EDR/SIEM for fellow Stingy Red Teamers

Repo with my config: https://github.com/kyle41111/WazuhRedTeamLab

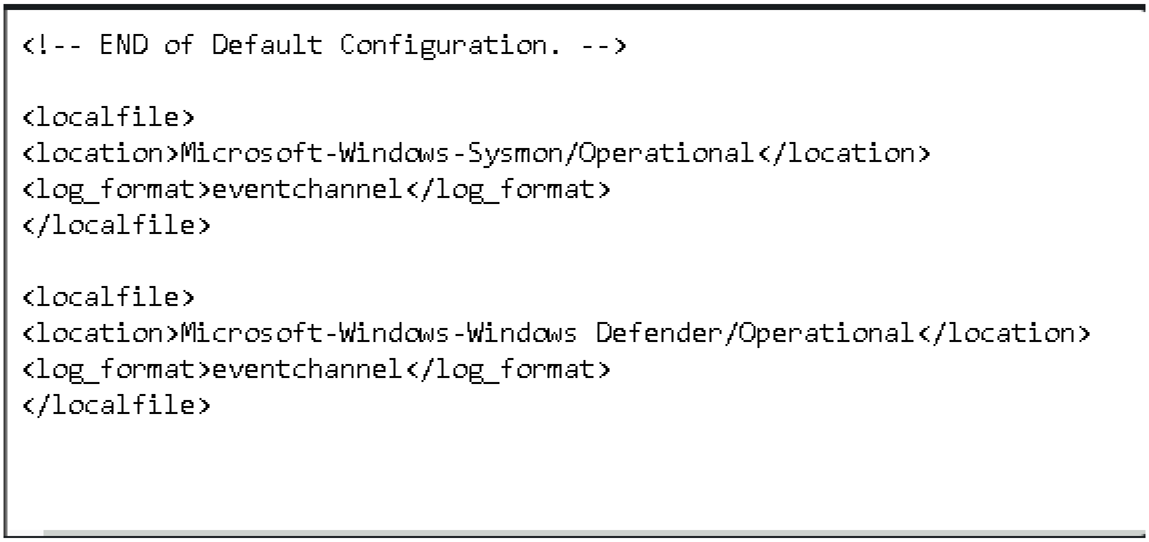
Lets get the downloads out of the way:

```
https://wazuh.com/resources/blog/detecting-process-injection-with-wazuh/sysmonconfig.xml
https://raw.githubusercontent.com/kyle41111/RedTeamHelp/main/infra/local_rules.xml
```

Install wazuh indexer on your linux distro of choice:

```
https://packages.wazuh.com/4.3/wazuh-install.sh
sudo bash ./wazuh-install.sh -a -i
```

Now just delete the local_rules.xml file and replace it with the modded one on my github and then restart wazuh manager:



```
<!-- END of Default Configuration. -->

<localfile>
<location>Microsoft-Windows-Sysmon/Operational</location>
<log_format>eventchannel</log_format>
</localfile>

<localfile>
<location>Microsoft-Windows-Windows Defender/Operational</location>
<log_format>eventchannel</log_format>
</localfile>
```

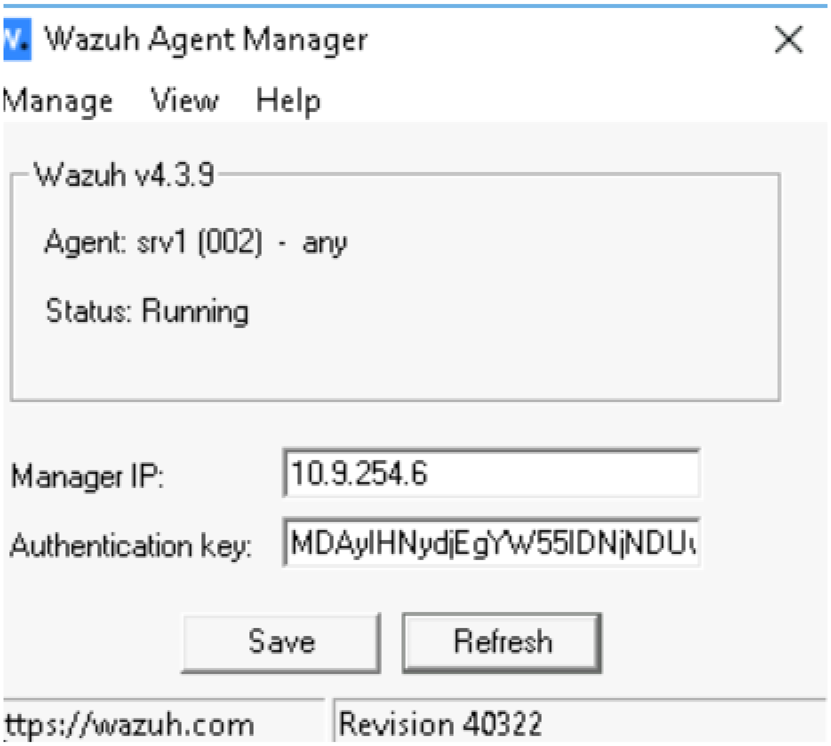
Lastly we need to setup our sysmon config.

