Matt Scheurer *presents...*

Picky Purple Teamers pick

Black Hat 2023

Hosted by: ATTACKIQ®

About Me

I work for a big well-known organization...

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

I am also a Podcast Host for

ThreatReel

https://threatreel.com

Follow / contact Matt:

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

https://twitter.com/c3rkah

Where I volunteer...

I am an Official

HACKING IS NOT A CRIME

Advocate

https://www.hackingisnotacrime.org

I am also a

WOMSA
Empowering Women in Cybersecurity

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.

While my primary focus is DFIR

I’ve given lots of Talks

- And I’m renowned for
  - Technical Deep Dives
  - Live Demos
  - Plus Over-the-Top Theatrics

Many of those talks went purple

- Phishing Forensics
  - Is it just suspicious or is it malicious?
- Lend me your IR's!
- Learn by Doing
  - Improve by showing & telling
- Why Script Kiddies Succeed
- Stupid Cyber Criminal Tricks
  - And How to Combat Them
- Active Defense
  - Helping Threat Actors Hack Themselves
- AppSec Primer
- Exploiting Web APIs

Why those talks were popular

- The aforementioned list of talks were immensely popular
- In large part, because they were based on real attacks
- That’s also what MITRE ATT&CK is based on!

How MITRE defines ATT&CK

ATT&CK®

"*MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.*"

Source: https://attack.mitre.org/

However,

- I’m a big proponent of **K.I.S.S**.

However,

- I’m a big proponent of **K.I.S.S**.
- No, not that KISS...

However,

- I’m a big proponent of **K.I.S.S**.
- No, not that KISS...
  - Though, admittedly, I do like their music!

However,

- I’m a big proponent of **K.I.S.S**.
- No, not that KISS...
  - Though, admittedly, I do like their music!
- The Acronym...

However,

- I’m a big proponent of **K.I.S.S**.
- No, not that KISS...
  - Though, admittedly, I do like their music!
- The Acronym...
  - “*Keep It Simple, Stupid!*”

How Matt defines ATT&CK

The MITRE ATT&CK framework maps out the real-world **Tactics**, **Techniques**, and **Procedures** (TTPs) used by offensive security professionals and cyber criminals alike!

But wait, there's more!

- Tech defenders can also use the MITRE ATT&CK mappings to harden their own defenses
- Which is the very essence of having a **Threat-Informed Defense** (**TID**) strategy

Conclusions

- Purple team to identify and remediate the vulnerabilities in your enterprise environment

Conclusions

- Purple team to identify and remediate the vulnerabilities in your enterprise environment
  - Testing your monitoring, detection, prevention, and response capabilities along the way

Conclusions

- Purple team to identify and remediate the vulnerabilities in your enterprise environment
  - Testing your monitoring, detection, prevention, and response capabilities along the way
  - Before the cyber criminals do!

Conclusions

- Purple team to identify and remediate the vulnerabilities in your enterprise environment
  - Testing your monitoring, detection, prevention, and response capabilities along the way
  - Before the cyber criminals do!
- **TID** helps organizations improve their security posture and security maturity

Conclusions

- Purple team to identify and remediate the vulnerabilities in your enterprise environment
  - Testing your monitoring, detection, prevention, and response capabilities along the way
  - Before the cyber criminals do!
- **TID** helps organizations improve their security posture and security maturity
  - Based on real-world threats!

Questions

Who?

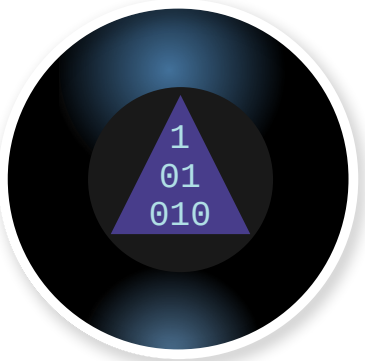
What?

When?

Where?

Why?

How?



Thank you for attending!

Picky Purple Teamers pick

Black Hat 2023

Hosted by: ATTACKIQ®