Bridging the Gap Between Threat Intelligence and Risk Management

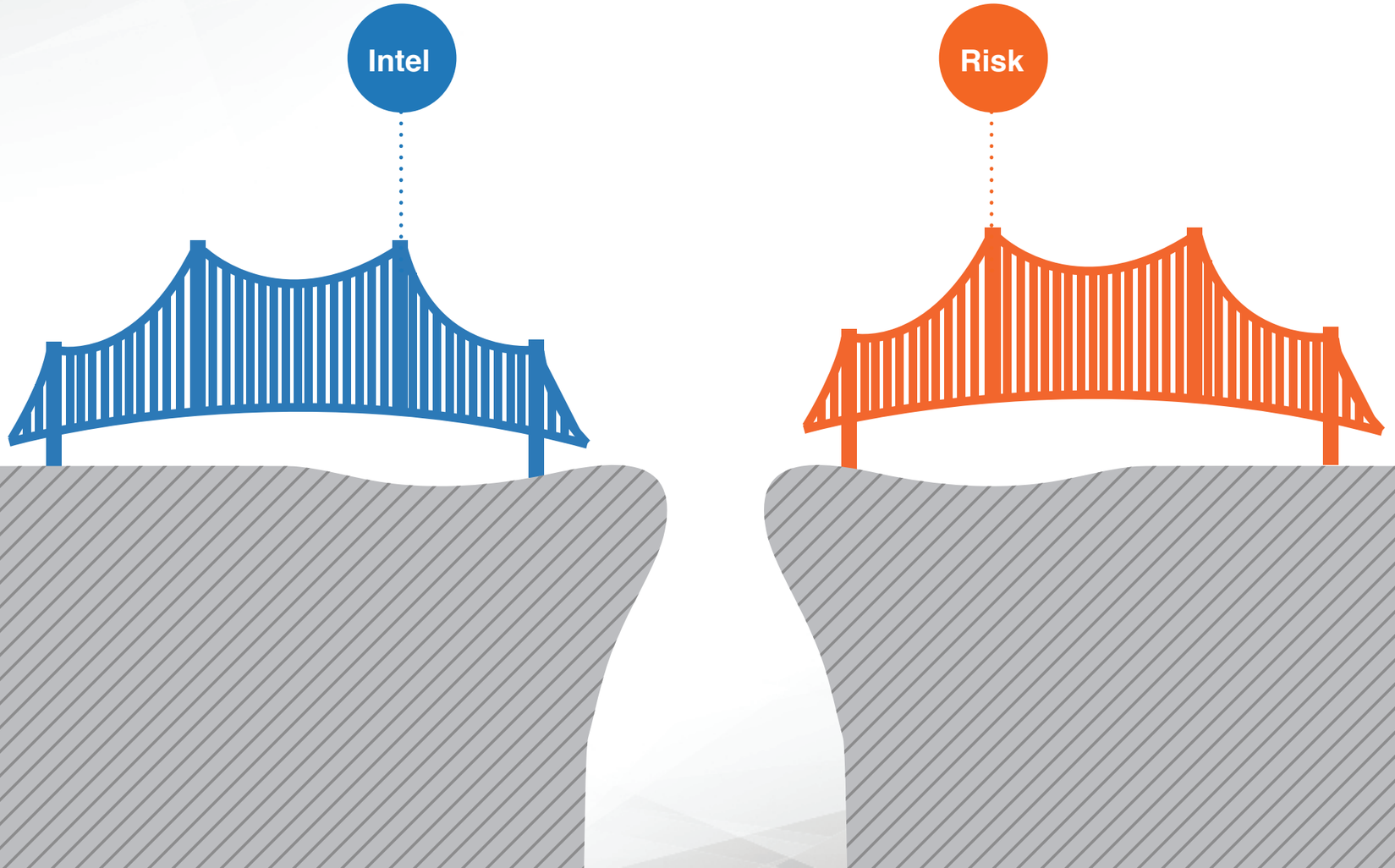
Toni Gidwani
Director of Research Operations

