



Open Source and Free EDR

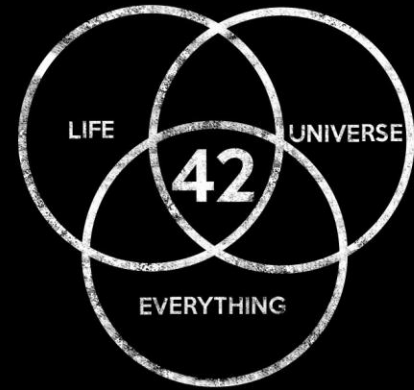
John Strand



© Black Hills Information Security | @BHInfoSecurity

Why we are here

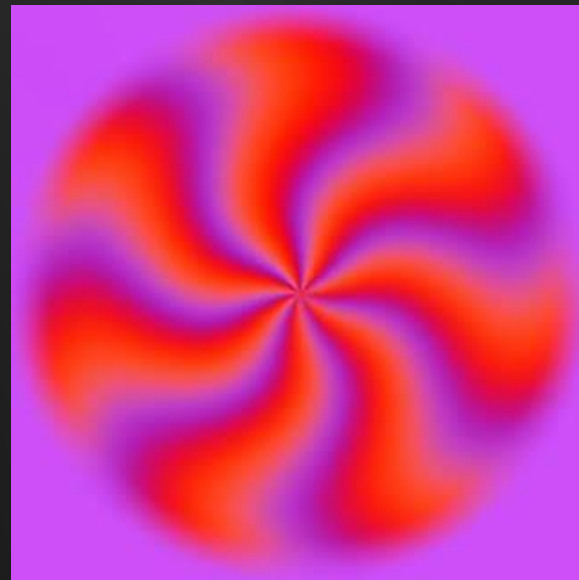
- Free and Open tools for Endpoint Detection and Response
- There is Free and there is "Free"
- We will not demo all of them
- A shoutout and apology to some vendors... But we have to clear some things up



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....



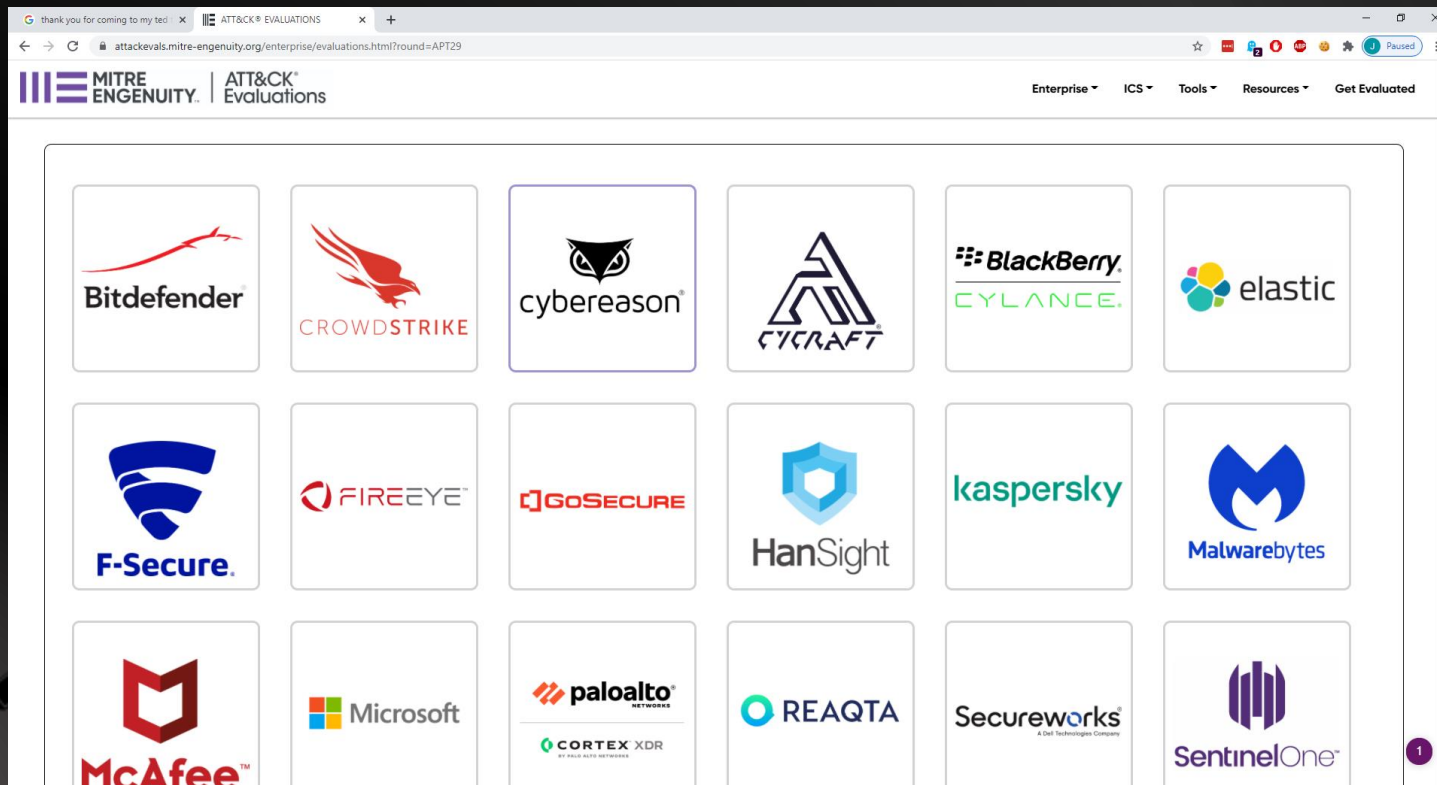
© Black Hills Information Security | @BHInfoSecurity

