

Matt Scheurer *presents*

★ Rocking with ★

 **TANIUM**™

THREAT RESPONSE

Introducing: Matt Scheurer

Matt works for a big well-known organization...



As an Assistant Vice President (AVP) of Computer Security and Incident Response (IR). However, he has many years of hands-on technical experience, including Digital Forensics & Incident Response (DFIR).

He is also a Podcast Host for

ThreatReel

<https://threatreel.com>

Follow / contact Matt:



<https://www.linkedin.com/in/mattscheurer>



<https://twitter.com/c3rkah>

Where Matt volunteers...

Matt is an Official



Advocate

<https://www.hackingisnotacrime.org>

He is also a



Women's Security Alliance
(WomSA) Technical Mentor

<https://www.womsa.org>

Disclaimer!

Yes, I have a day job.
However...

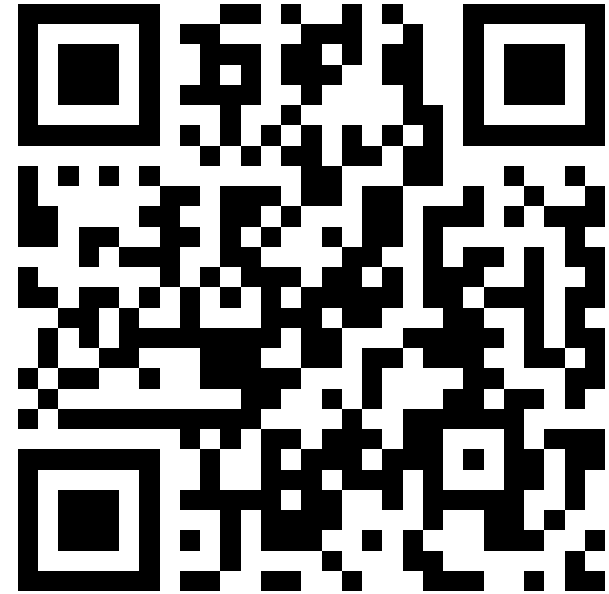
Opinions expressed are
based solely on my own
independent security
research and do not
express or reflect the views
or opinions of my employer.



The YouTube Video

I recorded a video with
Tanium for their
YouTube channel back
in July titled:

**“Threat Response In
Real Life - Tanium Tech
Talks #66”**



<https://youtu.be/kjf-fBrSzVA>

The YouTube Video Game Plan

Showcase the “**Interact**” and “**Threat Response**” Modules

- Alerts' details and MITRE ATT&CK techniques
- Live Endpoints connections
- Browsing the File System in Tanium
- Saved Evidence (Saving & Retrieving)
- Quarantining an endpoint
- Live Response
- Beyond file names: magic numbers & hashes
- Interact questions and Threat Hunting at scale
- Determining if file execution happened

My Plan for Today

- Rather than rehash a video that everyone here can (and I hope does) watch online
 - I'd rather use this time to show some of the behind-the-scenes effort that went into making the recording
- The demo environment
 - Unfortunately there were no **Alerts** in **Threat Response**
 - So I created my own **Insider Threat** storyboard scenarios
 - Good thing I'm a skilled **Purple Teamer!** ;)

Impair Defenses

I authored and executed a script to completely disable the Windows firewall using the following code...

```
netsh firewall set opmode mode=disable profile=all
```


Living off the Land

Sweet! I found a “secret-webapp” folder on the Dev box in the demo environment. I can build this into my data exfiltration scenario!

```
PS C:\> \Users\cgibson\secret-webapp\_
```

Evasion Technique: Encoding

Code snippet from another demo script I created, leveraging PowerShell using an encoded command to make detection more difficult...

```
powershell.exe -NoProfile -NonInteractive -  
ExecutionPolicy Bypass -EncodedCommand  
JABFAG4AdgA6AEMATwBNAFAAVQBUAEUAUgBOAEEATQBFAA== | Out-  
File -FilePath "$home\secret-webapp\1337.txt" -Append
```

Fully Decoded

Here is what that same PowerShell command looks like fully decoded...

```
powershell.exe -NoProfile -NonInteractive -  
ExecutionPolicy Bypass -EncodedCommand  
$Env:COMPUTERNAME | Out-File -FilePath "$home\secret-  
webapp\1337.txt" -Append
```

More Post-Exploitation Details

Here is the decoded format of all the other encoded commands I used to populate the secrets (1337.txt) in the exfiltration example...

```
$Env:USERDOMAIN  
Get-NetIPConfiguration  
Get-Localuser | Select * | Format-List -Property *  
whoami /priv  
net user /domain  
net group "Domain Admins" /domain
```

File Execution Demo Playbook

- 1) Create a “**badware.exe**” file.
 - Doesn’t really do anything (It’s only a demo)
- 2) Copy to “C:\Users\cgibson\AppData\Local”.
- 3) Rename the copied file to “**goodware.exe**”.
- 4) Run the “**goodware.exe**” file.
 - Finding it in Tanium makes for a good demo!

Hilarious Outtakes

Oh those unforgettable
face-palm moments...

Let's all have a good
laugh about them
together!