ThreatConnect
@ThreatConnect

Underlying assumption

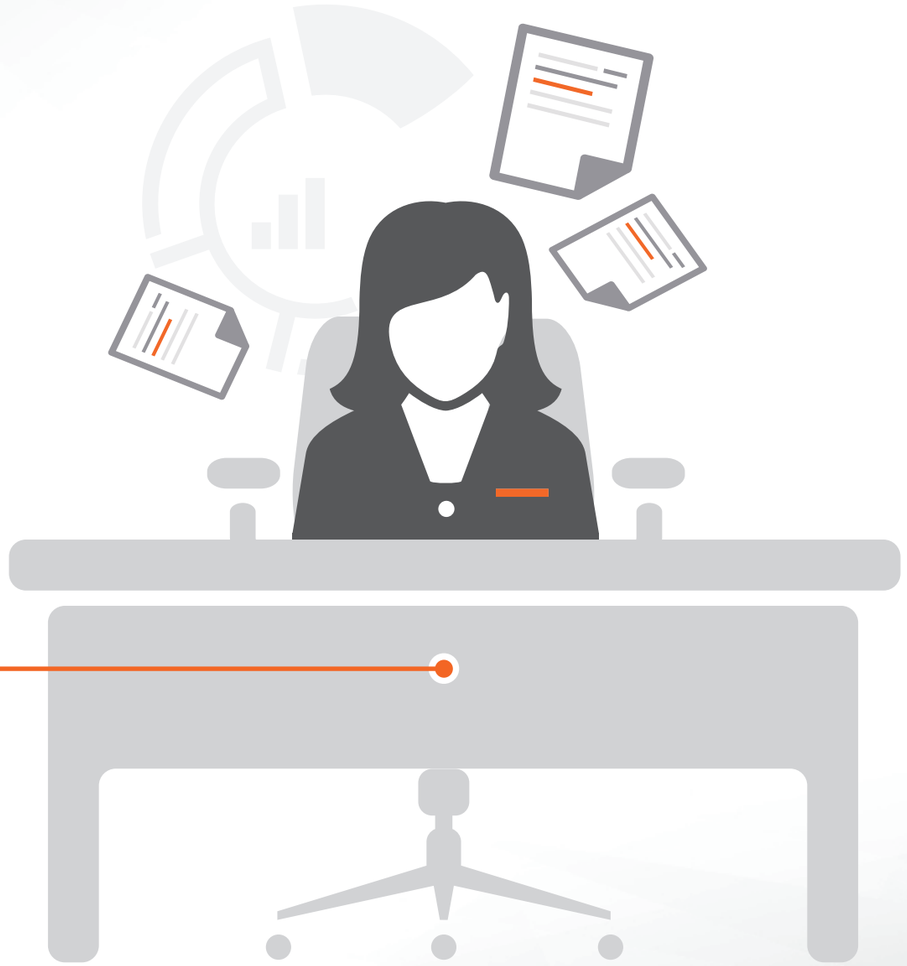
Good **intelligence** makes smarter **models**;
Smarter models inform **decisions**;
Informed decisions drive better **practice**;
Better practice improves **risk** posture;
which, done efficiently,
Makes a successful security **program**.

Does your security program look like this?



Threat Intelligence

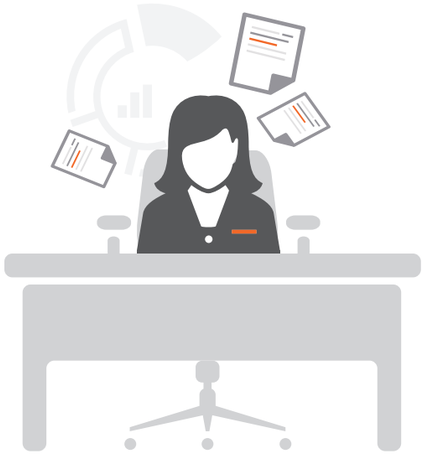
Risk Management



They have some issues dividing them...

Threat Intelligence

- “There’s way too much uncertainty around her. I live and die in a binary world.”
- “I beat adversaries with STIX and detonate their remains. She plays with numbers.”
- “People say she’s ‘stochastic.’ That explains a lot; she needs serious help.”
- “She doesn’t even cyber! Need I say anything more?”



Risk Management

- “He’s intolerable. I assess he needs to be treated and transferred to a third party.”
- “One look at his laptop makes me panic. It’s a giant audit finding with a keyboard.”
- “He never shares with coworkers. I swear, if he TLP-Red’s us one more time...”
- “What’s his deal with China, anyway? It’s an HR liability if you ask me.”

... but they'd make such a great team.

Agenda

- Bridging risk & IR in Verizon's DBIR
- Building understanding
- Finding common ground
- Bridging the gap
- Crossing the divide (apply)