Vendors....



© Black Hills Information Security | @BHInfoSecurity

MITRE Evaluations



Also... Vendors



**Don't Be Like
This Guy!**



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.

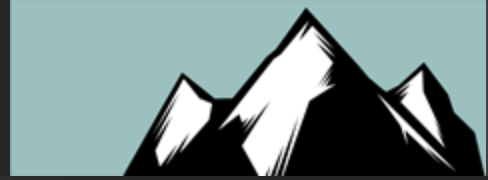


© Black Hills Information Security | @BHInfoSecurity





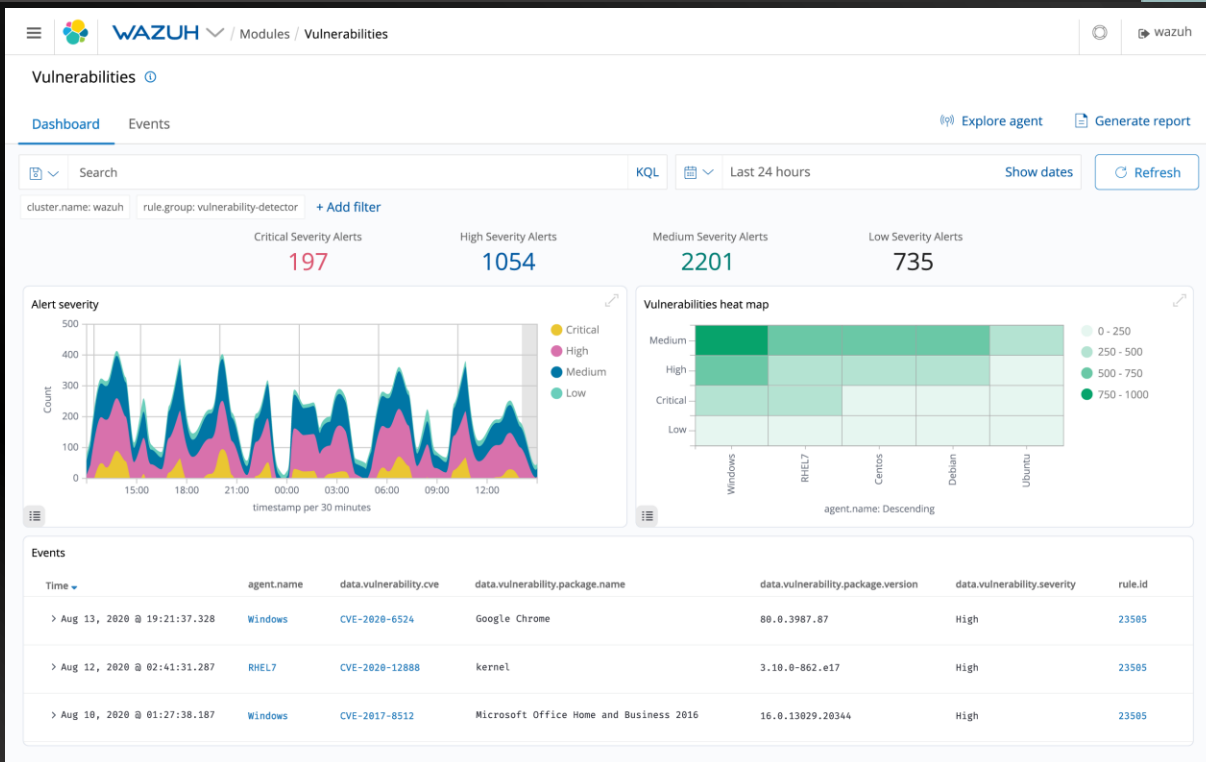
- Not sure... But this one has been around possibly longer than anyone else
- Used for years on Linux systems for Rootkit detection
- Monitors key files and logs
- Now adding in anti-malware features and response
- Can be intimidating to get started, not all that bad
- "Worst selling security book in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

