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!”

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

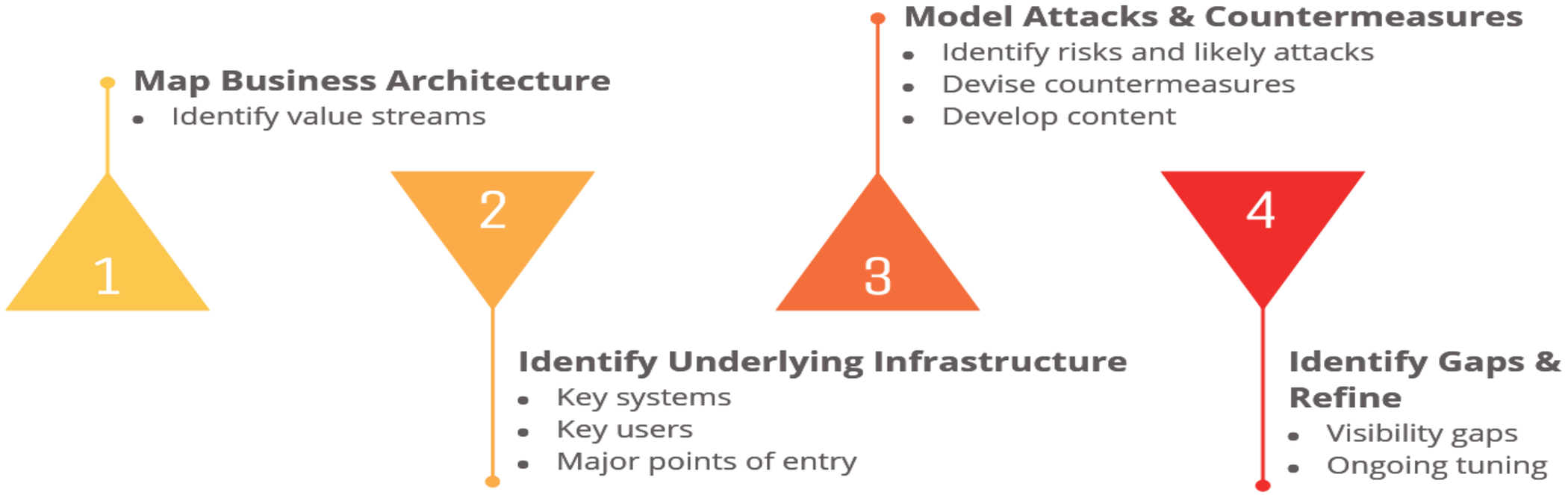
- Stakeholders tend not to care about the cool rules you're writing
- Transparent, measurable, business-aligned
- Can flow down to other models
- Helps identify risky (or at-risk) processes

