Adversarial Thinking

Using Attack Path Mapping to Develop Your ICS Security Roadmap

Hudson Bush

RST

RSTCON
Savannah, GA 2024

This television series is inspired by true events.
Some of the characters, names, businesses,
incidents and certain locations and events have
been fictionalized for dramatization purposes.
Any similarity to the name, character or history
of any person is entirely coincidental and unintentional.

NETFLIX

NARCOS

```
PS > Get-User | Select Name, Alias, Location, *Company, Role

Name                                : Hudson Bush
Alias                               : @HomeBrewedSec
Location                            : Chattanooga, TN
Company                             : Seguri
Role                                : Practice Lead - Security Operations
SpeakingOnBehalfOfCompany           : FALSE
```

How do teams typically prioritize?

Historical Bias

“I’ve never done it that way before.”

“This is how we’ve always done it”.

“This is how I’ve always done it”.

Fire Fighting

“This vulnerability is in the news.”

“The board said we had to.”

“We got breached.”

Random

“It sounded fun”

“It sparked joy”

"Our systems are air-gapped, so we're safe."

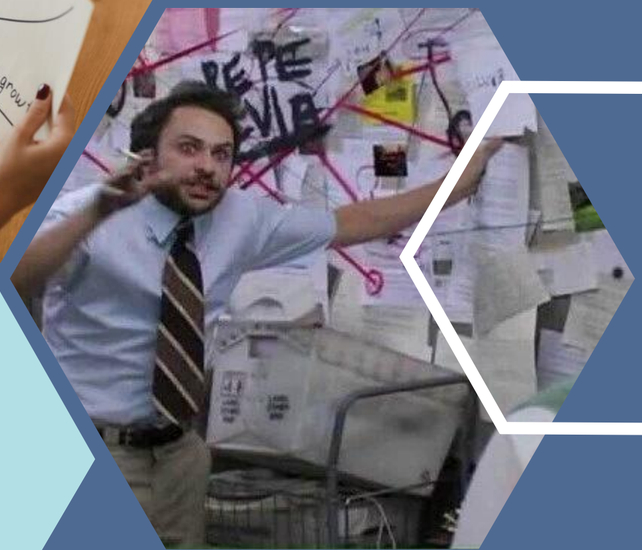
Compliance

“(Insert standards body here) said we had to.”

“Insurance said we had to.

“It was on a customer questionnaire.”

Why Attack Path Mapping?



“Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win.”

-John Lambert
@JohnLaTwC

Why Attack Path Mapping?

Shift to Graph Thinking

Aligns defender mindset with attacker strategies, providing a comprehensive view of interconnected attack vectors.

