"response","@timestamp":"2024-08-05T05:36:10Z","tags":[],"pid":57473,"method":"get","statusCode":200,"req":{"url":"/ui/favicons/favicon.ico","method":"get","headers":{"host":"143.110.234.22","connection":"keep-alive","sec-ch-

wazuh. Modules Security events

Dashboard Events Explore agent

sysmon DQL Refresh

manager.name: waza + Add filter

wazuh-alerts-*

Search field names

Filter by type 0

Selected fields

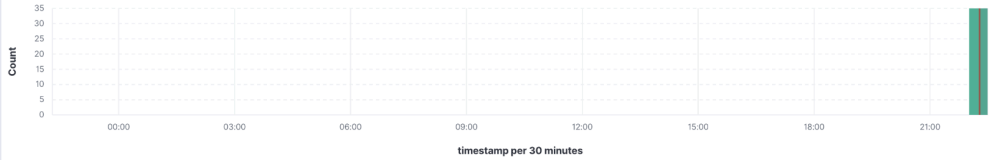
- agent.name
- rule.description
- rule.id
- rule.level

Available fields

- agent.id
- agent.ip
- data.dstuser
- data.extra_data
- data.file
- data.sca.check.command
- data.sca.check.compliance.cis
- data.sca.check.compliance.cis_csc
- data.sca.check.compliance.gdpr_IV
- data.sca.check.compliance.gpg_13
- data.sca.check.compliance.gpg13

35 hits

Aug 3, 2024 @ 22:17:07.959 - Aug 4, 2024 @ 22:17:07.959 Auto



Time	agent.name	rule.description	rule.level	rule.id
Aug 4, 2024 @ 22:16:42.792	mydfir	Powershell process created an executable file in Windows root folder	9	92205
Aug 4, 2024 @ 22:16:40.761	mydfir	Discovery activity executed	3	92031
Aug 4, 2024 @ 22:16:40.699	mydfir	Discovery activity executed	3	92031
Aug 4, 2024 @ 22:16:40.671	mydfir	A net.exe account discovery command was initiated	3	92039
Aug 4, 2024 @ 22:16:40.671	mydfir	A net.exe account discovery command was initiated	3	92039
Aug 4, 2024 @ 22:16:40.654	mydfir	A net.exe account discovery command was initiated	3	92039
Aug 4, 2024 @ 22:16:39.659	mydfir	A net.exe account discovery command was initiated	3	92039
Aug 4, 2024 @ 22:16:39.636	mydfir	A net.exe account discovery command was initiated	3	92039

STATUS

- Active (1)
- Disconnected (0)
- Pending (0)
- Never connected (0)

DETAILS

Active	Disconnected	Pending	Never connected	Agents coverage
1	0	0	0	100.00%

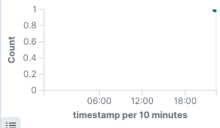
Last registered agent: mydfir

Most active agent: mydfir

EVOLUTION

Last 24 hours

active



Agents (1)

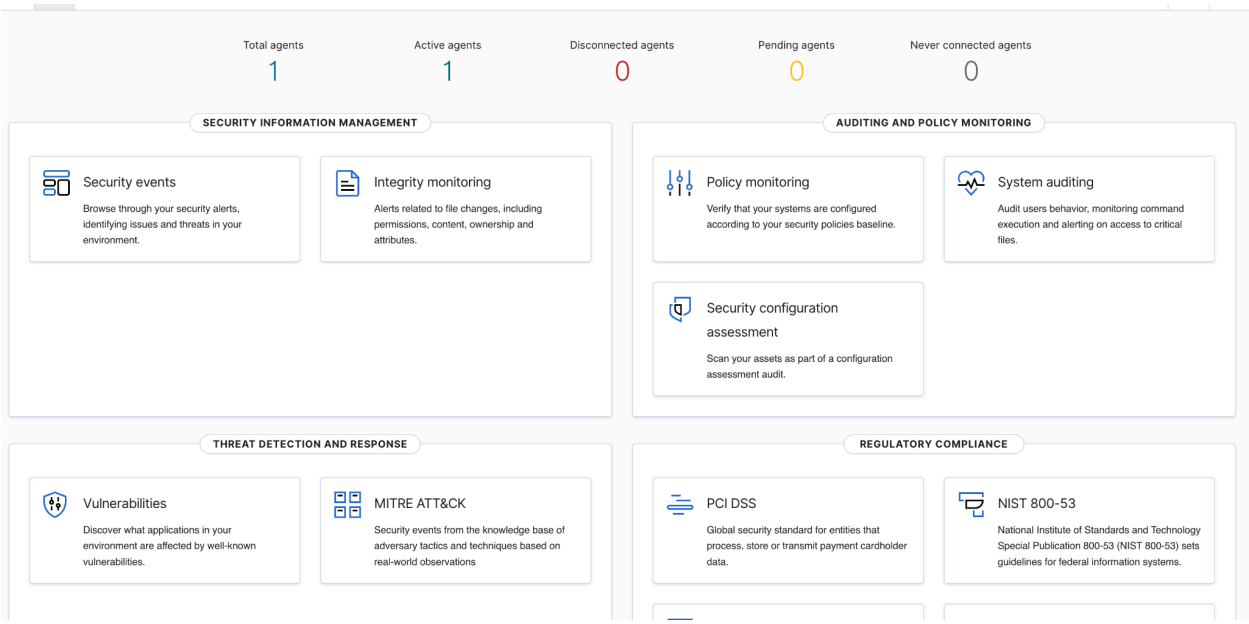
Deploy new agent Refresh Export formatted

