Raising the Effectiveness of Your Threat Management Program

Agenda

Threat Management Today

How Threat Intel helps

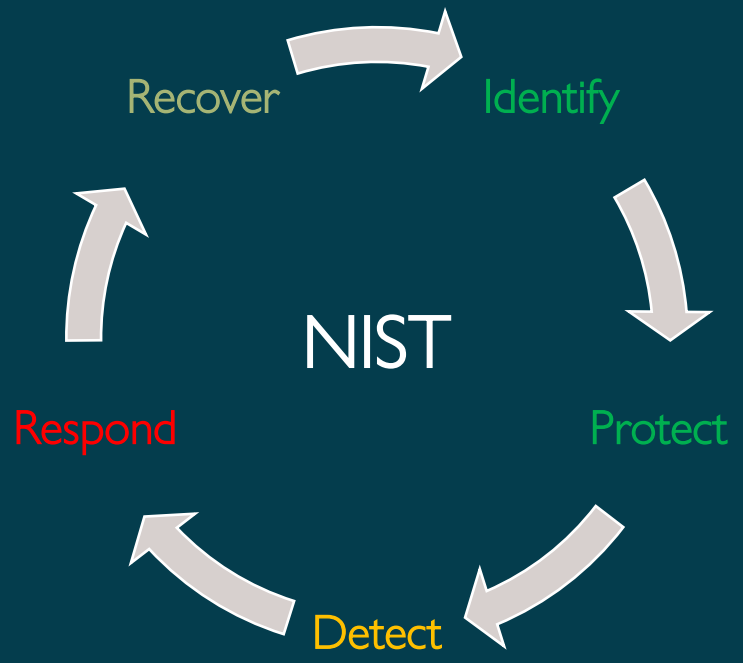
Potential Solution

What it looks like

Why your organisation may not be ready

Threat Management Today

Core: Prevent cyberattacks, detect cyberthreats and respond to security incidents.



Threat Intel helps

Core: Collect, process, analyse data to understand a threat actor's motives, targets, and attack behaviours.

	Prime Enablers	Order	Aim	Target Points	Material Impact
APTs	Funding	Organised	High-impact damage	Valuable Assets (constants)	• Finances • Business Operations • Legal Consequences • Customer Trust
Threat Intel knows	Abundant resources for high-impact damage; concurrent ops.	Relatively predictable	Potential impact likely severe	Risk-based defence	Cost of impact

What does this look like?

Threat Operations Manager,
HerkshireWay & Co.

Hot from the Press …

Russian APT claim responsibility for hack at Hyugo Contracting Services…

Email servers at Harland Hospital ransomed in a sophisticated cyber-attack. Activity attributed to APT 9358.

…novel tactics attributed to APT 90210…

…Another retail company hit in another sophisticated DDoS attack…

"These APT groups are unrelenting."

Proceeds to write detections…

Later that month, on a call with CISO…

Dan, how secure are we? Our competitors are in the news for cyber-attacks!

We are secure.
Detections are in line with best practices.
We have coverage for 95% of APT tactics based on MITRE's ATT&CK Framework.
I am confident we will be fine.

Three months later…

HerkshireWay & Co. website down due to ransomware attack.

Impossible!!!
How could this have happened?!

It must be that inter...
…
…

CISO calls…

Why are we in the news, Dan?

Hello Kate!
It was the …janitor…

What could have gone wrong?

They used best practices.

Threat Intel helps, but...

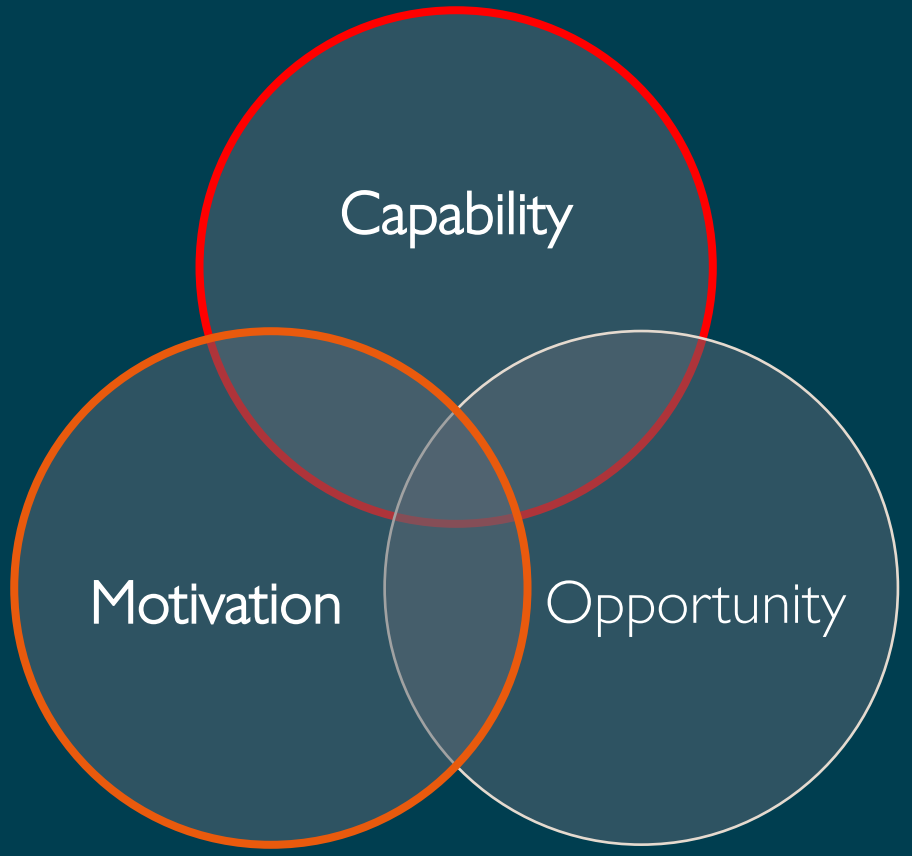
Core: Collect, process, analyse data to understand a threat actor's motives, targets, and attack behaviours.

