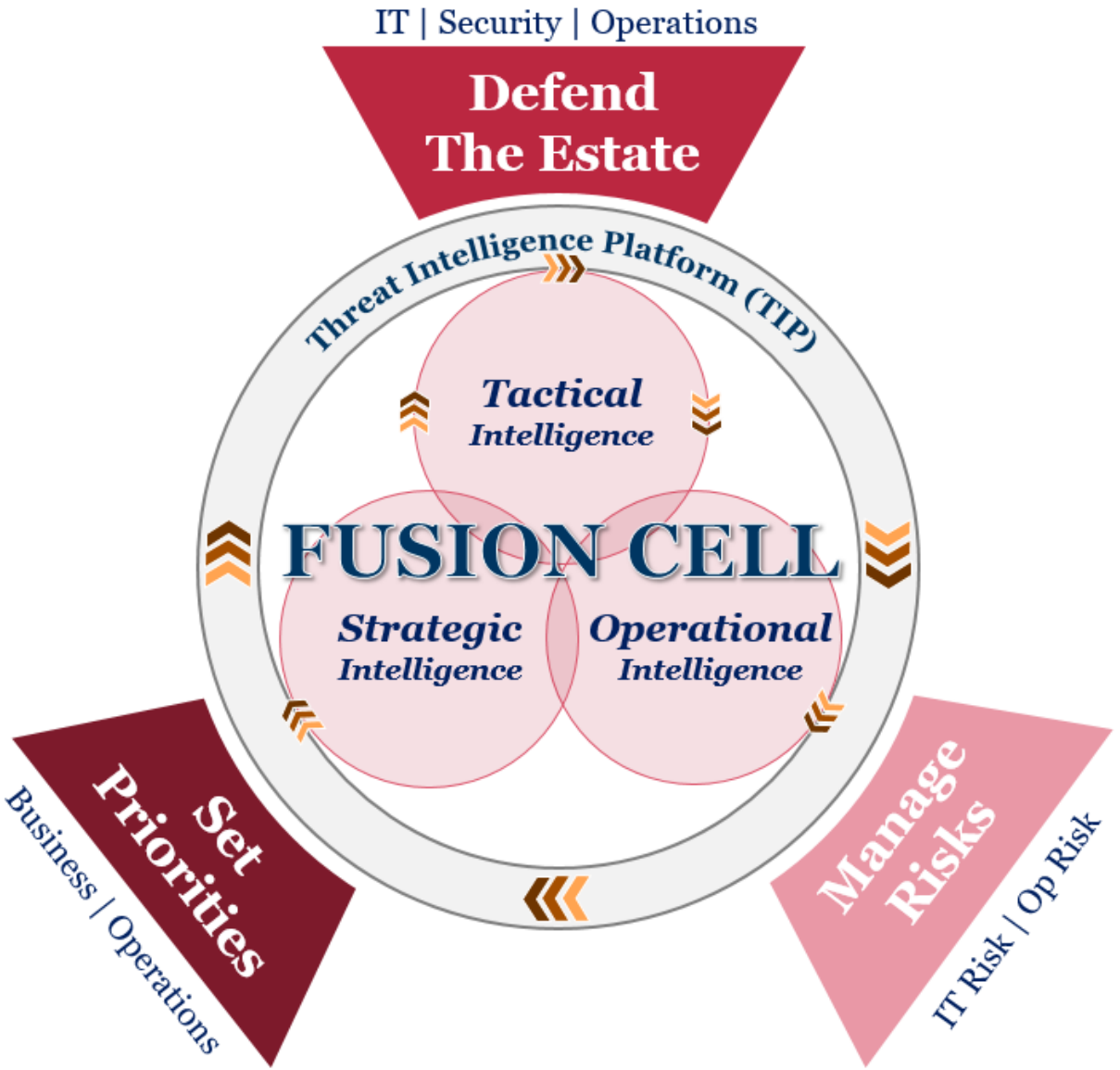
CTI Crash Course

Intel in hunting & IR

SANS CTI Summit
January 20, 2019
@smoothimpact

Threat intel 101

More than just IOCs



Threat Intel 101

In hunting

1. The application of threat intel to **uplift and mine** enterprise security telemetry in order to explore hypotheses.
2. There are some basic **data and tooling** prerequisites, which don't have to break the bank.
3. **Hunting is a subset of network defence**. Threat intel supports both in different ways.
4. **Scope and documentation** are two of the most important aspects of hunting.
5. **Start small** and iterate quickly.

pwc

Threat intel 101

Hunting maturity model

HMM0

Initial

- Reliant on automated off-the-shelf alerting solutions
- Reliant on SIEM and IDSs
- Minimal (if any) environment data collection
- No proactive or retrospective analysis

Base

Basic knowledge of threats to organisation, using generic external data. IT staff deal with any threats. Basic indicators for IT consumption.

HMM1

Minimal

- Reliant on automated off-the-shelf alerting solutions
- Reliant on SIEM and IDS
- Performs some enterprise data collection
- Uses threat reports from open or closed resources for insight
- Ability to apply indicators at bottom of pyramid of pain

Nascent

Long term approach to security being considered. Ability to apply familiar indicators and track reoccurrences.

HMM2

Procedural

- Able to research, learn, modify, and apply community procedures and intelligence to search for adversaries
- Regularly performs searches across the enterprise
- Collect large data sets from across IT estate, including endpoints

Established

Threat intelligence obtained from a wider source base is factored into security. Developing specialists. Robust application of intel.

HMM3

Innovative

- Much more significant use of manual risk based approach in intelligence & hypothesis generation
- In-house expertise developing and publishing procedures rather than consuming procedures from others
- More sophisticated analysis
- Collect large data sets from across IT estate

Dynamic

Driving technical decisions at enterprise level, in-house full-cycle team. Proactive identification of new threats to environment.

HMM4

Leading

- Able to automate Innovative (HMM3) state
- Shorten detection and mitigation time
- Prolific at hunting processes development
- Formalized and documented hunting program

Holistic

Feedback loop between business activities, future strategy and threat intel function. Executive reporting and engagement.

*Hunting Maturity Model (HMM) by David J Bianco.

Threat Intel 101

In incident response

1. How long do you **observe an intrusion for**? Do you **even need to**? How do you define a **red line**?

2. How do you **prioritise preemptive containment measures** or **telemetry uplift**?

3. Do you know **what they want**, or how they're likely to **react to response activity**? What collection bias might have informed this?

4. Do you know **what else they are up to** outside your environment?

5. How quickly can you run a **feedback loop**? How confident can you be that you know the **extent of their capability**?

pwc

Threat Intel 101

In incident response