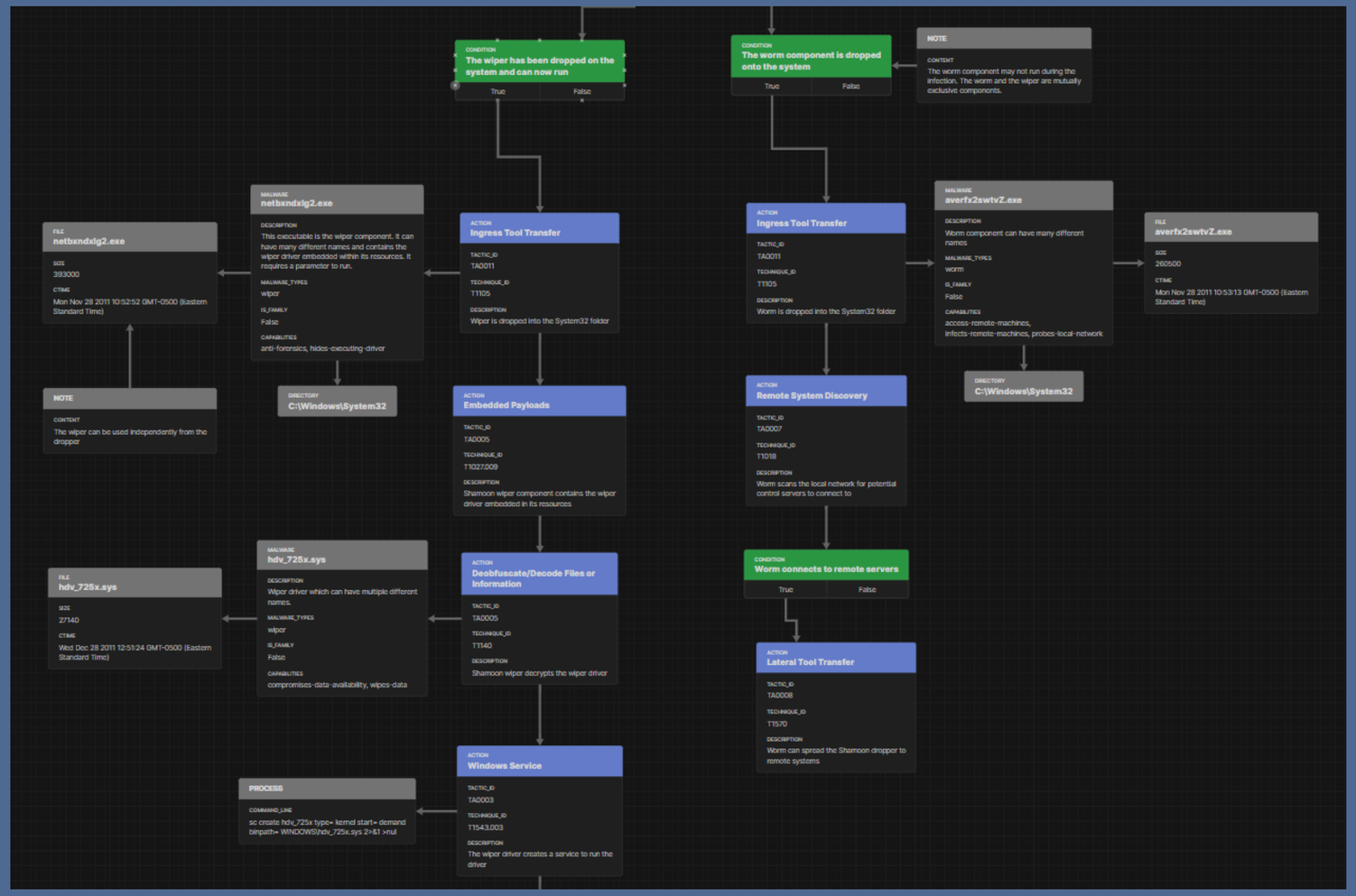
Data-Driven Prioritization

Enables logical, bias-free decision-making for implementing and prioritizing security controls based on actual attack paths.

Enhanced Communication

Creates visual representations ("pretty graphs") to effectively convey complex security landscapes to both technical and non-technical stakeholders.

Attack Path Mapping



MITRE Attack Flow Builder

Prerequisites

Crown Jewel Analysis

You need to know what you're protecting

Asset Inventory

You need to know what you're protecting

Define your ICS Perimeter

Jump boxes, OT DMZ, (hopefully not) internet connected systems

The Process

1. Brainstorm Attack Paths

A good place to start is by "journaling" all the things that scare you.

Write down every conceivable attack path, no matter how small

Include both technical and non-technical vectors

2. Map to MITRE ATT&CK for ICS

Correlate attack paths with specific ATT&CK techniques

Cluster similar technique under their respective tactics

Add paths as necessary based on missing techniques (focus heavily on initial access)

3. Assess Current Defenses

Use MITRE D3FEND to map existing security controls

Identify gaps in your current defense strategy

Add additional attack paths as you identify them

4. Get Outside Perspectives

Work with other teams to challenge your expectations

5. Present!

Create multiple versions:

Internal only

Security Leadership

IT/Other Stakeholders

Execs

Lessons Learned

- Be prepared to challenge your biases of your attack surface
- Don’t dismiss attack vectors just because you don’t think they’ll lead anywhere
- Don’t be afraid to remove attack paths if they don’t lead to results

tl;dr

(Too long; didn't read)

- Use all the techniques available to you to conceptualize your attack surface (because the attackers sure are)
- Use logic, not habit or bias to decide what controls to implement and prioritize
- Make pretty graphs

Resources

Attack Flow Builder: https://center-for-threat-informed-defense.github.io/attack-flow/ui/

Good intro to Attack Flow Builder: https://medium.com/mitre-engenuity/attack-flow-make-threat-informed-decisions-based-on-steps-in-a-cyber-attack-aaa54767282b

5 Critical Controls: https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

The Defender's Mindset: https://medium.com/@johnlatwc/defenders-mindset-319854d10aaa

Seguri

Tailored Cyber Defense Solutions

Slides at HomeBrewedSec.com/talks

@HomeBrewedSec

@Seguri_io