



A SIEM Engineer's Guide to Threat Modeling

Mark Orlando

SANS SIEM Summit

October 7, 2019

About Me

- 17 years in secops
- DoD, FedCiv, Executive Branch, MSSP, MDR
- CTO, Raytheon Cyber & Founder of Bionic

 @markaorlando



Early Days of Data Collection



You.

The Few Alerts
You Can Get

Data Collection Today



You.

Very Important
Security Data

Enter Content Development

Raw Data



Stock SIEM



SIEM Engineer



DATA

INFORMATION

Let's Jump In! Right...?



"Ooh, look...So much interesting data!"

SANS SIEM Summit 2019

@markaorlando

Threat Modeling is Already a Thing

Lots of different things, actually.

- Threat-centric
- System-centric
- Asset-centric

For our purposes, we want to steer away from surveys and complicated documentation

The Case for *Organizational* Threat Modeling

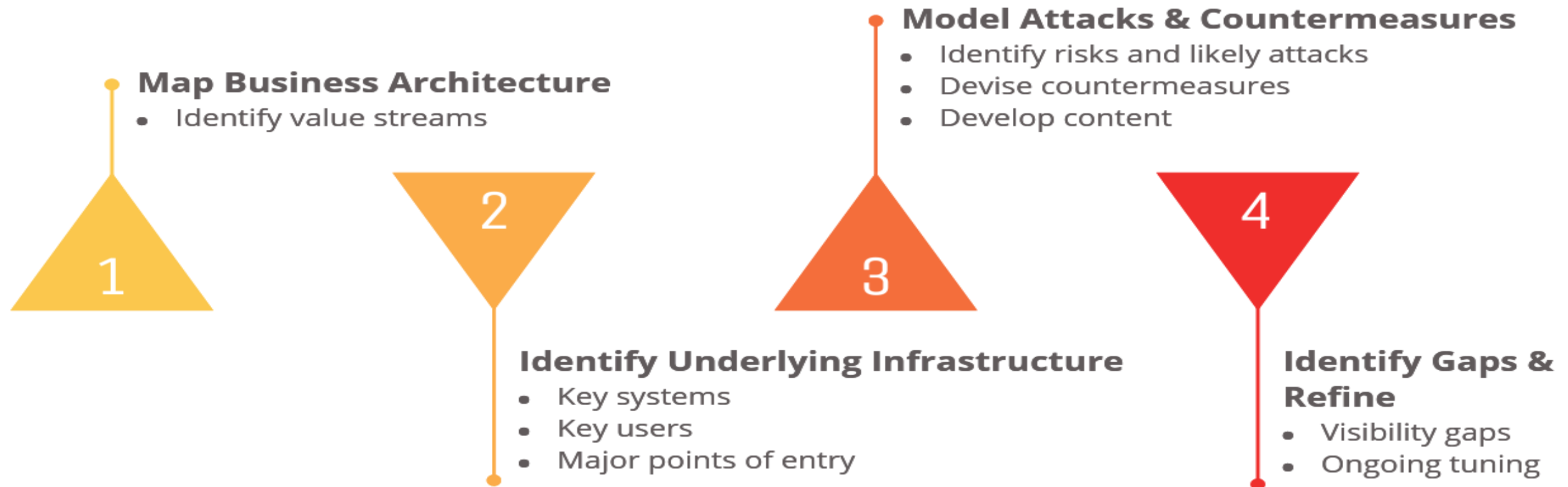
- Stakeholders tend not to care about the cool rules you're writing
- Transparent, measurable, business-aligned
- Can flow down to other models
- Helps identify risky (or at-risk) processes

Challenge: you won't know everything

4-Step Process

This can be another rabbit hole.

Best to stay high level and refine over time.