	Prime Enablers	Order	Aim	Target Points	Material Impact
APTs	Funding	Organised	High-impact damage	Valuable Assets (constants)	• Finances • Business Operations • Legal Consequences • Customer Trust
Threat Intel knows	Abundant resources for high-impact damage; concurrent ops.	Relatively predictable	Potential impact likely severe	Risk-based defence	Cost of impact

- APTs are not the only threat actors.
- The company's security does not depend on TM alone.

Threat Intel helps, but...

Capability and Motivation are variables. Their combined product is not always low for non-APTs.



Threat Intel helps, but...

Core: Collect, process, analyse data to understand a threat actor's motives, targets, and attack behaviours.

	Prime Enablers	Order	Aim	Target Points	Material Impact
APTs	Funding	Organised	High-impact damage	Valuable Assets (constants)	• Finances • Business Operations • Legal Consequences • Customer Trust
Threat Intel knows	Abundant resources for high-impact damage; concurrent ops.	Relatively predictable	Potential impact likely severe	Risk-based defence	Cost of impact
Opportunists/ Script Kiddies/ Hacktivists	Motivation	Less Organised / Random	Any Damage	Any entry	• Finances • Business Operations • Legal Consequences • Customer Trust
Threat Intel knows	Limited resources capacity for high-impact damage	Unpredictable	Potential impact unpredictable.	Harden perimeter	Cost of impact

How do we secure against opportunists/Non-APTs?

Why Business Threat Intelligence (BTI)?

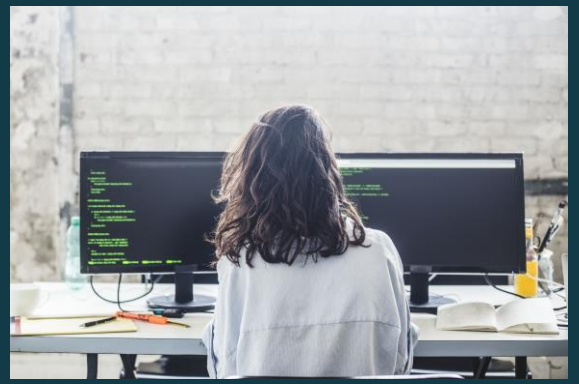
- Informs on specific threat realities of the business
- Communicates team impact beyond speed
- Provides business leaders with awareness and visibility to prioritise security projects and investments
- Helps detection teams prioritise detections for business soft spots
- Drives security for less likely APT targets (SMEs)
- Drives informed security decision-making

BTI & impact on overall security program

Security Awareness

Security Policy

Risk Management



Threat Management

CISO

Effectiveness
Efficiency

How to get it

Awareness of Business threat landscape

+

Business Context

=

Business Threat Intelligence

SOURCE	AIM
• Incident and near-miss trends over-time (true and false positives)	• Address systemic root causes where applicable
• Threat hunting	• Reveals nuances on business operations
• Observing intelligence over-time	• Validate and keep awareness current

What does output look like?

	SOURCE	AUDIENCE	PRODUCT
Awareness of Business threat landscape	• Incident and near-miss trends over-time	• Security Personnel (Team Leaders, Managers)	• Dashboard or Report
+			
Business Context	• Threat hunting	• Security Personnel (Team Leaders, Managers)	• Report
=			
Business Threat Intelligence	• Observing intelligence over-time	• Security & Tech. Leaders (Sec. Team Leaders, Sec. Managers, CISO, CIO, CTO)	• Report or Email

What a BTI report may contain

- Executive Summary
- Threats
- Recommendations
- Conclusion

Threat Management Today

Security Posture

- Business secured
- Resilience Poor

Efficiency

- Extinguished Threats
- Repeated incidents

Mindset

- Special Club (Heroes)
- Sole Protector Team

Adoptability for SMEs

- Quick fix
- Can be outsourced

Cross-team integrations

Difficulty integrating cyber into business operations

Cooperation from C-Suite

- Difficulty gaining C-Suite cooperation beyond emergencies

Threat Management Today + BTI

Security Posture

- *Business secured*
- *Resilience Poor*
- *Business secured*
- *Improved Resilience*

Efficiency

- *Extinguished Threats*
- *Repeated incidents*
- *Identify root causes*
- *Reduced incidents*

Mindset

- *Special Club (Heroes)*
- *Sole Protector Team*
- *Security everyone's responsibility*
- *Defender and Guide/Advisor*

Cross-team integrations

- *Difficulty integrating cyber into business operations*
- *Cyber integrates easier into business operations*

Cooperation from C-Suite

- *Difficulty gaining C-Suite cooperation beyond emergencies*
- *Easier gaining C-Suite cooperation*

Adoptability for SMEs

- *Quick fix*
- *Can be outsourced*
- *Not business priority*
- *Resource investment*

Best Solution:
Contracting service includes BTI in service offering.

Barriers to Adoption

- No capability for log collection
- Minimal Workforce
- Low on business priorities

Conclusion

- Managing threats ➡ Securing businesses
- Be curious about the business being secured
- Security is a business priority – help the business by education
- Document findings for reference
- Inform the business on their state of security to drive improvement.

Raising the Effectiveness of Your Threat Management Program