MANDIANT
NOW PART OF Google Cloud

Solving CISO Headaches
How to Align CTI and Risk Management

Dr Jamie Collier

Principal Threat Intelligence Advisor

John Doyle

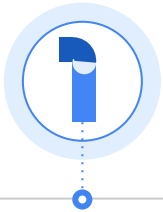
Applied Intelligence Mentorship Program Lead

7th November 2023

Introduction

- CTI and Risk Management have emerged as separate areas. This talk explores how we can bridge the gap.
- Transcending cyber risk-intelligence silos creates more **synchronized defense organizations**, **enabling larger strategic initiatives**.
- But, aligning the two is not always an easy task...

Challenges in Risk-Intelligence Integration



Role misperceptions

- ★ CTI often perceived as highly tactical
- ★ Risk can become detached from network defence

Unique lexicons

- ★ Risk frameworks rarely used in CTI
- ★ Many CTI processes detached from cyber risk

Cultural differences

- ★ Intelligence overwhelmingly threat-led
- ★ Different workflows

Dedicated career paths

- ★ Specialist skill sets required for each discipline

Why a CTI Team Benefits

- Build influence with executive audiences.
- Contribute to highly strategic initiatives beyond the security function.
- Make use of existing work and improve visibility of the internal organization.
- Mutual benefit vs. zero-sum game.

Risk and Intelligence: How to Play Nice

Build mutual understanding

A baseline understanding of the other discipline sets the foundation for long-term collaboration.

