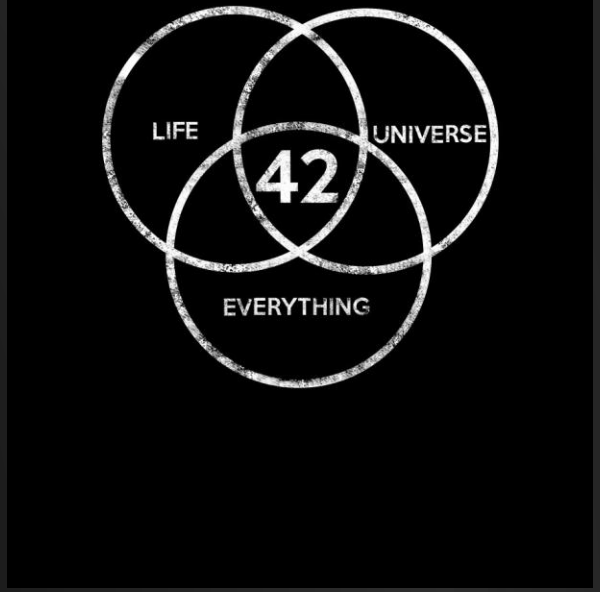
Open Source and Free EDR

John Strand

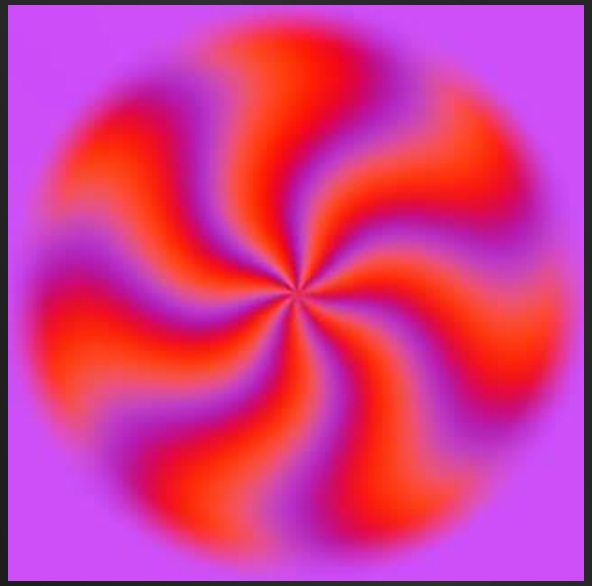
Why we are here

- Free and Open tools for Endpoint Detection and Response
- There is Free and there is "Free"
- We will not demo all of them
- A shoutout and apology to some vendors... But we have to clear some things up



What the hell EDR???

- Endpoint Detection and Response can mean a lot of things.....
- Does it include prevention?
- Is it just the black box flight recorder?
- What about SOAR?
- What about eXtended Detection and Response (XDR)?



What do you see?

I am soo sorry....

Vendors....

Cynet

CROWDSTRIKE

CISCO
AMP Threat Grid

FIREEYE

CYLANCE

Symantec.

Carbon Black.