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

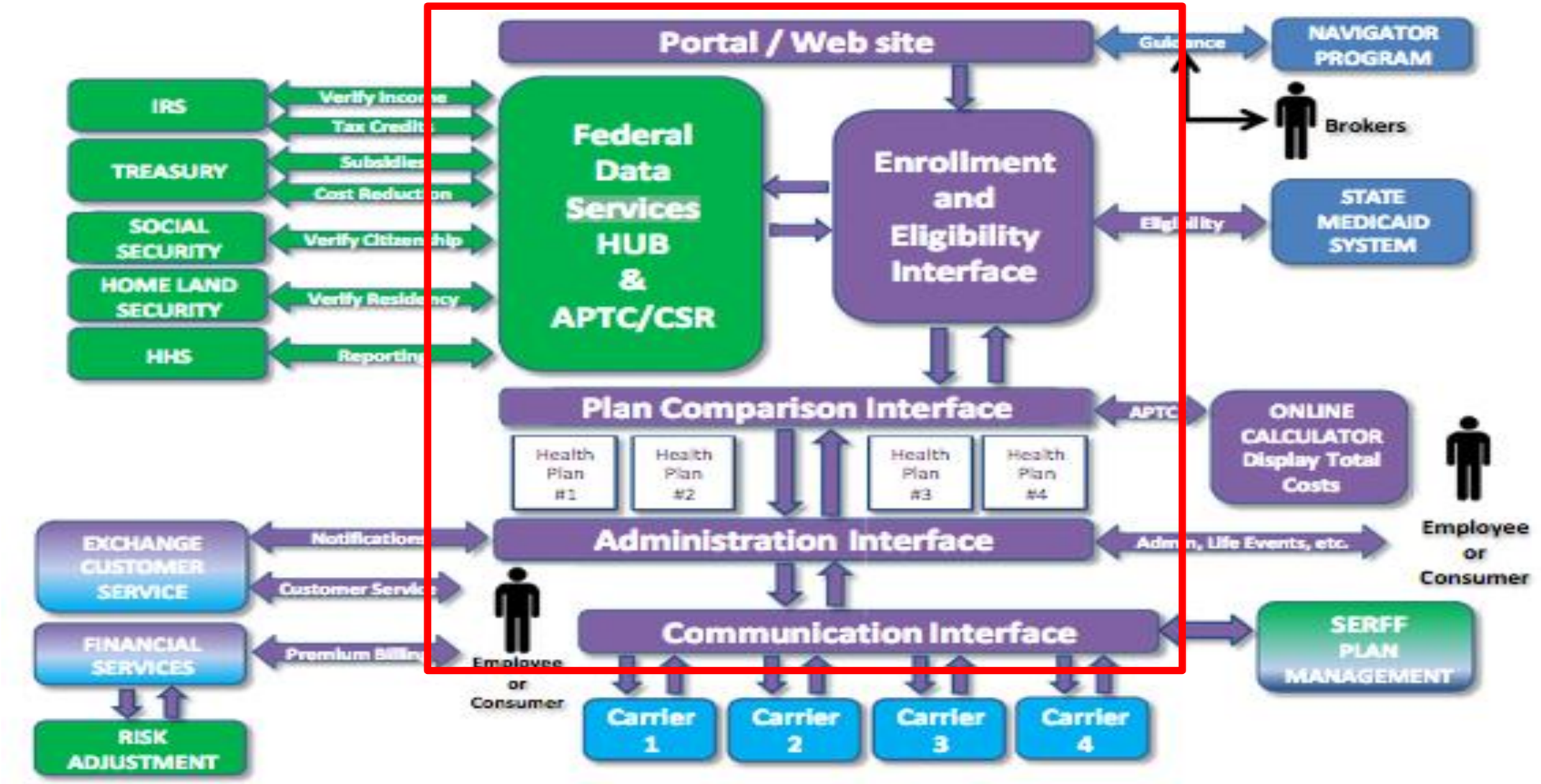
Element	Goal	Capability	Systems	Internal Users
Online enrollment	Zero-touch enrollment	Enrollment app available, back-end systems up, auth integration up	CDN, origin servers, third-party ID provider	Web admins, ID contractor(s)
State plan research	Up-to-date state data available	Integration w/ state 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