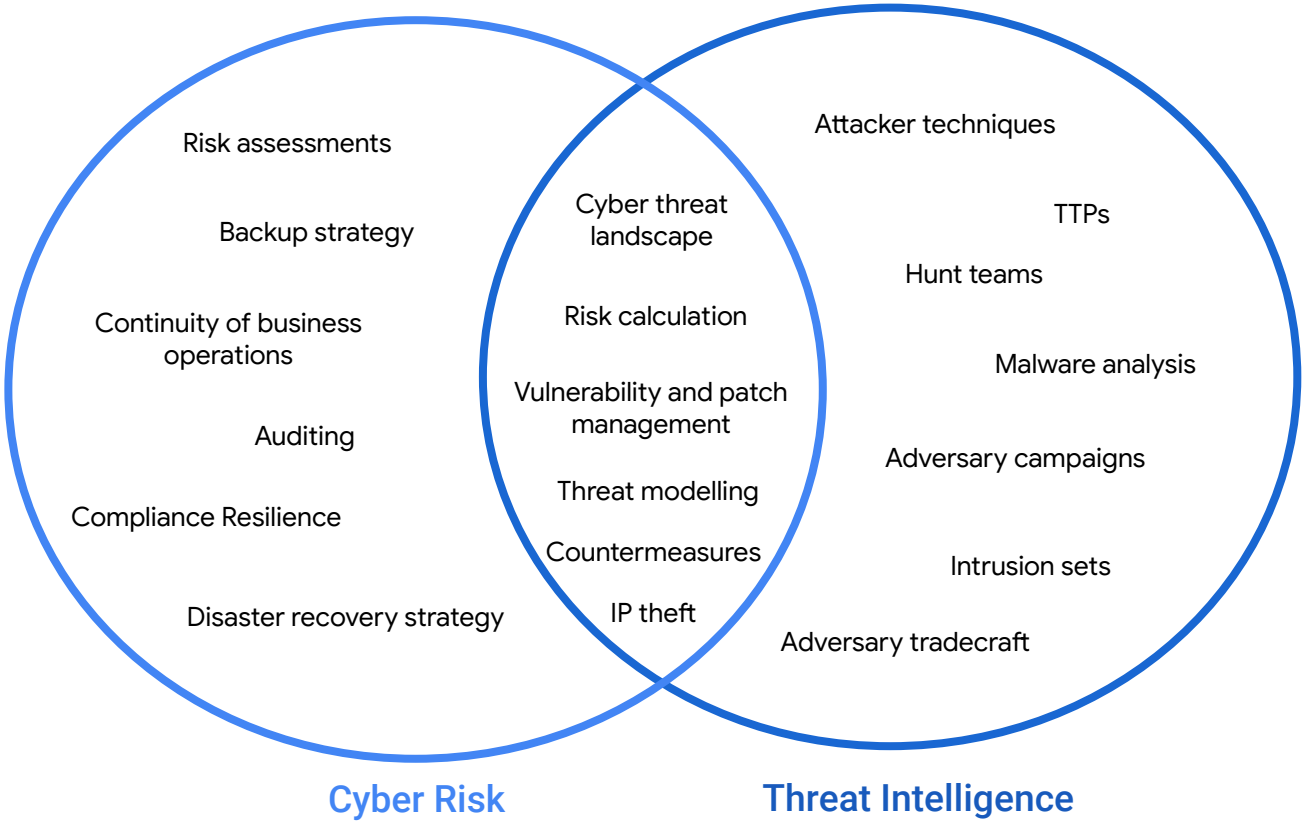
Identify foundational overlap

Understanding how key CTI products and processes relate to cyber risk will help CTI programs engage risk practitioners.

Build collaborative workflows

Cyber risk and CTI teams can work in tandem to create joint analysis that is collectively informed by each team's unique perspective.