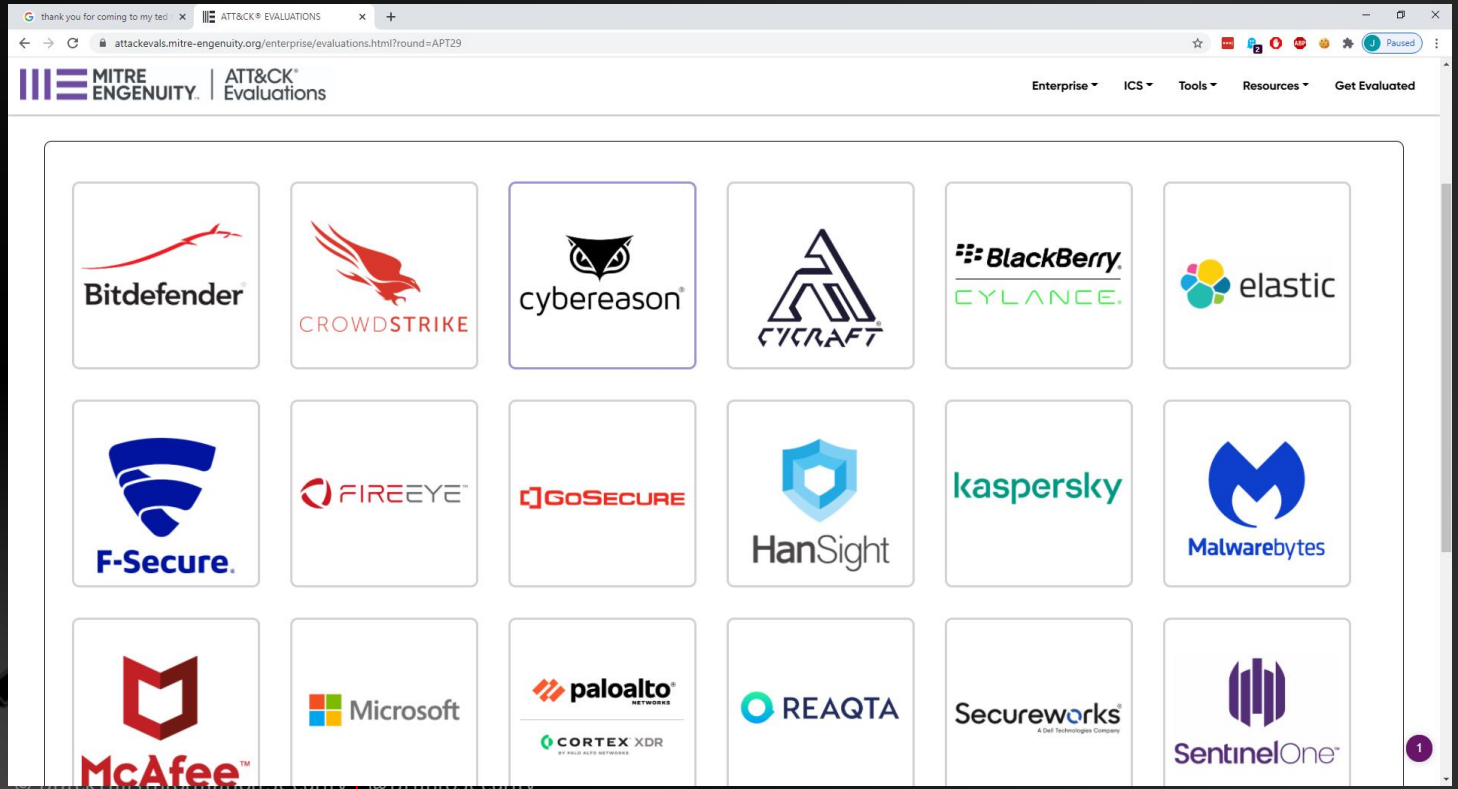
SentinelOne

McAfee

CORTEX XDR

cybereason

MITRE Evaluations



Also… Vendors

Why EDR?

- Because IR is a nightmare without it
- Quickly get information from multiple sources
- Correlate attack data < GOOD threat intelligence!!
- Because Windows logs suck
  - Not you Sysmon... You cool.

Why free and Open Source?