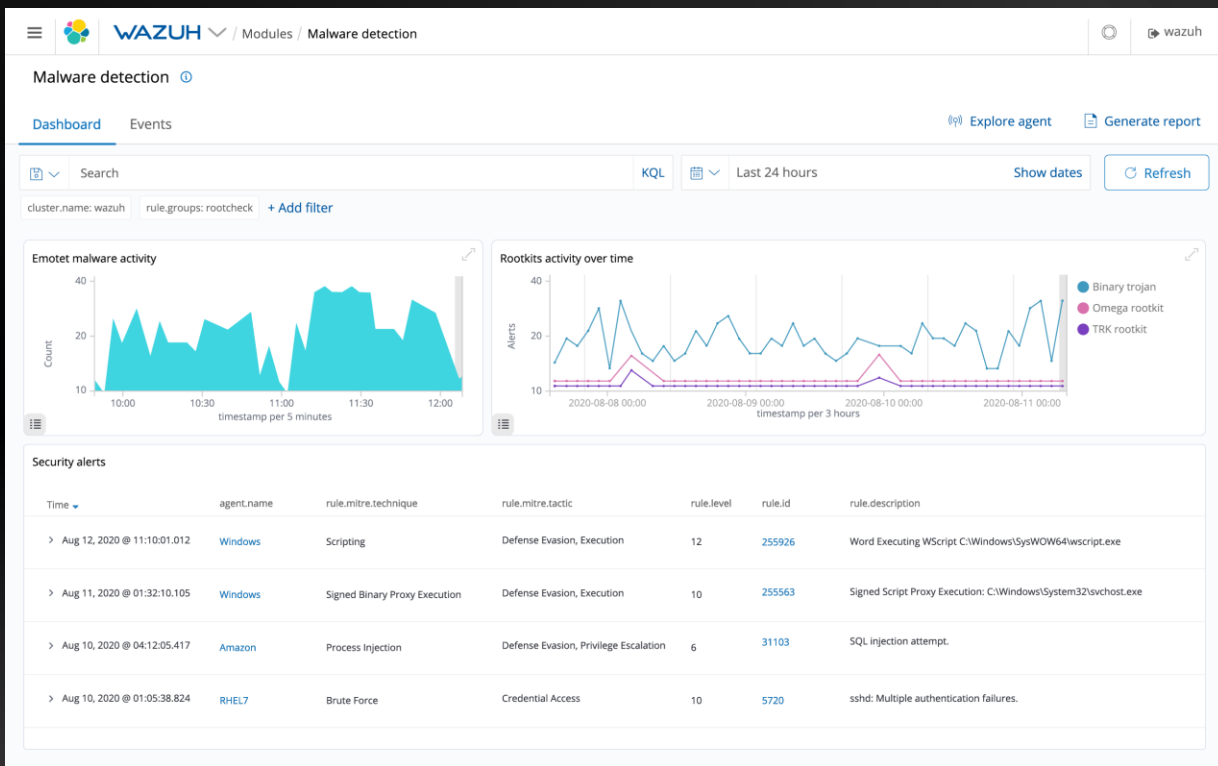


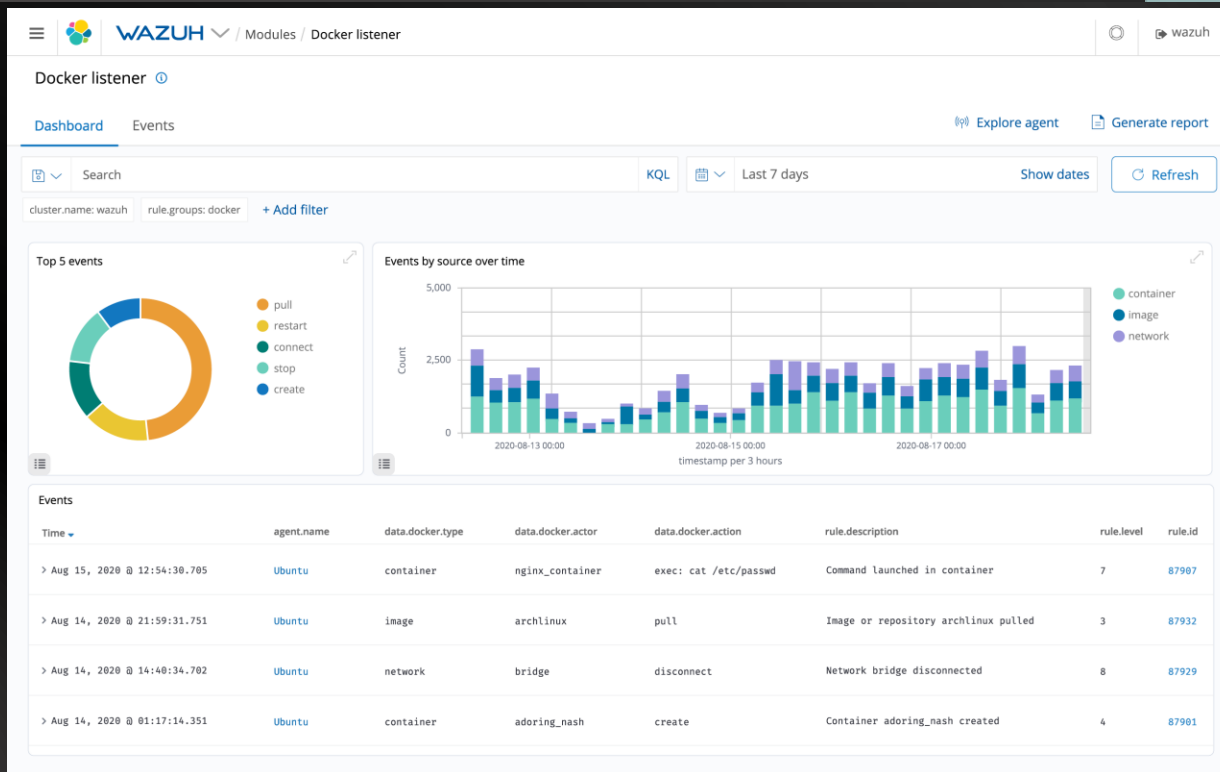
- Originally one of the more badass inventory systems
- Loved the query language across systems
- Full stack EDR
- Super easy to install, multiple agents
- Data feeds to an ELK stack... Because everything does...
- Easily one of the most asked about tools in my classes
- Just don't want to run a full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