Build Mutual Understanding



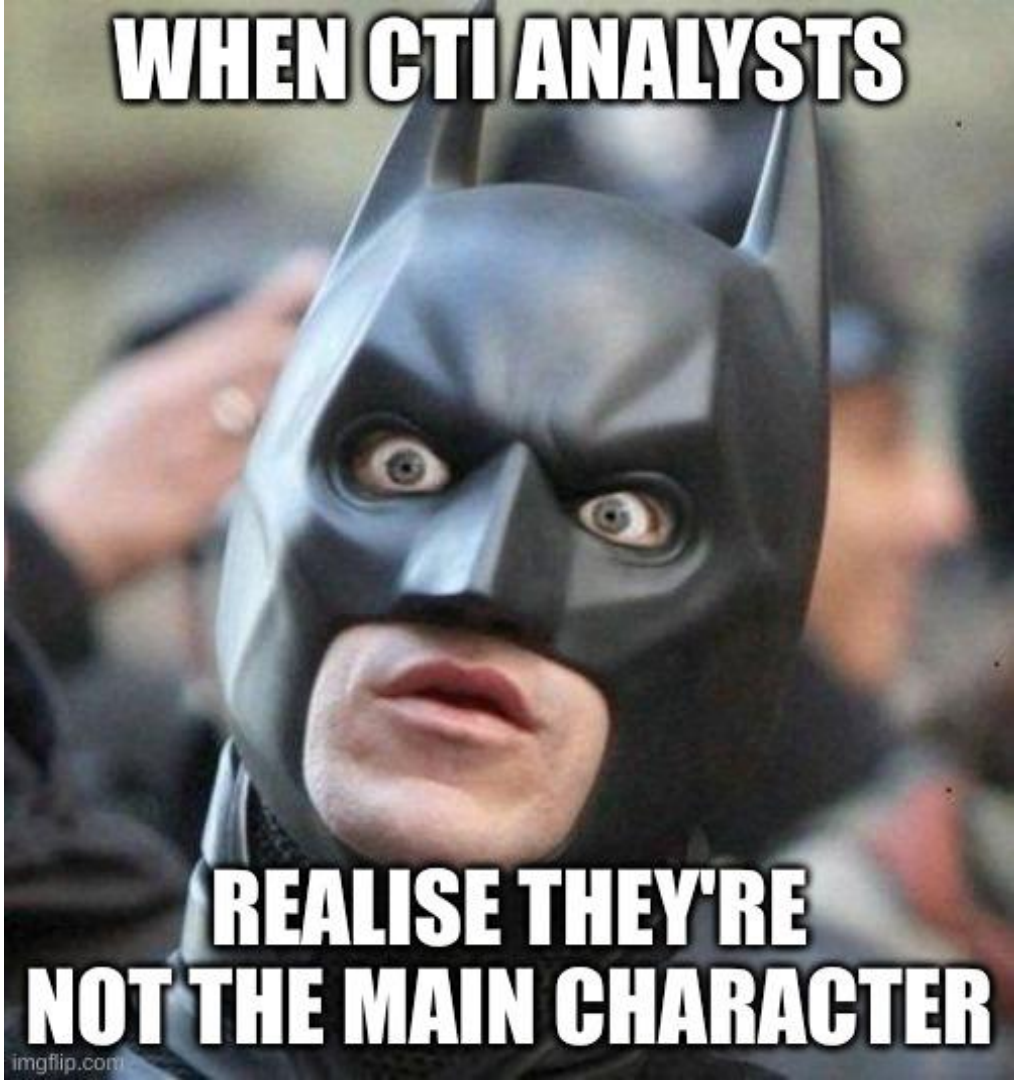
Secret Sauce vs CTI Fundamentals

vs.

Stakeholder analysis

Use cases

Intelligence requirements



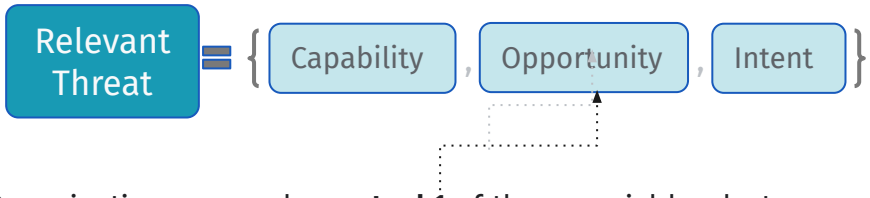
Advice on Engaging with Risk Stakeholders

- Embrace role as an **educator**.
- Start **simple**.
- Focus on what you can **control and manage**.
- Don’t be afraid to **push back**.

Focus on What You Can Control

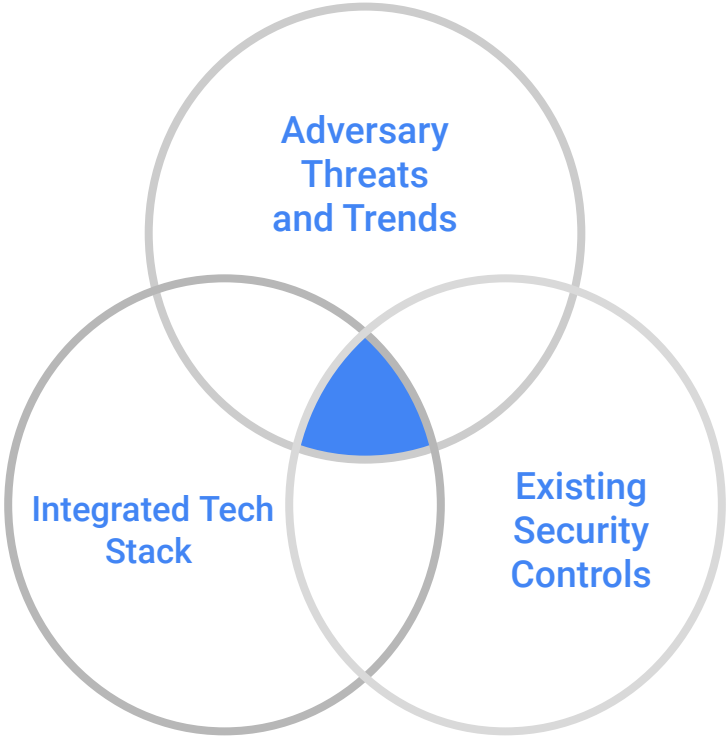
The shared goal is risk reduction

Threats are **an input** into overall risk.