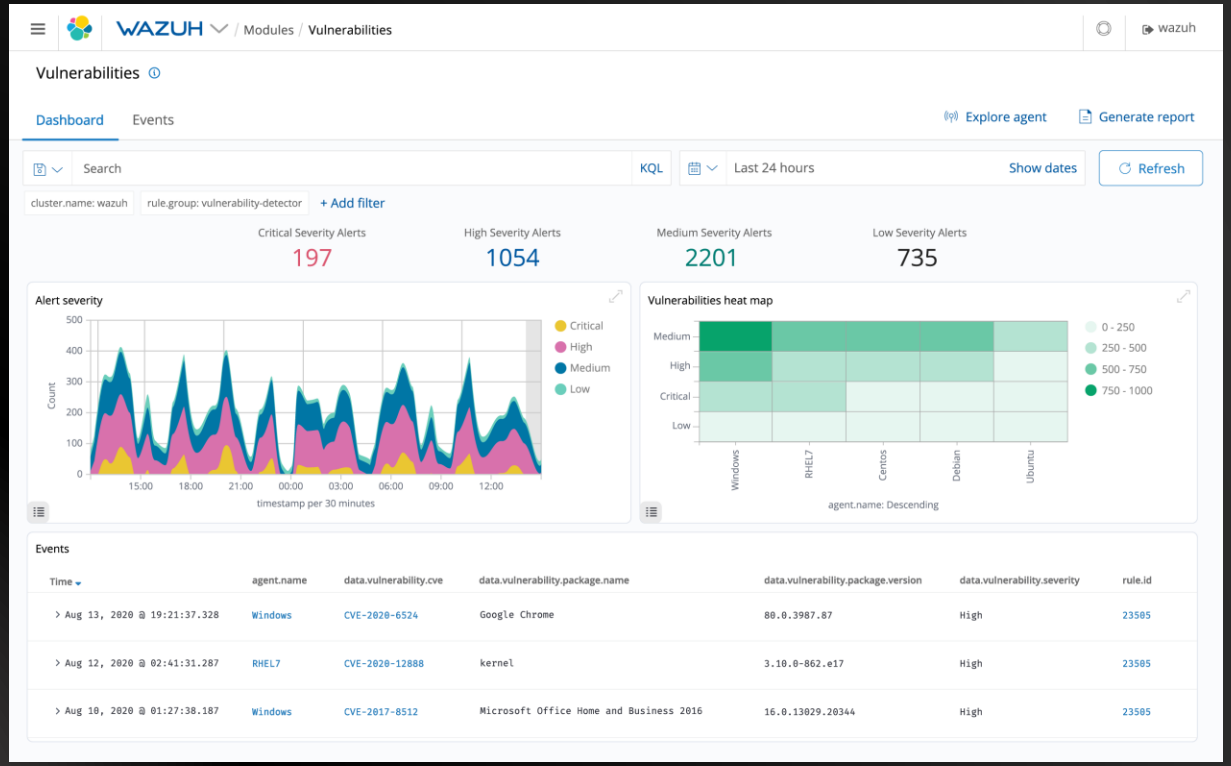
- I hate vendors that don't have free or Open Source Products
- How do you know if it works? Cool GUI? Trial? They promise?
- Also, many companies can't afford full solutions
  - A quick note on pricing
- You are not paying for what a commercial tool does... You are paying for what the free/OS tools do not provide.

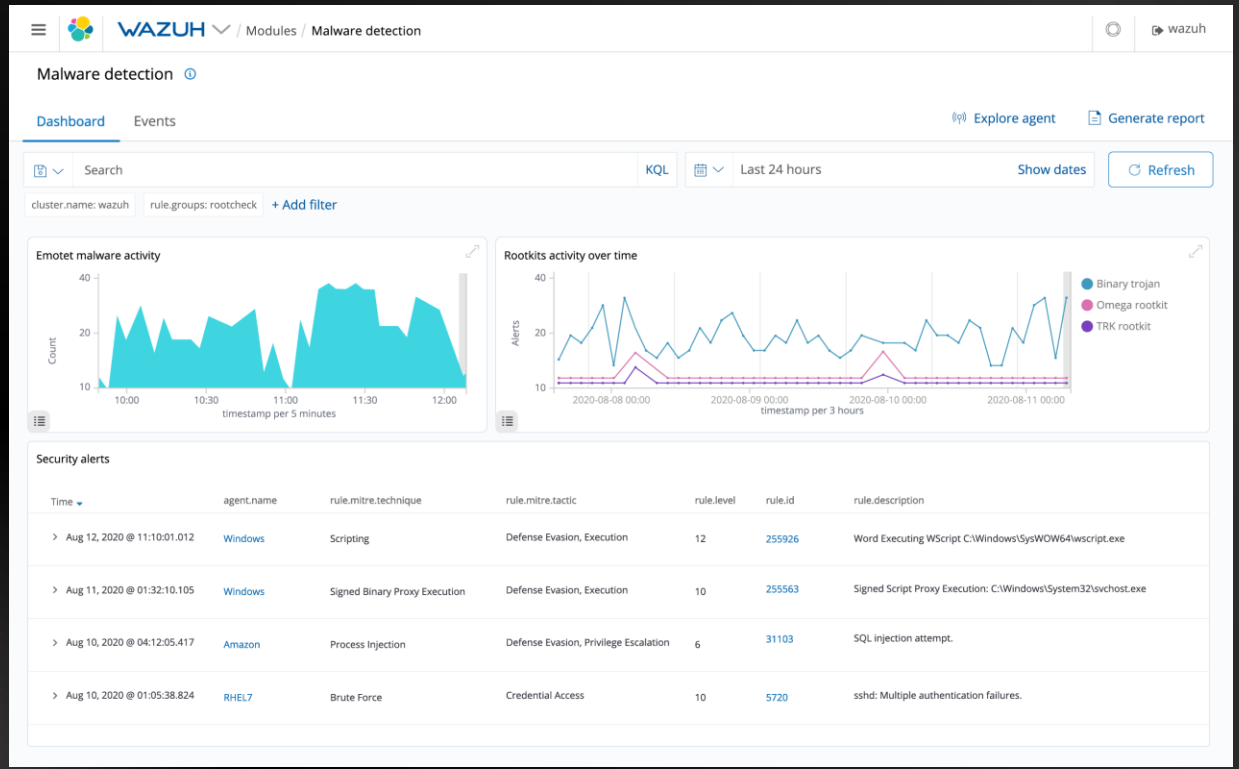
- Not sure... But this one has been around possibly longer than anyone else
- Used for years on Linux systems for Rootkit detection
- Monitors key files and logs
- Now adding in anti-malware features and response
- Can be intimidating to get started, not all that bad
- "Worst selling security book in history"
- Aversion to screenshots.....

