(please don't do these)

HOW TO ~~ATT&CK~~

Your ATT&CK Program

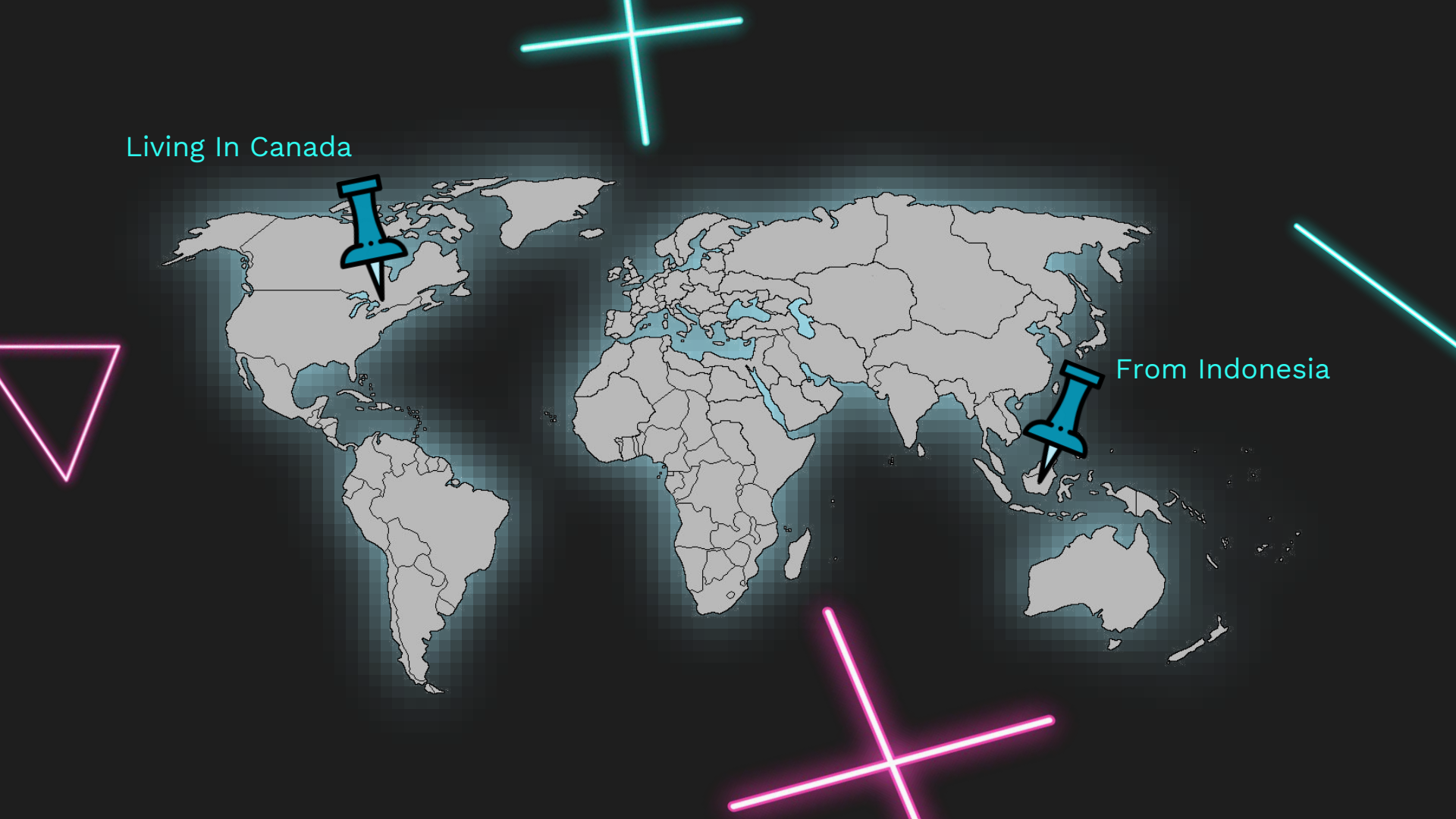
@tas_kmanager

Mangatas Tondang

Threat Hunting, Threat Intel and IR

@ Major Canadian Telco

Music and Astrophotography when AFK


Living In Canada
From Indonesia

Disclaimer

The views and opinions expressed in this presentation are those of the presenter and does not represent his employer or organization views

SIX COMMON MISTAKES

MADE WHEN APPLYING ATT&CK IN A SECURITY ORGANIZATION

EXPRESS STYLE

These are real common mistakes (from personal and community experience) made when applying ATT&CK in a security organization

Treating Everything As Equal

01 Treating Everything As Equal

Very first problem you will face when deploying ATT&CK, is *not all things in the framework are equal*

Treat everything differently:

- Tactics (e.g. discovery vs exfiltration)
- Techniques (e.g. PowerShell vs account creation)
- Log sources (e.g. AV logs vs Firewall logs)
- Detection (e.g. Kerberoasting vs Mshta)
- Mitigation (e.g. EDR vs IPS)