1. Mapping Business Value

Online Healthcare Marketplace

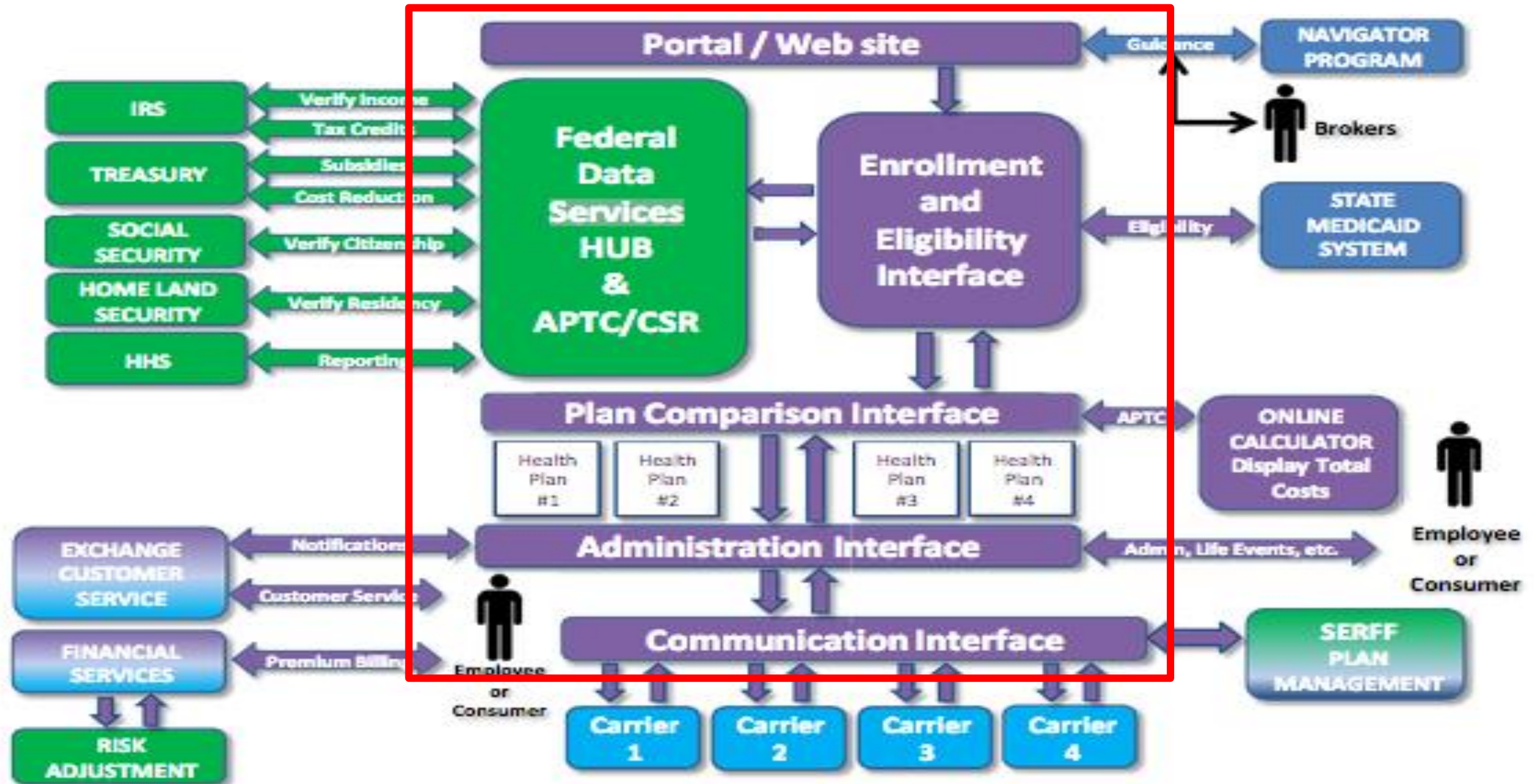
Element	Goal	Capability	Systems	Internal Users
Online enrollment	Zero-touch enrollment	Enrollment app available, back-end systems up, auth integration up	CDN, origin servers, third-party ID provider	Web admins, ID contractor(s)
State plan research	Up-to-date state data available	Integration w/ state exchanges	Web front end, state APIs	State liaisons, web admins
Small business option application	IRS connectivity, successful hand-off	Transparent integration w/IRS app process	SHOP app, IRS APIs	SHOP administrators, IRS liaison
Customer service (agent/broker)	<10 min wait time, first call resolution	Walk customers through app process, identify issues, receive complaints	Call routing system,	Customer service team, Tier 2 app support