I may be pronouncing it wrong

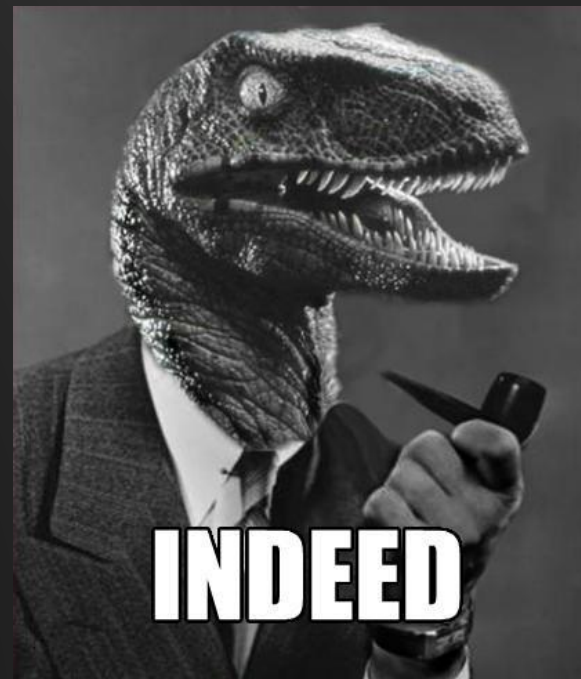








- This is the one we use in my classes
- Setup to pulling data is very, very quick
- Standalone agent and server in one executable
- From the folks that brought us Rekall
- So... They kind of know what they are doing
- No detection and prevention capability
- Great way to complement existing AV/Protection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