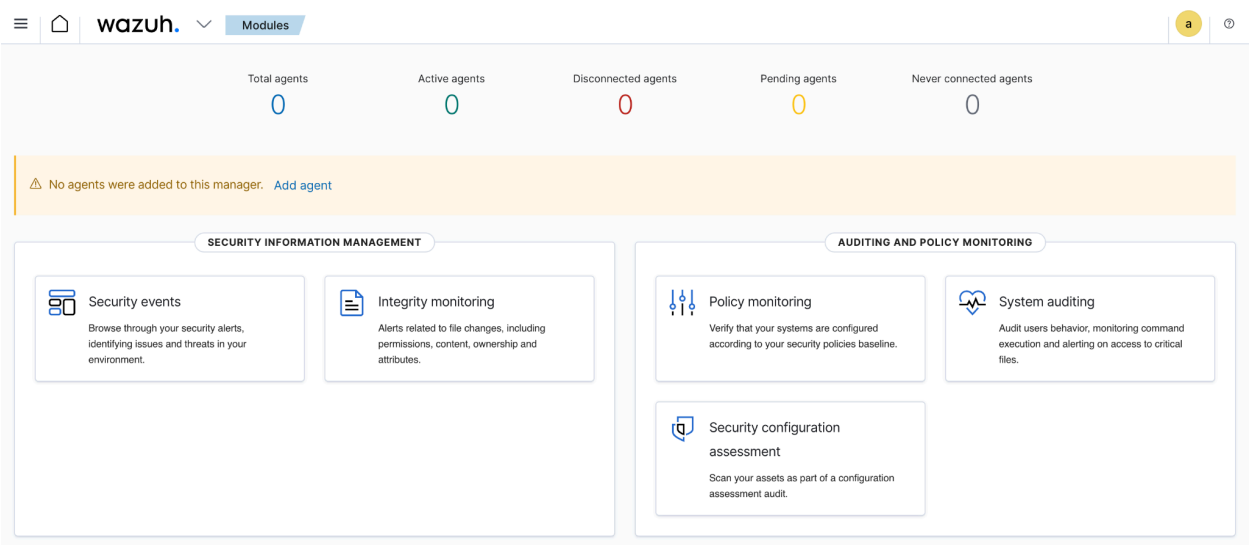
id!=000 and Search WQL Refresh

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	mydfir	172.31.30.4	default	Microsoft Windows Server 2022 Datacenter 10.0.20348.2582	node01	v4.7.5	active	

Rows per page: 10

1


Total agents
1
Active agents
1
Disconnected agents
0
Pending agents
0
Never connected agents
0
SECURITY INFORMATION MANAGEMENT
Security events
Browse through your security alerts, identifying issues and threats in your environment.
Integrity monitoring
Alerts related to file changes, including permissions, content, ownership and attributes.
AUDITING AND POLICY MONITORING
Policy monitoring
Verify that your systems are configured according to your security policies baseline.
System auditing
Audit users behavior, monitoring command execution and alerting on access to critical files.
Security configuration assessment
Scan your assets as part of a configuration assessment audit.
THREAT DETECTION AND RESPONSE
Vulnerabilities
Discover what applications in your environment are affected by well-known vulnerabilities.
MITRE ATT&CK
Security events from the knowledge base of adversary tactics and techniques based on real-world observations
REGULATORY COMPLIANCE
PCI DSS
Global security standard for entities that process, store or transmit payment cardholder data.
NIST 800-53
National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.


wazuh.
Modules
a
Total agents
0
Active agents
0
Disconnected agents
0
Pending agents
0
Never connected agents
0
No agents were added to this manager.
Add agent
SECURITY INFORMATION MANAGEMENT
Security events
Browse through your security alerts, identifying issues and threats in your environment.
Integrity monitoring
Alerts related to file changes, including permissions, content, ownership and attributes.
AUDITING AND POLICY MONITORING
Policy monitoring
Verify that your systems are configured according to your security policies baseline.
System auditing
Audit users behavior, monitoring command execution and alerting on access to critical files.
Security configuration assessment
Scan your assets as part of a configuration assessment audit.