The Planning Meeting



Hey Matt, I like to keep our videos between 15 - 20 minutes in length. That looks like a lot of material! Maybe we should split this up into a 2-part video series. What do you think?

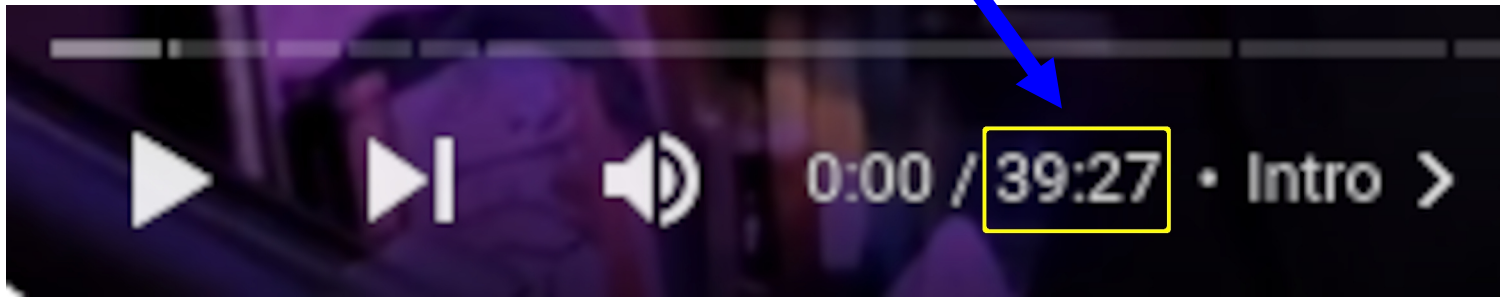
Timing is Everything!

Oh, I might have to maintain a brisk pace, but I'm pretty sure I can get through all of the demos in about 20-minutes. No problem!

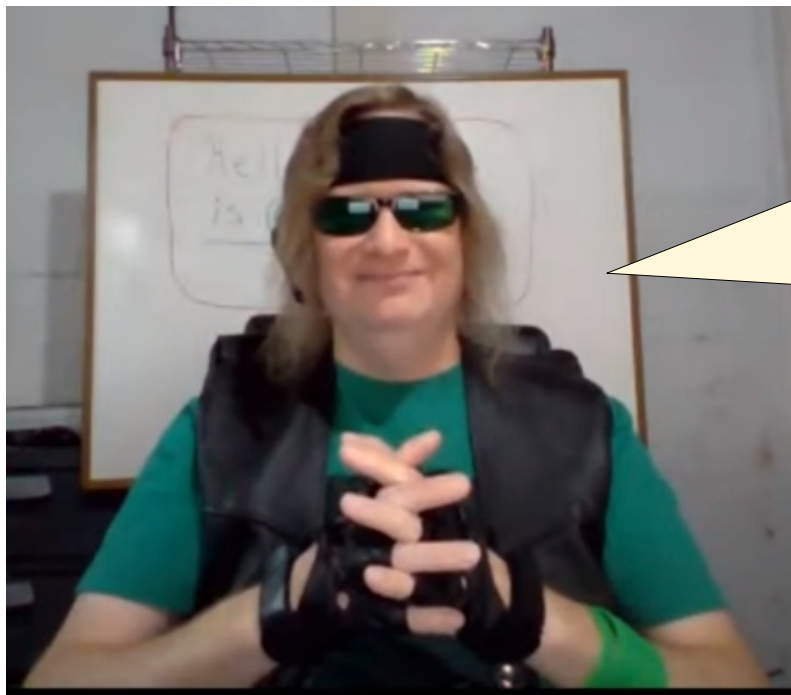


Actual Video Runtime...

Oops!



“Live Endpoints” query demo



Showing how Tanium helps users determine if file execution occurred or not should make for a really cool demo!

The epic “Demo Fail”



Dang it, why
isn't this
working now?

Later that day...






Hey Ashley, I think I know what I did wrong earlier... Any chance we can rerecord that last demo again?

Always Remember...

If at first you don't succeed, you're running about average.

- And -

All is well that ends well!

T..	I...	Start Time (UTC) ↓	Process Path	PID	User	Command Line
■	 	2023-07-21 18:43:44.777	C:\Users\cgibson\AppData\Local\goodware.exe	 7488	cgibson	"C:\Users\cgibson\AppData\Local\goodware.exe"

Another Lesson Learned...



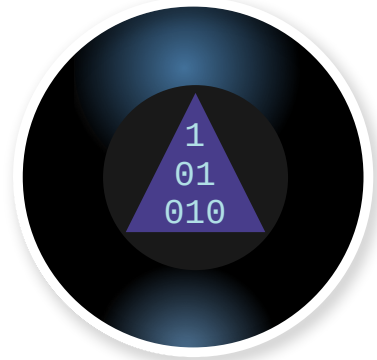
Pro-Tip: If you want to perform a demo of "File Execution"...

Make sure that you remember to actually execute the file!

Questions



Who?
What?
When?
Where?
Why?
How?



Thank you for attending!



Rocking with



THREAT RESPONSE