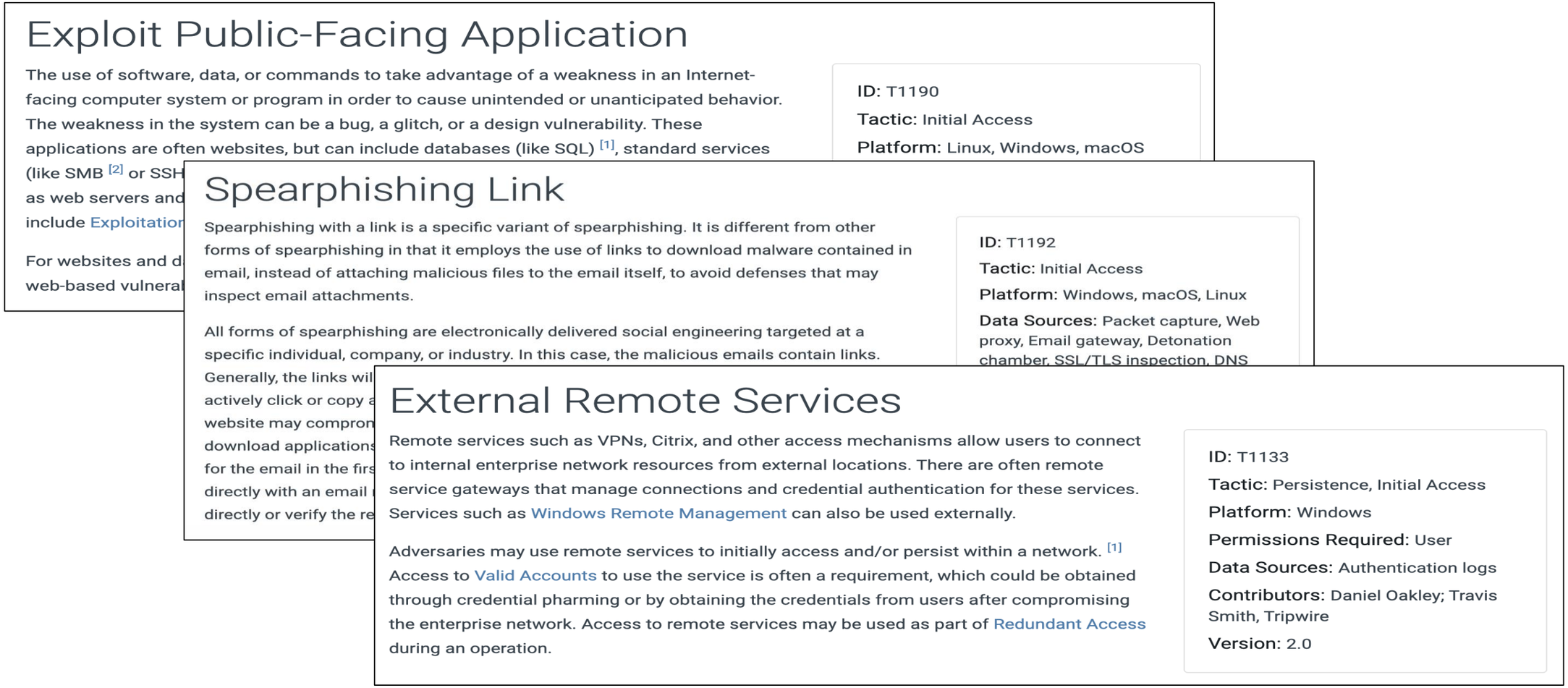


https://pt.slideshare.net/pcorsano/structure-of-us-healthcare/19

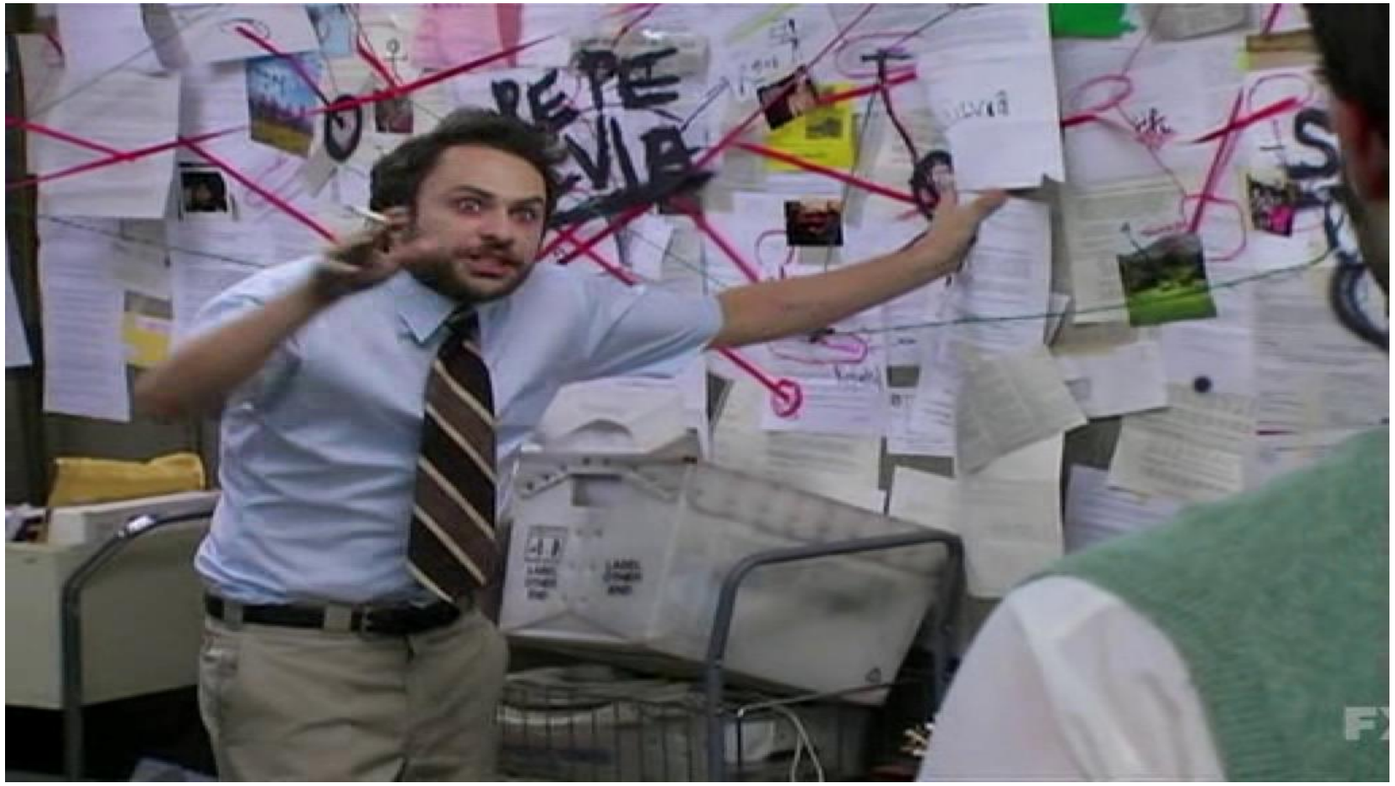
2. Identifying Infrastructure

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

3. Model Attacks and Countermeasures

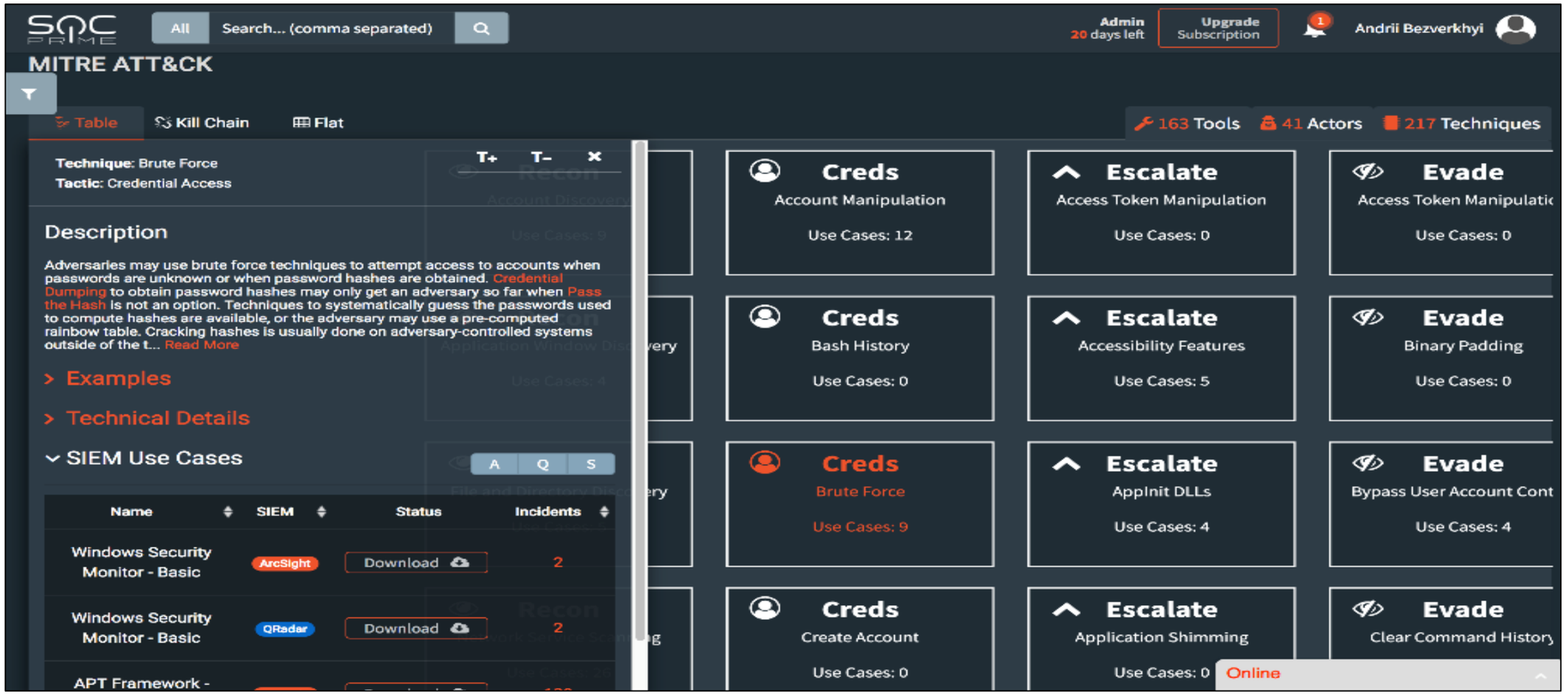


<Record Scratch>
What About Threat Intelligence?



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

4. Measure and Iterate!



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 Foxhttps://www.mitre.org/publications/technical-papers/cyber-threat-modeling-survey-assessment-and-representative-framework

Thank You!

mark@bioniccyber.com

@markaorlando