© Black Hills Information Security | @BHInfoSecurity

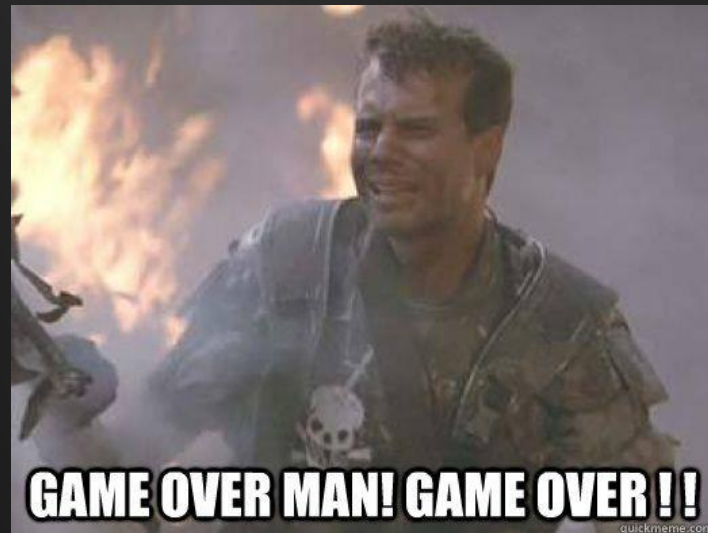




(Formerly Endgame)



- 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?



© Black Hills Information Security | @BHInfoSecurity





Easy Install



Fleet / Agents

Agents

Manage and deploy policy updates to a group of agents

Agents Enrollment tokens

Search

Showing 0 agents

Host	Status	Age
------	--------	-----

Add agent

Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.

Enroll in Fleet Run standalone

From the agent directory, run the appropriate command to install, enroll, and start an Elastic Agent. You can reuse these commands to set up agents on more than one host. Requires administrator privileges.

Linux, macOS

```
./elastic-agent install -f --kibana-url=http://localhost:5601 --enrollment-token=
```

Windows

```
.\elastic-agent.exe install -f --kibana-url=http://localhost:5601 --enrollment-token=
```

See the [Elastic Agent docs](#) for more instructions and options.

Cancel Continue

Beta release – Ingest M...



© Black Hills Information Security | @BHInfoSecurity





Out of the box... ~5 min



elastic Search Elastic

Security / Detections

Overview **Detections** Hosts Network Timelines Cases Administration

Search KQL Last 24 hours + Add filter

Showing 2 alerts | Selected 0 alerts | Take action | Select all 2 alerts

	@timestamp	Rule	Version	Method	Severity	Risk Score	event.module	event.action	event.category
<input type="checkbox"/>	Mar 4, 2021 @ 03:54:12.576	Malware Prevention Alert	2	query	high	73	endpoint	execution	malware intrusion_detection process
<input type="checkbox"/>	Mar 4, 2021 @ 03:49:12.321	Malware Prevention Alert	2	query	high	73	endpoint	execution	malware intrusion_detection process

Alert details

Message
Malware Prevention Alert

Summary **Table** JSON View

Filter by Field, Value, or Description...

<input type="checkbox"/>	file.Ext.code_signature	("trusted":false,"subject_name":"","exists":false,"status":"noSignature")
<input type="checkbox"/>	file.Ext.malware_classification.identifier	endpointpe-v4-model
<input type="checkbox"/>	file.Ext.malware_classification.score	0.9957315325737
<input type="checkbox"/>	file.Ext.malware_classification.threshold	0.62
<input type="checkbox"/>	file.Ext.malware_classification.version	4.0.3000
<input type="checkbox"/>	file.Ext.quarantine_path	C:\e\quarantine\90752e67598d6d0d4929f2b00502212417336a9f



