Exchange WAF

https://www.crowdsec.net/blog/how-to-protect-microsoft-exchange-server-crowdsec

CrowdSec Commands

```
cscli.exe collections list
cscli.exe bouncers list
cscli.exe collections install NAME
cscli.exe collections inspect NAME

cscli.exe decisisions list
cscli.exe decisions add --ip "IP"  # Ban specific IP
cscli.exe decisions delete --ip "IP"  # Remove blacklist on IP
```

Install

CrowdSec Agent

- Download and run: https://github.com/crowdsecurity/crowdsec/releases/download/v1.6.6/crowdsec_1.6.6.msi
- Creates a service called `CrowdSec`

```
cscli.exe collections list
```

Install IIS Collection

```
cscli.exe collections install crowdsecurity/iis

cscli collections inspect crowdsecurity/http-cve
```

Bouncer Download

- https://github.com/crowdsecurity/cs-windows-firewall-bouncer/releases
  - Download and install `cs_windows_firewall_installer_bundle.exe`
  - (Or directly) `https://github.com/crowdsecurity/cs-windows-firewall-bouncer/releases/download/v0.0.5/cs_windows_firewall_installer_bundle.exe`

```
cscli bouncers list
```

```
PS C:\> cscli bouncers list
-------------------------------------------------------------------------------------------------------------------------------------------------------
 NAME                                          IP ADDRESS  VALID  LAST API PULL         TYPE                  VERSION  AUTH TYPE
-------------------------------------------------------------------------------------------------------------------------------------------------------
 windows-firewall-bouncer-20221102105006017 6  127.0.0.1   ✔      2022-11-02T09:50:43Z  cs-windows-fw-bouncer  0.0.5    api-key
-------------------------------------------------------------------------------------------------------------------------------------------------------
```

Add IIS Log Support

In `C:\ProgramData\CrowdSec\config\acquis.yaml`

```
---
source: wineventlog
event_channel: Microsoft-IIS-Logging/Logs
event_ids:
    - 6200
event_level: information
labels:
    type: iis
```

- Add this to the very bottom of the yaml. Do NOT leave space between rules
- Use 4 spaces in notepad...NOT TABS

```
Restart-Service CrowdSec
Get-Content "C:\ProgramData\CrowdSec\log\crowdsec.log" -Wait
```