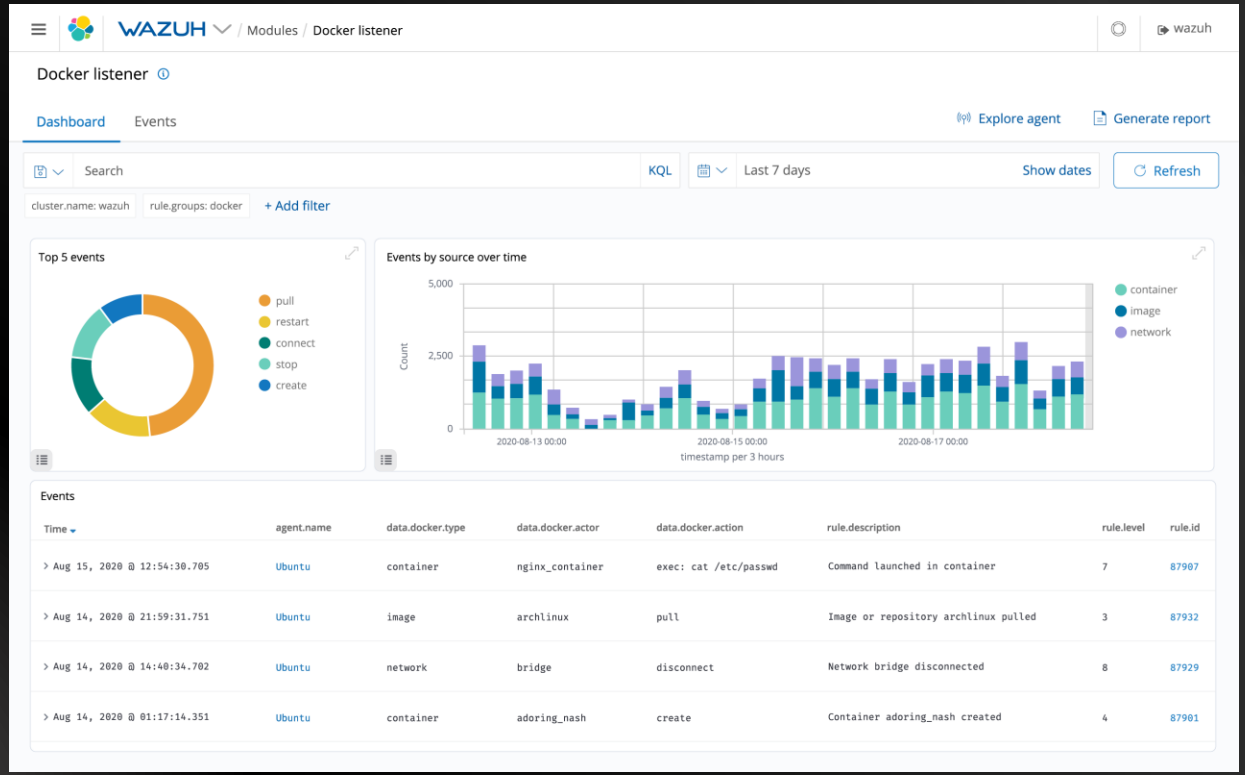
WAZUH

- Originally one of the more badass inventory systems
- Loved the query language across systems
- Full stack EDR
- Super easy to install, multiple agents
- Data feeds to an ELK stack... Because everything does...
- Easily one of the most asked about tools in my classes
- Just don't want to run a full ELK stack in my labs

