COMP 6448 - Week 6

Security Engineering Masterclass

ATT&CK Navigator:

- Multi Tactic techniques: By default, the navigator will show techniques that belong to more than one tactic.
- Presentation feature.
- https://mitre-attack.github.io/attack-navigator/enterprise/#

Applying Technique Intelligence to Defense - Making Recommendations:

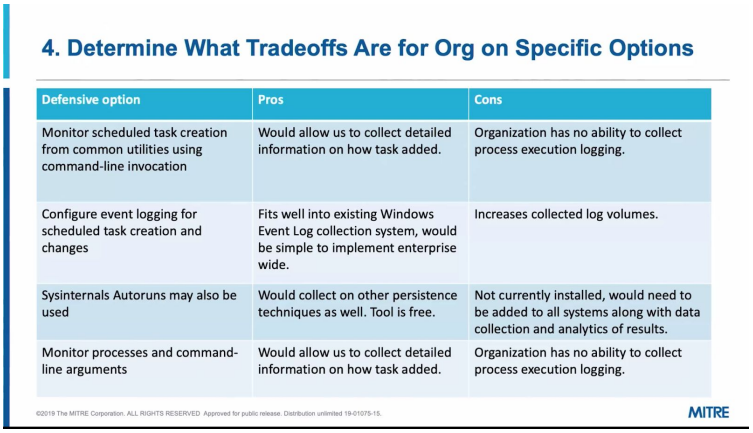
1. Determine priority techniques
- What data do you have
- What are your adversaries doing?
- What can the current tools cover?
- What can you see the red teamers doing.

- What specific procedures are being used for a given technique?

2. Research how techniques are being used
- E.g. A lot of user execution results from spear phishing

3. Research defensive options related to technique
- Research linked to from Technique pages
    - **Data sources**: What current visibility do we have
    - **Detection**: Data models - user analytics.
    - **Mitigations**: Incident response
- These can be found on the mitre page.

4. Research organizational capability/constraints
- What data sources, defenses, mitigation sare already collected/in place.
- What products are already deployed that may have additional capabilities.
- What changes will make operations difficult.
    - E.g. developers that run random binaries will be heavily inconvenienced from whitelisting certain binaries.



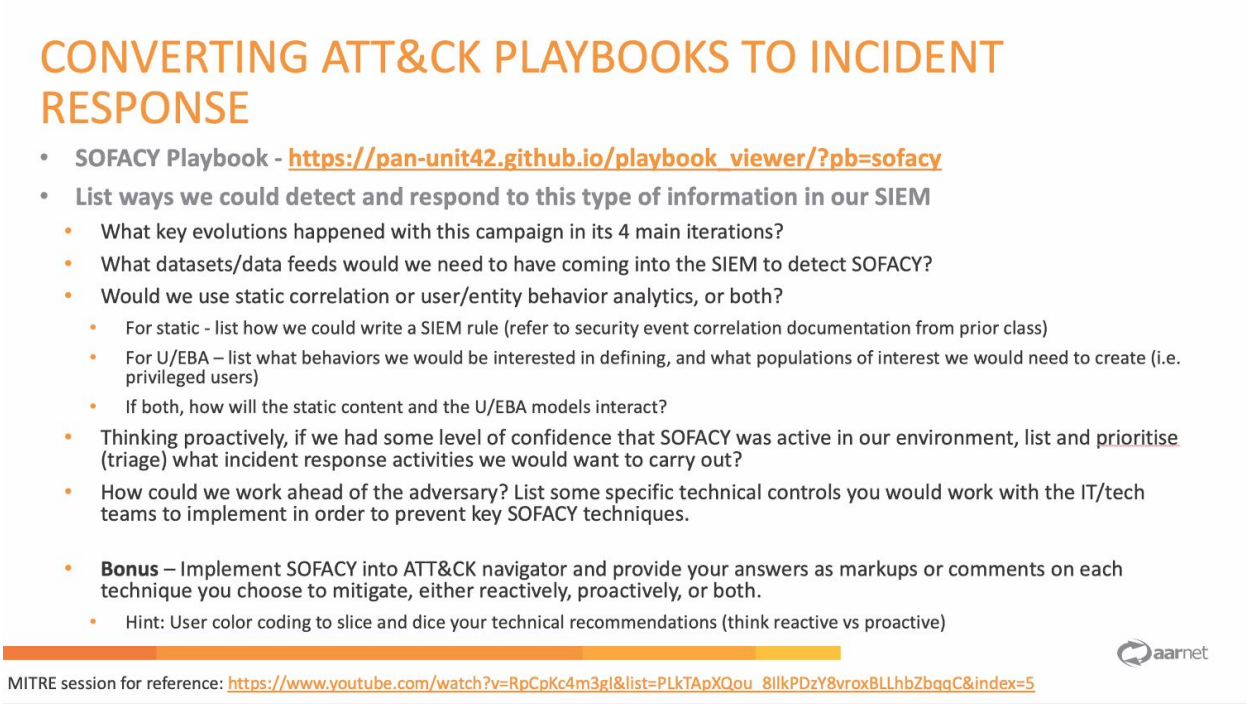
4. Determine What Tradeoffs Are for Org on Specific Options

Defensive option	Pros	Cons
Monitor scheduled task creation from common utilities using command-line invocation	Would allow us to collect detailed information on how task added.	Organization has no ability to collect process execution logging.
Configure event logging for scheduled task creation and changes	Fits well into existing Windows Event Log collection system, would be simple to implement enterprise wide.	Increases collected log volumes.
Sysinternals Autoruns may also be used	Would collect on other persistence techniques as well. Tool is free.	Not currently installed, would need to be added to all systems along with data collection and analytics of results.
Monitor processes and command-line arguments	Would allow us to collect detailed information on how task added.	Organization has no ability to collect process execution logging.

MITRE

5. Recommendations

- Different types:
    - Technical
        - E.g. collect a new data source, write detection/analytic from existing data
    - Policy changes
        - Technical or human.
        - E.g. user training
    - Accept risk
        - Undetectable
        - Mitigation not worth the trade off.



Evolutions:

- What techniques stay the same and which ones evolve?
- If they tend to change a lot, there is an intel person and is highly motivated/funded.
- If it's constantly changing, then the incident response team also has to move quickly to stop them.

Static correlation:

- If I were to build rule sets, what data would I need? What do I need to build static rules?
- Static can only influence the data model.

Proactive Thinking:

- If you knew something would happen, what technical controls would you put in, in advance?

Working ahead:

- What common techniques could we do to make it much harder for the adversary

Word doc: due 12 Jul 2 pm