1. Mapping Business Value

Online Healthcare Marketplace

Element	Goal	Capability	Systems	Internal Users
Online enrollment	Zero-touch enrollment	Enrollment app available, back-end systems up, auth integration up	CDN, origin servers, third-party ID provider	Web admins, ID contractor(s)
State plan research	Up-to-date state data available	Integration w/ state exchanges	Web front end, state APIs	State liaisons, web admins
Small business option application	IRS connectivity, successful hand-off	Transparent integration w/IRS app process	SHOP app, IRS APIs	SHOP administrators, IRS liaison
Customer service (agent/broker)	<10 min wait time, first call resolution	Walk customers through app process, identify issues, receive complaints	Call routing system,	Customer service team, Tier 2 app support

2. Identifying Infrastructure



2. Identifying Infrastructure

- Web browser (untrusted)
- API call (semi-trusted)
- Administrative access (trusted)
- Trust but verify

3. Model Attacks and Countermeasures

Exploit Public-Facing Application

The use of software, data, or commands to take advantage of a weakness in an Internet-facing computer system or program in order to cause unintended or unanticipated behavior.

The weakness in the system can be a bug, a glitch, or a design vulnerability. These applications are often websites, but can include databases (like SQL) ^[1], standard services

(like SMB ^[2] or SSH) as web servers and include [Exploitation](#)

For websites and d web-based vulnera

ID: T1190

Tactic: Initial Access

Platform: Linux, Windows, macOS

Spearphishing Link

Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this case, the malicious emails contain links.

Generally, the links will actively click or copy a website may compromise download applications for the email in the first directly with an email directly or verify the re

ID: T1192

Tactic: Initial Access

Platform: Windows, macOS, Linux

Data Sources: Packet capture, Web proxy, Email gateway, Detonation chamber, SSL/TLS inspection, DNS

External Remote Services

Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management](#) can also be used externally.

Adversaries may use remote services to initially access and/or persist within a network. ^[1] Access to [Valid Accounts](#) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network. Access to remote services may be used as part of [Redundant Access](#) during an operation.