I may be pronouncing it wrong


WAZUH / Modules / Vulnerabilities
wazuh
Vulnerabilities
Dashboard
Events
Explore agent
Generate report
Search
KQL
Last 24 hours
Show dates
Refresh
cluster.name: wazuh
rule.group: vulnerability-detector
+ Add filter
Critical Severity Alerts
197
High Severity Alerts
1054
Medium Severity Alerts
2201
Low Severity Alerts
735
Alert severity
Count
timestamp per 30 minutes
Critical
High
Medium
Low
Vulnerabilities heat map
Medium
High
Critical
Low
Windows
RHEL7
Centos
Debian
Ubuntu
agent.name: Descending
0 - 250
250 - 500
500 - 750
750 - 1000
Events
Time
agent.name
data.vulnerability.cve
data.vulnerability.package.name
data.vulnerability.package.version
data.vulnerability.severity
rule.id
Aug 13, 2020 @ 19:21:37.328
Windows
CVE-2020-6524
Google Chrome
80.0.3987.87
High
23505
Aug 12, 2020 @ 02:41:31.287
RHEL7
CVE-2020-12888
kernel
3.10.0-862.e17
High
23505
Aug 10, 2020 @ 01:27:38.187
Windows
CVE-2017-8512
Microsoft Office Home and Business 2016
16.0.13029.20344
High
23505





Velociraptor

- This is the one we use in my classes
- Setup to pulling data is very, very quick
- Standalone agent and server in one executable
- From the folks that brought us Rekall
- So... They kind of know what they are doing
- No detection and prevention capability
- Great way to complement existing AV/Protection
- Let's do a demo...

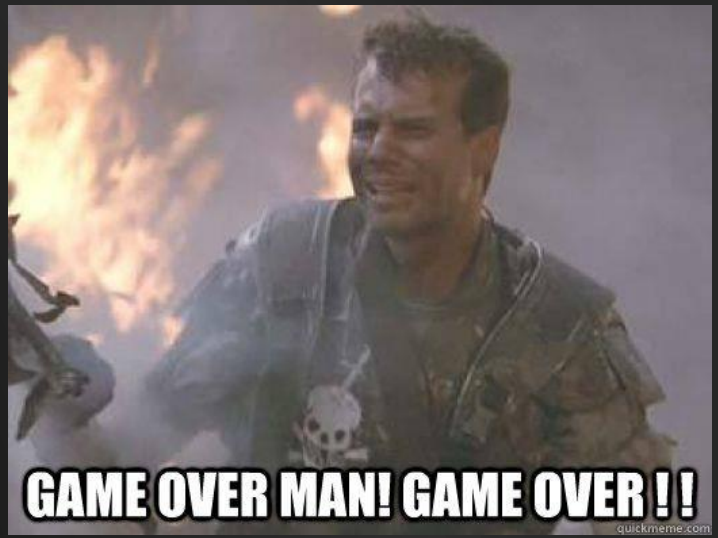
Vendors and Free/OS

- A number of vendors are making their agents free/open source
- This is.... Huge.
- Que rant on people using your product before they spend huge amount of cash on them
- Let's talk about Elastic and Comodo

What "Proudly Sucking At Capitalism" Might look like...