download sysmon64.exe and the sysmon config from wazuh here and set the configuration:

download sysmon64.exe and the sysmon config from wazuh here and set the configuration

```
https://wazuh.com/resources/blog/detecting-process-injection-with-wazuh/sysmonconfig.xml
sysmon64.exe -c sysmonconfig.xml
```

Now just start the endpoint manager. if you want the ui its in the install folder.



Wazuh v4.3.9

Agent: srv1 (002) - any

Status: Running

Manager IP: 10.9.254.6

Authentication key: MDAyIHNydjEgYW55IDNjNDU

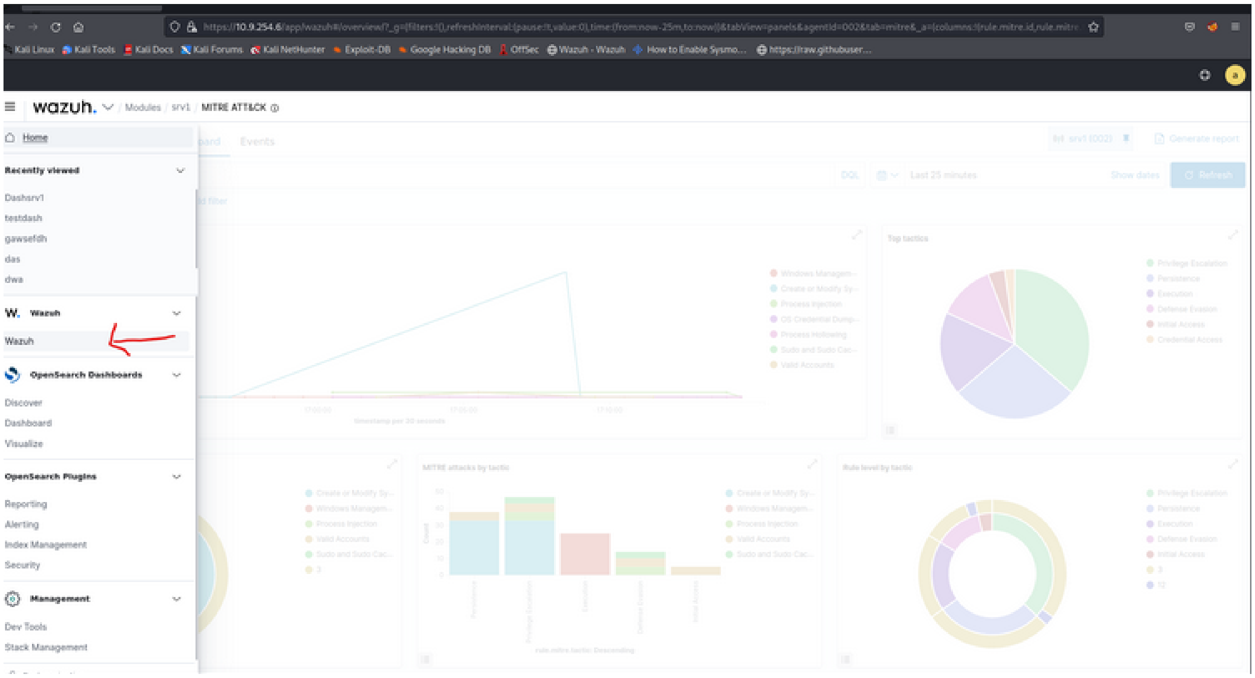