ID: T1133

Tactic: Persistence, Initial Access

Platform: Windows

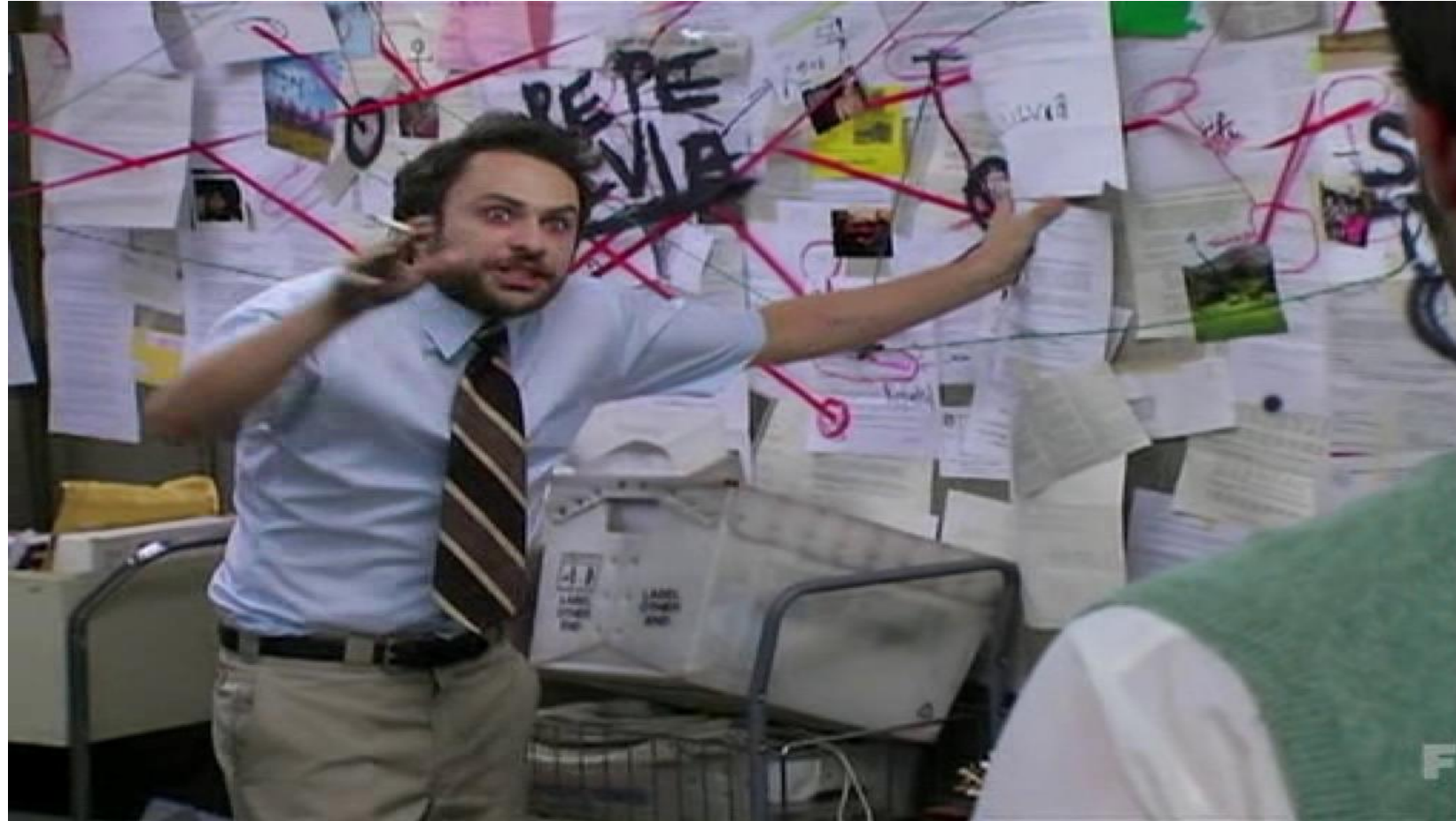
Permissions Required: User

Data Sources: Authentication logs

Contributors: Daniel Oakley; Travis Smith, Tripwire

Version: 2.0

<Record Scratch> What About Threat Intelligence?



Intelligence should inform your threat model and serve as
nexus for analyst focus/input

4. Measure and Iterate!

The screenshot displays the SANS SIEM Summit 2019 interface, which is a dashboard for managing and analyzing security incidents. The interface is divided into several sections:

- Header:** Includes the SANS logo, a search bar, and user information (Admin, 20 days left, Upgrade Subscription, Andrii Bezverkhyi).
- MITRE ATT&CK:** A section for viewing and managing MITRE ATT&CK techniques. It includes a table view, a kill chain view, and a flat view. The table view shows a list of techniques, including Brute Force, Credential Access, and Account Manipulation. The kill chain view shows a sequence of techniques used in an attack.
- SIEM Use Cases:** A section for viewing and managing SIEM use cases. It includes a table view, a kill chain view, and a flat view. The table view shows a list of use cases, including Windows Security Monitor - Basic and APT Framework - Basic.
- Techniques Grid:** A grid of technique cards, each representing a specific technique. The cards are categorized by tactic (Creds, Escalate, Evade) and include details such as the technique name, description, and number of use cases.

The interface is designed to be user-friendly and intuitive, allowing users to quickly find and manage security incidents. The use of color and icons helps to distinguish between different types of techniques and use cases. The overall layout is clean and professional, reflecting the high-quality standards of the SANS SIEM Summit 2019.

In Conclusion

- Ad hoc content development doesn't resonate with business owners
- Threat model should be an overlay for your use case framework(s)
- Show progress over time – sprints, goals, metrics

This is a good way to get out of the SOC and talk to system owners!

References

- “Organizational Threat Modeling” by Jack Whitsitt:
<http://www.energysec.org/wp-content/uploads/2016/05/Organizational-Threat-Modeling.pdf>
- “Cyber Threat Modeling: Survey, Assessment, and Representative Framework” by Bodeau, McCollum, and Fox
<https://www.mitre.org/publications/technical-papers/cyber-threat-modeling-survey-assessment-and-representative-framework>

Thank You!

mark@bionicyber.com

@markaorlando