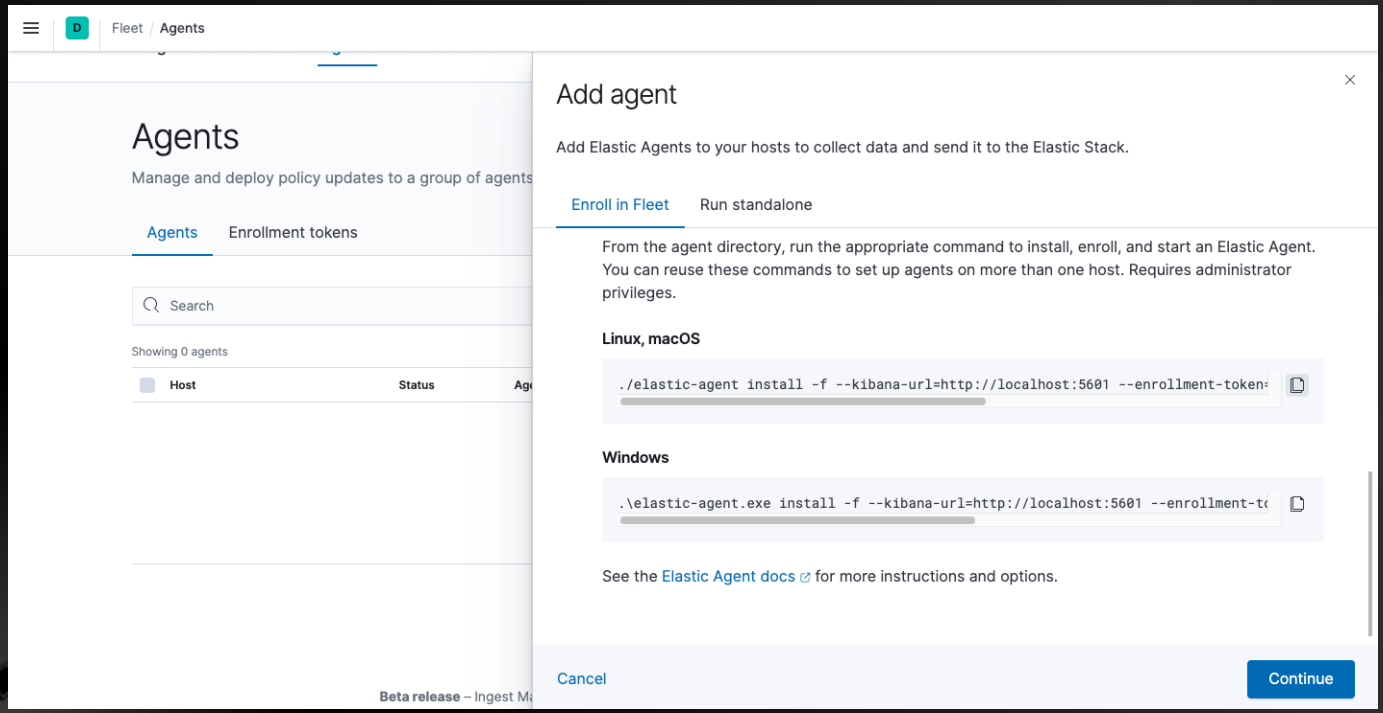
elastic (Formerly Endgame)

- Almost everyone uses ELK
- Many commercial tools use ELK
- Endgame was a solid EDR
- All the "cool kids" use it
  - Sorry Splunk
- Now, they give it away for free*
  - They want the sweet, sweet ELK fees
- Even AMAZON uses ELK!! < -- Too Soon?