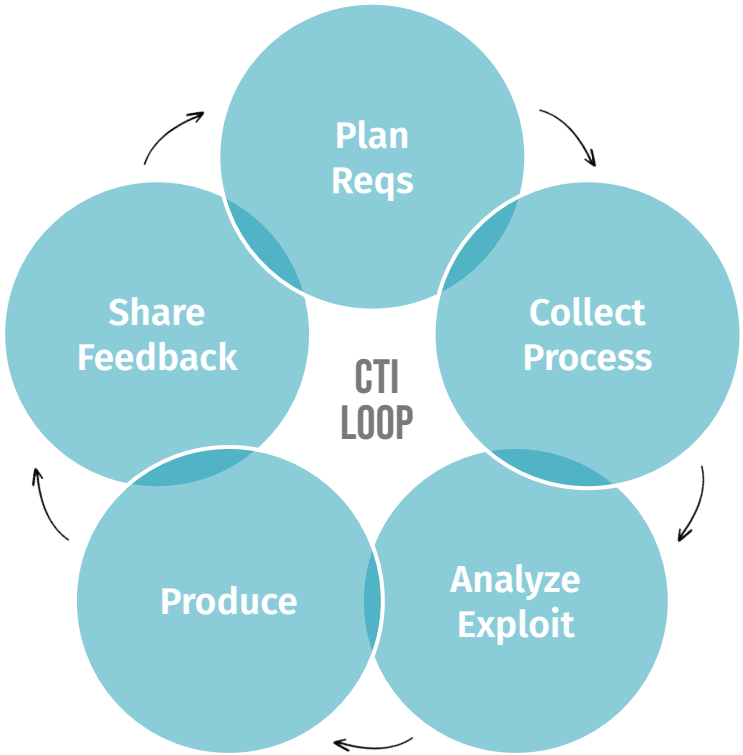


Organizations can only **control 1** of these variables, but...

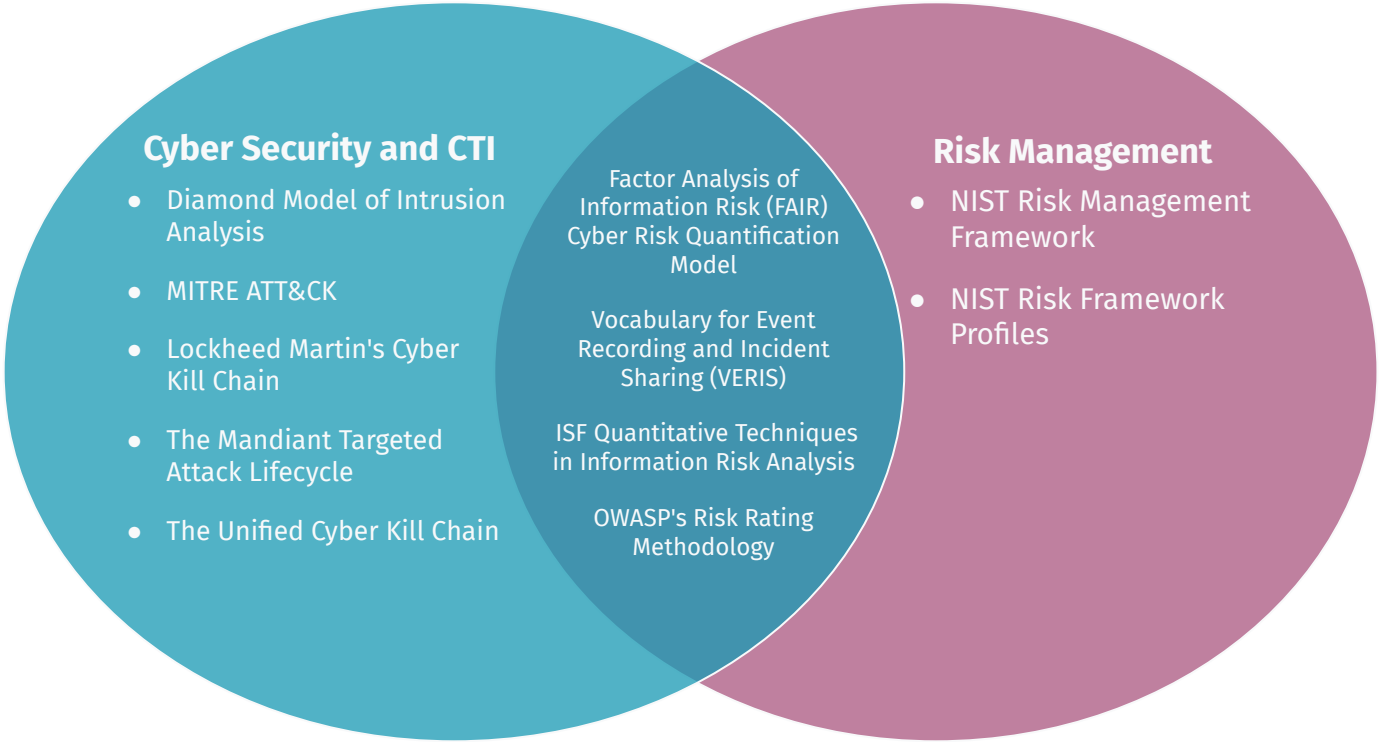
a reduction in any of the three drives down overall threat and provides a more scoped focus for risk management decisions