ttps://wazuh.com

Revision 40322

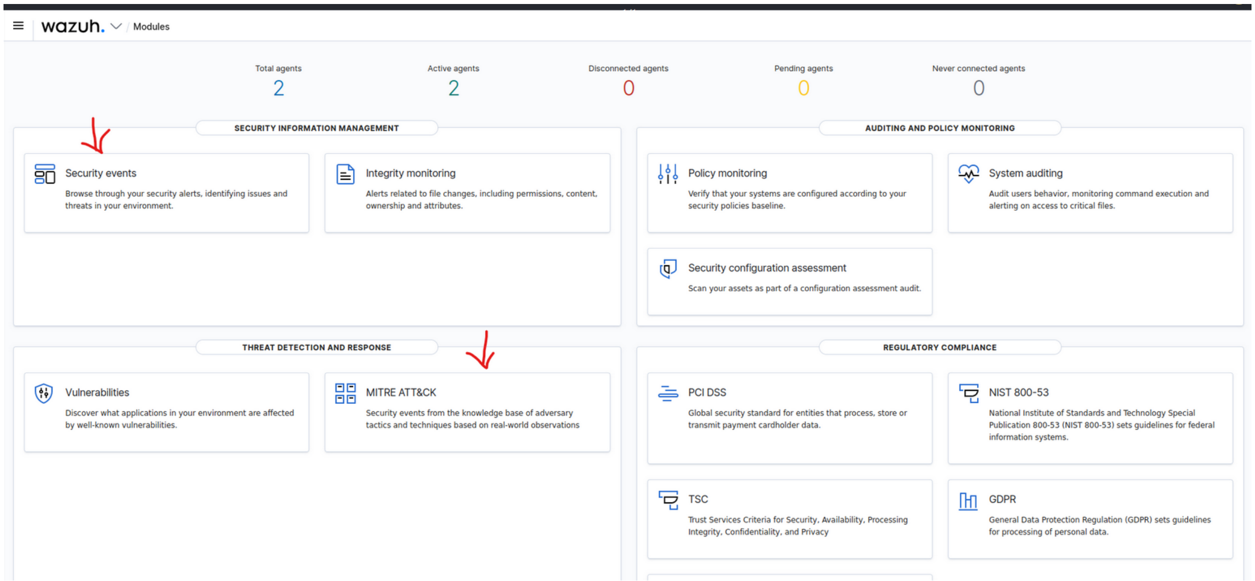
Restart the wazuh manager to update rules:

```
sudo systemctl restart wazuh-manager
```

Heres where you wanna click to get info:



From here you have two options of views. The MITRE framework view, and the security alerts view. Use mitre if youd prefer.



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.

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.

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

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.