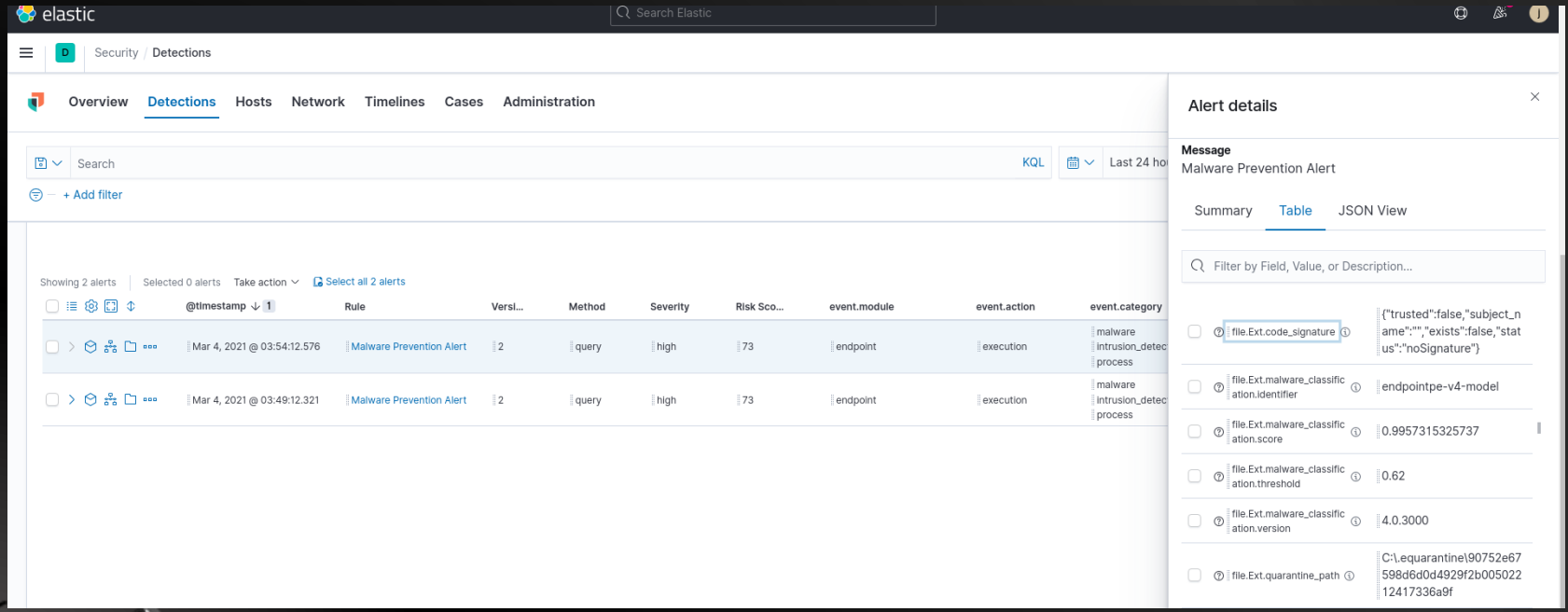


Backdoors & Breaches

Easy Install

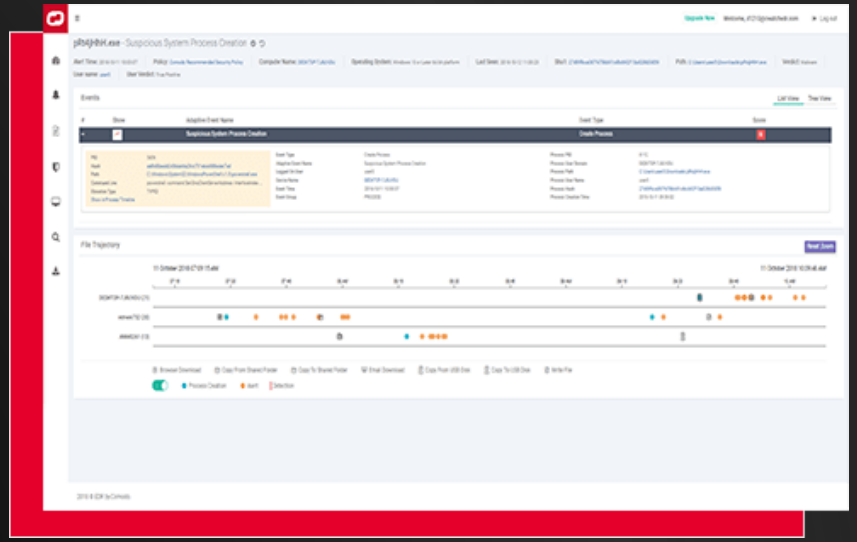


Out of the box... ~5 min

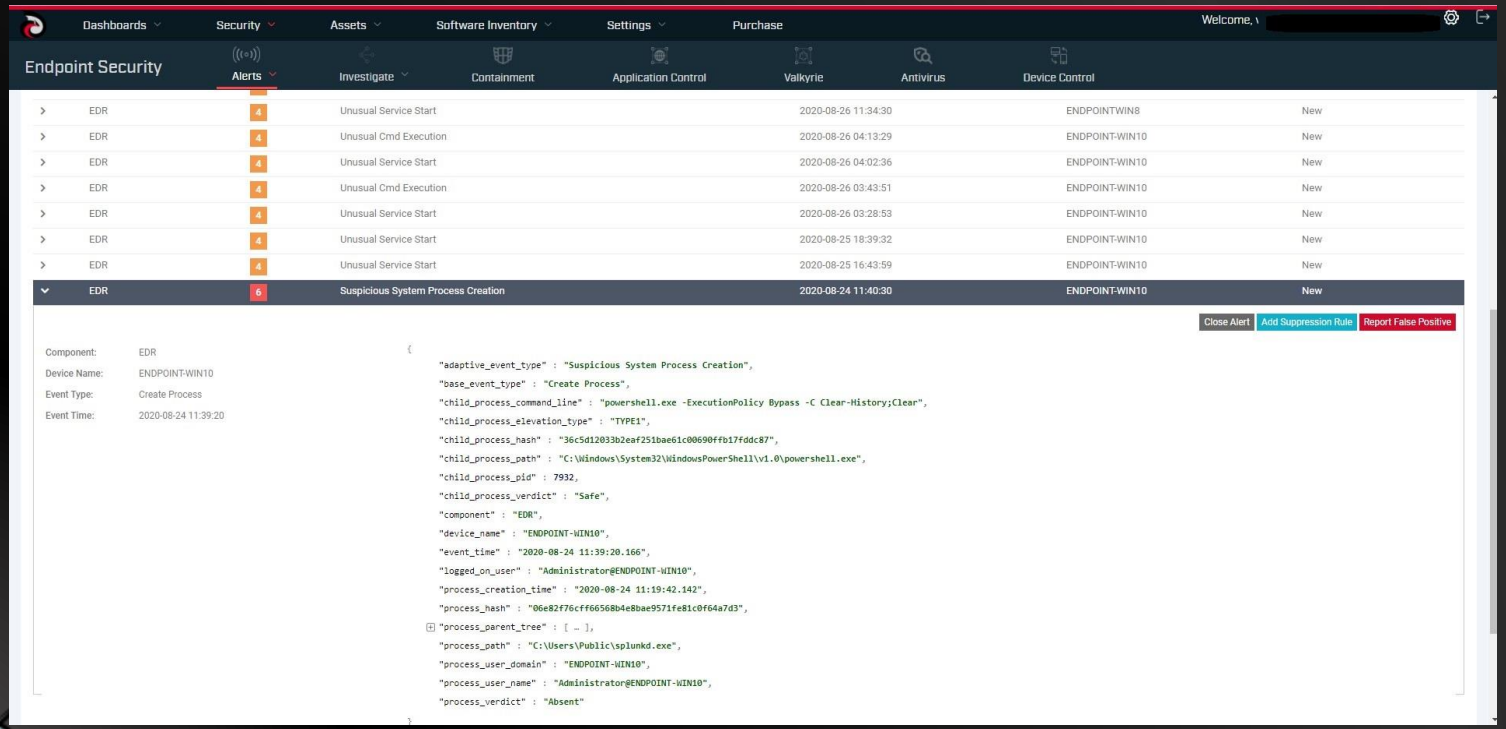


OPEN EDR From Comodo

- Did not see this one coming...
- Wow.
- Full source code on Github
- Want to make your product better fast?
- Solid detection and EDR capabilities
- Works best with their server infrastructure
- Can integrate with ELK



Mad marketing props...



Enhance..


"process_hash" : "06e82f76cff66568b4e8bae9571fe81c0f64a7d3"
"process_parent_tree" : […],
"process_path" : "C:\Users\Public\splunkd.exe",
"process_user_domain" : "ENDPOINT-WIN10",
"process_user_name" : "Administrator@ENDPOINT-WIN10",
"process_verdict" : "Absent"


BLACK HILLS
Information Security

Seriously, not a fluke

Alert List

	Component	Score	Alert Name	Alert Time	Device
⌄	EDR	10	Credential Stealing with Mimikatz	2021-02-01 03:17:15	BLACKWIDDOW

Component: EDR
Device Name: BLACKWIDDOW
Event Type: Virtual Memory Access
Event Time: 2021-02-01 03:16:54


```
{
    "adaptive_event_type" : "Credential Stealing with Mimikatz",
    "base_event_type" : "Virtual Memory Access",
    "component" : "EDR",
    "device_name" : "BLACKWIDDOW",