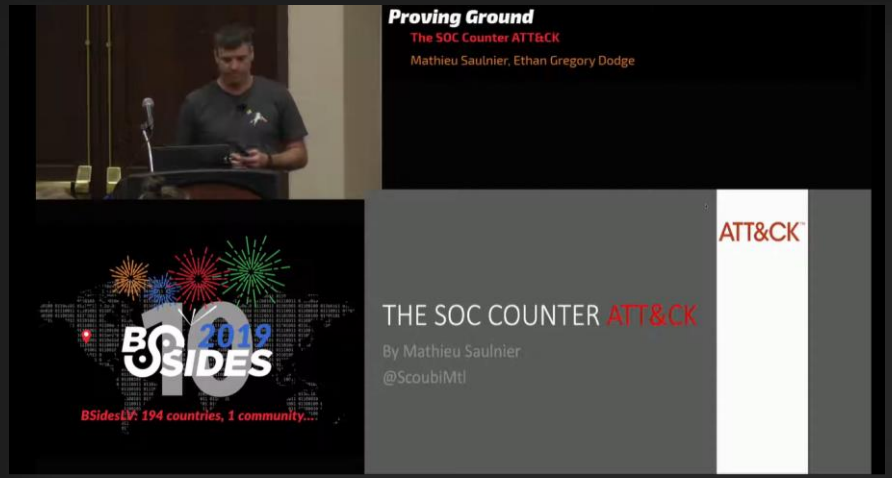
Planning and Prioritization are necessary before starting an ATT&CK program!

Resource

Planning and Prioritization

This presentation by @ScoubiMtl can help you on how to plan and prioritize an ATT&CK program

https://www.youtube.com/watch?v=j8MZJ1xU-3k



Only Starting From ATT&CK

02 Only Starting From ATT&CK

Starting From ATT&CK

Ending with ATT&CK

Brainstorming Ideas? Where to Get Them From?

Resource

Twitter
Reddit
Blog (Medium, etc.)
Blue Team channel (Discord, Slack, etc.)
Red Team channel (Discord, Slack, etc.)
Conference presentations
Conference white papers
Offensive tools GitHub repository
Open source detection GitHub repository
CVEs POC
CTI Report
Risk Assessment Report
Hypothesis

ATT&CK Only For Detection

03 ATT&CK Only For Detection

ATT&CK can also be used for lot of other things other than detection!

Visibility or Gap Analysis
- Logging, Tools, People

Planning and Prioritization
- @ScoubiMtl's SOC Counter Attack Presentation on Section 01

Tools Acquisition
- Via ATT&CK Evals - https://attackevals.mitre-engenuity.org/
- @digitoktav's Leverage Endpoint Visibility with MITRE ATT&CK Presentation

Training and Procedure Development
- Difficult TTPs require advanced knowledge and proper training
- Difficult TTPs will also require extensive Incident Response procedure
- Section 05 will show tools that you can use

Hypothetical ATT&CK Detection

04 Hypothetical ATT&CK Detection

Do not assume that the detection will works perfectly 100% of the time

Things will go wrong, eventually:

- SysAdmin doing SysAdmin stuff
- Company acquisition
- Onboarding new server
- Technology update/upgrade (SIEM, Log Source, etc.)

How can you be sure the rules are working without continuously testing them?

04 Hypothetical ATT&CK Detection

To ensure functionality of the rule and the whole detection pipeline (Event Forwarding, Parsing, Log Source Availability, Data Quality, Alerting, Ticketing, etc.) are working properly

Multiple ways to test

- Manual (emulate TTPs on production machine)
- Automated (Caldera, ART, RTA, METTA, or paid solutions)
- Penetration Testing and Red Team engagements
- Purple Teaming exercises

Resource

Test… Test… 1…2…3…

RTA
https://github.com/endgameinc/RTA
ART
https://github.com/redcanaryco/atomic-red-team
METTA
https://github.com/uber-common/metta
CALDERA – More extensive
https://github.com/mitre/caldera
VECTR – To track Red and Purple Teaming Results
https://github.com/SecurityRiskAdvisors/VECTR

ATT&CK But No DEFENSE

05 ATT&CK But No DEFENSE

Detection is one part,
Responding is another part!

Detection developer often forgot that not everyone in the Security organization is as knowledgeable as them.

Equip the IR and SOC people with detailed information and documentation!

- Context of the attack, what's the goal and how the attacker achieve it
- How is the detection working
- What information need to be gathered to validate the alert
- What are the next steps need to be taken
- What are some known false positive (also related to organizational awareness)

Resource

Tools to Document Better?

You need to understand the TTP and your environment first!

Use these tools to create a standardized format, fill with relevant information
ps: you can always adjust and modify it to your org needs

Incident Response
- https://atc-project.github.io/atc-react/

Documentation
- https://github.com/palantir/alerting-detection-strategy-framework

Underselling Your ATT&CK Program

06 Underselling Your ATT&CK Program

At the end of the day, if all your progress and coverage are not presented to management, it doesn't means much!

Why presenting metrics and statistic is important:

- Shows value (progress and coverage)
- Shows gaps
- Shows current plan and develop future plan
- Determines where and what additional resource are needed

You can use these tools to show progress to management

- ATT&CK Navigator - https://mitre-attack.github.io/attack-navigator/enterprise/
- DETT&CT - https://github.com/rabobank-cdc/DeTTECT

SUMMARY
do these instead!

Treat everything in ATT&CK differently
- Techniques, Tactics, Log Source, Detection, etc.

Start AND END with ATT&CK
- Apply threat research not only from but to ATT&CK too

Continued testing on ATT&CK detection
- Deploy continuous testing and improvement

Apply ATT&CK on everything
- Gap analysis, planning, tools acquisition, etc.

ATT&CK and DEFENSE
- Equip your IR and SOC people with ATT&CK knowledge

Show progress on your ATT&CK program
- Expose your progress and challenge to management

THANKS!

Do you have any questions?

twitter.com/tas_kmanager
linkedin.com/in/tondangmangatas
github.com/tas-kmanager

slide will be available on my github