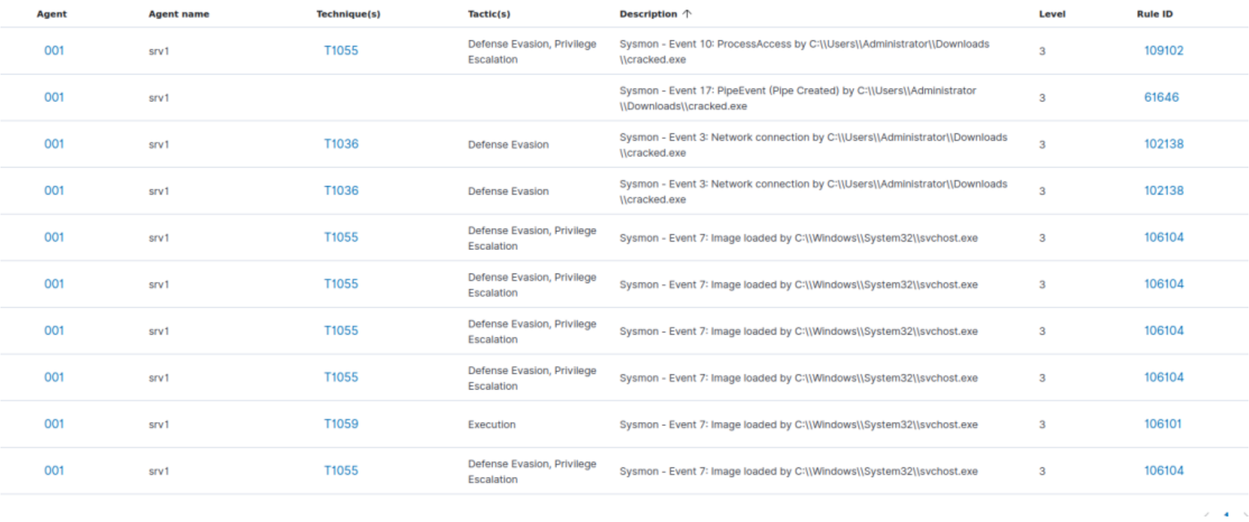
TSC

Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy

GDPR

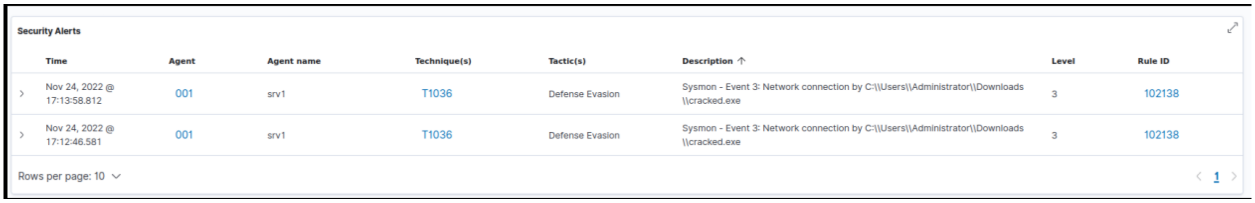
General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.

I was honestly skeptical if this was functioning as an EDR or not and tested it out with inlineExecute-Assembly. Heres the image load events from execute-assembly on a ntMapSection runner. loud af.



Agent	Agent name	Technique(s)	Tactic(s)	Description ↑	Level	Rule ID
001	srv1	T1055	Defense Evasion, Privilege Escalation	Sysmon - Event 10: ProcessAccess by C:\\Users\\Administrator\\Downloads \\cracked.exe	3	109102
001	srv1			Sysmon - Event 17: PipeEvent (Pipe Created) by C:\\Users\\Administrator \\Downloads\\cracked.exe	3	61646
001	srv1	T1036	Defense Evasion	Sysmon - Event 3: Network connection by C:\\Users\\Administrator\\Downloads \\cracked.exe	3	102138
001	srv1	T1036	Defense Evasion	Sysmon - Event 3: Network connection by C:\\Users\\Administrator\\Downloads \\cracked.exe	3	102138
001	srv1	T1055	Defense Evasion, Privilege Escalation	Sysmon - Event 7: Image loaded by C:\\Windows\\System32\\svchost.exe	3	106104
001	srv1	T1055	Defense Evasion, Privilege Escalation	Sysmon - Event 7: Image loaded by C:\\Windows\\System32\\svchost.exe	3	106104
001	srv1	T1055	Defense Evasion, Privilege Escalation	Sysmon - Event 7: Image loaded by C:\\Windows\\System32\\svchost.exe	3	106104
001	srv1	T1055	Defense Evasion, Privilege Escalation	Sysmon - Event 7: Image loaded by C:\\Windows\\System32\\svchost.exe	3	106104
001	srv1	T1059	Execution	Sysmon - Event 7: Image loaded by C:\\Windows\\System32\\svchost.exe	3	106101
001	srv1	T1055	Defense Evasion, Privilege Escalation	Sysmon - Event 7: Image loaded by C:\\Windows\\System32\\svchost.exe	3	106104

Now we try inlineExecute-Assembly and utilize its ETW patching functionality. The load image events were not flagged/existent.



Security Alerts

	Time	Agent	Agent name	Technique(s)	Tactic(s)	Description ↑	Level	Rule ID
›	Nov 24, 2022 @ 17:13:58.812	001	srv1	T1036	Defense Evasion	Sysmon - Event 3: Network connection by C:\\Users\\Administrator\\Downloads \\cracked.exe	3	102138
›	Nov 24, 2022 @ 17:12:46.581	001	srv1	T1036	Defense Evasion	Sysmon - Event 3: Network connection by C:\\Users\\Administrator\\Downloads \\cracked.exe	3	102138

Rows per page: 10

Now go ahead and be wreckless! and then be sneaky!