    "event_time" : "2021-02-01 03:16:54.948",
    "logged_on_user" : "SYSTEM@NT AUTHORITY",
    "process_creation_time" : "2021-02-01 02:42:24.557",
    "process_hash" : "28fa59e9ce120da59009da4c9b9b15ed082427ce",
    "process_parent_tree" : [ … ],
    "process_path" : "C:\Program Files\Elastic\Agent\data\elastic-agent-1da173\install\metricbeat-7.10.1-windows-x86\metricbeat.exe",
    "process_user_domain" : "NT AUTHORITY",
    "process_user_name" : "SYSTEM@NT AUTHORITY",
    "process_verdict" : "Unknown"
}
```

Conclusions

- There is no reason to not have EDR in your toolbox
- It makes life so much easier in an incident
- There is also no reason to live all YOLOSEC!
  - Sure! Take my hundreds of thousands of dollars without trying your product!
- Possibly, we can push all vendors do be more like Comodo and Elastic?
- Mabey?
- Ok... Probably not.
- Oh... And one more thing...

Be most excellent to each other!

I am going to try and sell you something...

It's ok.. You can leave now if you want.

I too, hate it when the sales pitch is at the start or slipped in middle

Seriously, I am not offended if you don't stay

Questions?


BLACK HILLS
Information Security
• 2008 •


BLACK HILLS
Information Security