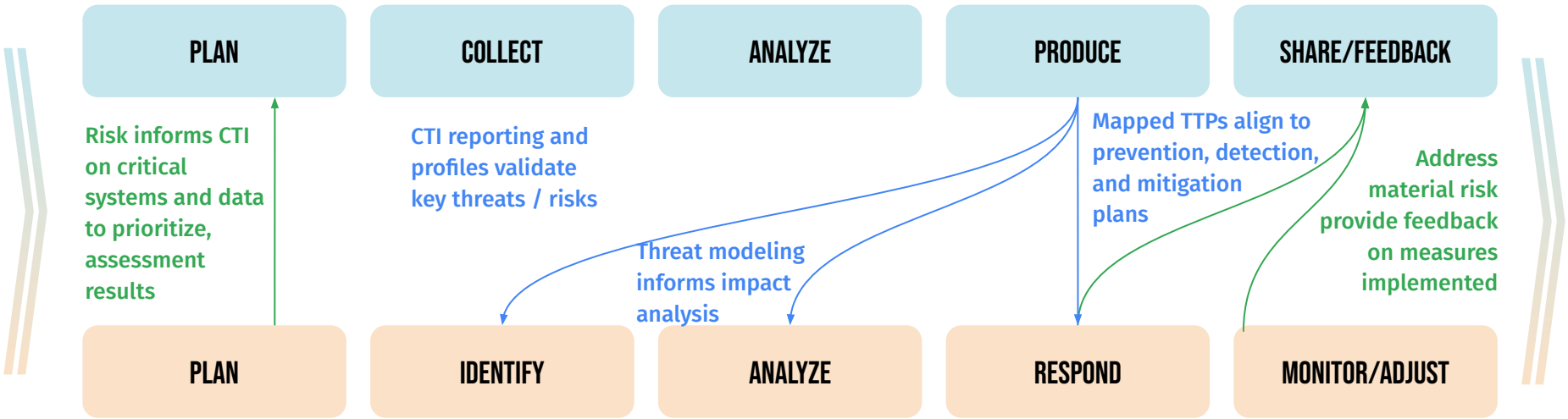
Each Discipline Has Separate Processes



Each Discipline Leverages Separate Mental Models



Yet Multiple Integration Opportunities Exist



Understand the threats associated with the industry and to the organization, taking informed decisions as appropriate to the risk posed to the organization.