© Black Hills Information Security | @BHInfoSecurity

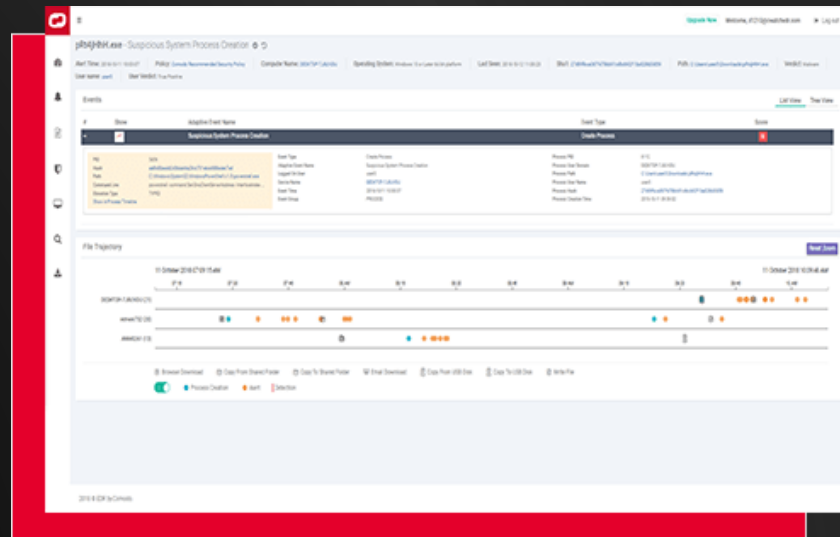




From Comodo



- 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...



Endpoint Security

Alerts	Investigate	Containment	Application Control	Valkyrie	Antivirus	Device Control
> EDR	4	Unusual Service Start	2020-08-26 11:34:30	ENDPOINT-WIN8	New	
> EDR	4	Unusual Cmd Execution	2020-08-26 04:13:29	ENDPOINT-WIN10	New	
> EDR	4	Unusual Service Start	2020-08-26 04:02:36	ENDPOINT-WIN10	New	
> EDR	4	Unusual Cmd Execution	2020-08-26 03:43:51	ENDPOINT-WIN10	New	
> EDR	4	Unusual Service Start	2020-08-26 03:28:53	ENDPOINT-WIN10	New	
> EDR	4	Unusual Service Start	2020-08-25 18:39:32	ENDPOINT-WIN10	New	
> EDR	4	Unusual Service Start	2020-08-25 16:43:59	ENDPOINT-WIN10	New	
▼ EDR	6	Suspicious System Process Creation	2020-08-24 11:40:30	ENDPOINT-WIN10	New	

Close Alert Add Suppression Rule Report False Positive

Component: EDR

Device Name: ENDPOINT-WIN10

Event Type: Create Process

Event Time: 2020-08-24 11:39:20

```
{
  "adaptive_event_type": "Suspicious System Process Creation",
  "base_event_type": "Create Process",
  "child_process_command_line": "powershell.exe -ExecutionPolicy Bypass -C Clear-History;Clear",
  "child_process_elevation_type": "TYPE1",
  "child_process_hash": "36c5d1203b2eaf251bae61c00690fffb17fddc87",
  "child_process_path": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",
  "child_process_pid": 7932,
  "child_process_verdict": "Safe",
  "component": "EDR",
  "device_name": "ENDPOINT-WIN10",
  "event_time": "2020-08-24 11:39:20.166",
  "logged_on_user": "Administrator@ENDPOINT-WIN10",
  "process_creation_time": "2020-08-24 11:19:42.142",
  "process_hash": "06e82f76cff66568b4e8bae9571fe81cf64047d3",
  "process_parent_tree": [ ... ],
  "process_path": "C:\\Users\\Public\\splunkd.exe",
  "process_user_domain": "ENDPOINT-WIN10",
  "process_user_name": "Administrator@ENDPOINT-WIN10",
  "process_verdict": "Absent"
}
```



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"
```



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!



© Black Hills Information Security | @BHInfoSecurity





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



© Black Hills Information Security | @BHInfoSecurity



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



© Black Hills Information Security | @BHInfoSecurity



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



© Black Hills Information Security | @BHInfoSecurity



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



© Black Hills Information Security | @BHInfoSecurity

Questions?



© Black Hills Information Security | @BHInfoSecurity