Build Collaborative Workflows

Threat profile

CTI team identifies key external threats

Risk management

CTI & risk collaborate to determine which threats pose a material risk

Crown jewels

Risk teams inform CTI teams about the most critical data and systems

Threat modelling

Threat profile informs actions adversaries take to inform modelling & impact analysis

Countermeasure testing

Adversary techniques used by risk team to map prevention & detection measures

Cyber Threat Profile

A cyber threat profile is arguably the most important document for any cyber intelligence program.

Responsible, Accountable, Consulted and Informed (RACI) Matrix

Clarifies which individuals or groups are responsible for a project's successful completion, and the roles that each will play throughout the project.

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED	INFORMED
Identify and document cyber threat factors	CTI	CTI	IT Leadership	Risk
Lead cyber risk assessments	Risk	Risk	CTI	IT Leadership
Develop threat models	IT Security	IT Security	Risk, CTI	IT Leadership
Validate cyber threats to crown jewels	CTI (or red team)	Risk	Risk	IT Leadership

CASE STUDY

SUPPLY CHAIN RISKS & DEVELOPER ENVIRONMENTS

Building a Software Team from 0

- Exec team wants to understand risks
- Prominent use of open-source tools and software dependencies makes supply chain security a key issue

CTI & Risk Actions

- Provide Supply Chain Risk assessment
- Help identify peer and third party incidents to demonstrate org, sector, regional threat relevance
- Support defense with up-to-date TTPs
- Recommend and build successful resiliency measures

CASE STUDY

SUPPLY CHAIN RISKS & DEVELOPER ENVIRONMENTS

SITUATION REQUIRING ASSESSMENT	CTI CONTRIBUTION	SIMPLE RISK ASSESSMENT	CROWN JEWEL IMPACT
Supply chain risks associated with developer environments and interest in developing software team	Since 2013 supply chain risks associated with developer environments have grown significantly in both frequency and severity. This includes targeting of both open-source libraries and developer tools across a range of sectors and regions. During this period, threat actors have continually improved their compromise tactics and tools. Typical post-compromise activity includes credential theft and the deployment of cryptominers.	**Frequency** - Moderate and increasing **Severity** - High	**HIGH PROBABILITY**

Recommendations include mitigation steps, for example:

- Utilize SBOM methods to document, understand, and track build components associated with application development.
- Establish a change control process and board for all enterprise hardware and software changes. (E.g. centralized IT or IT security managed process for downloading, testing, and pushing updates out to users.)
- Use an advanced endpoint security solution, such as EDR, to detect malicious behavior if a tainted software package is DLed and executed.
- Security assessments and audits should be an integral part of the software development lifecycle or continuous integration and deployment (CI/CD) pipeline for any internally developed software that is customer facing or integral to internal functions of the organization.

Conclusion

Both cyber risk and CTI operate better together.

The value of what are **often siloed** and **disparate functions** multiplies when brought together.

Combining CTI and risk management is **easier than you think**!

A lot of the work comes down to the foundational elements of CTI (stakeholder analysis, intelligence requirements, and a threat profile).

Combing CTI and risk management increases the relevance and effectiveness of both parts of the organization.

- Better Together: The Benefits of Integrating Cyber Threat Intelligence and Risk Management

Conclusion

Everyone has intrinsic drivers. Identify and leverage them!

Organizational constructs run on KPIs

Share the spotlight, give praise and glory

Feedback drives relationships and outcomes

Champion, advocate, woo, and win hearts and minds to best position ourselves for success

Bonus Ask

bit.ly/ctisurvey23

Get In Touch

@_John_Doyle

in/john-doyle-a02bab10/

@TheCollierJam

in/collierjs

@euphoricfall

in/graceschi

grace@pulsedive.com