Bridging Risk and IR in Verizon's DBIR

Bridging risk and IR in the DBIR

Frequency of incident classiciation patterns per victim industry

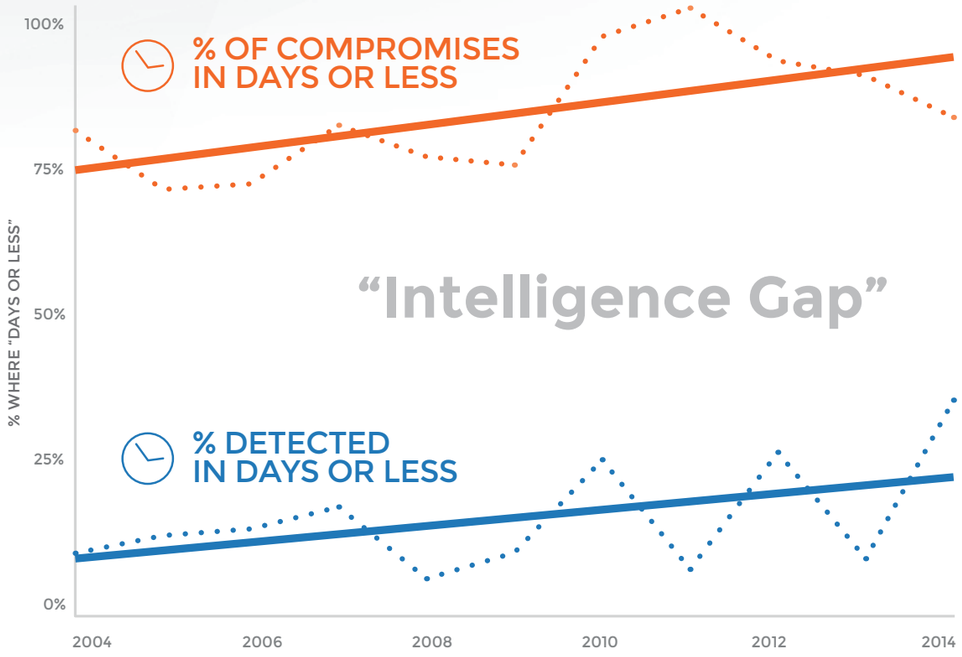
INDUSTRY	POS INTRUSION	WEB APP ATTACK	INSIDER MISUSE	THEFT/LOSS	MISC. ERROR	CRIMEWARE	PAYMENT CARD SKIMMER	DENIAL OF SERVICE	CYBER ESPIONAGE	EVERYTHING ELSE
Accommodation	74%	1%	2%	1%	1%	<1%	<1%	20%	<1%	1%
Administrative	4%	11%	22%		2%			56%		4%
Education		5%	1%	3%	4%	2%		81%	2%	2%
Entertainment	1%	1%		<1%				99%		
Finance	<1%	48%	3%	<1%	1%	2%	6%	34%	<1%	5%
Healthcare	5%	4%	23%	32%	18%	4%			2%	11%
Information	<1%	12%	2%	<1%	11%	4%		46%	3%	21%
Manufacturing	1%	6%	6%		1%	5%		33%	16%	33%
Professional		1%	2%	1%	1%	1%		90%	2%	2%
Public	<1%	<1%	22%	20%	24%	16%		1%	<1%	17%
Retail	32%	13%	1%		1%	1%	3%	45%	<1%	2%
Transportation		35%	6%		6%	10%		26%	16%	

Source: 2016 Verizon DBIR

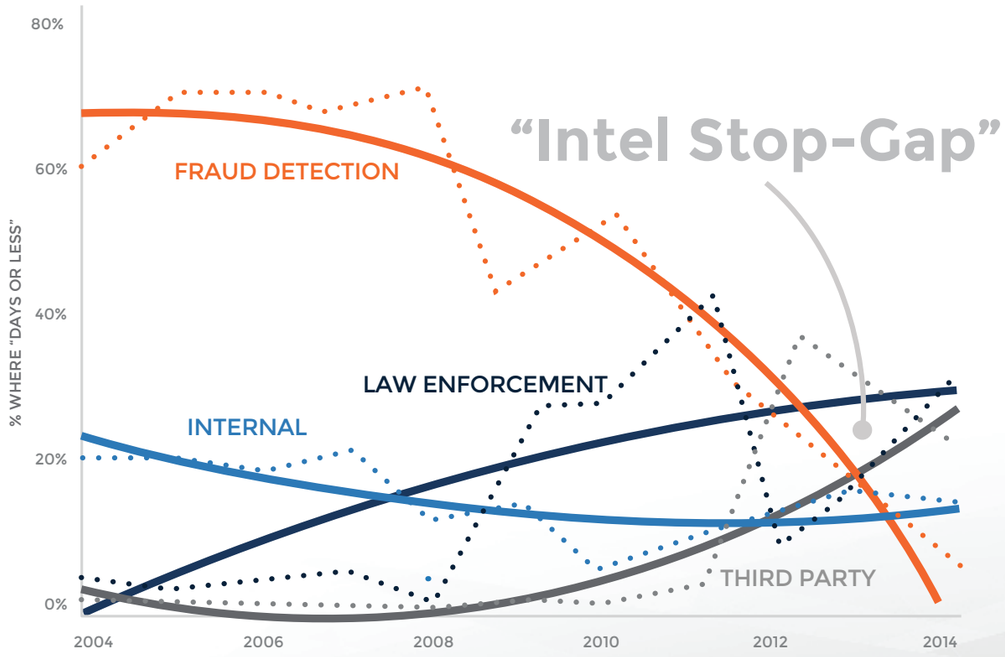
Bridging risk and IR in the DBIR

The Intelligence Gap

Percent of breaches where time to compromise (red)/time to discovery (blue) was day or less



Breach discovery methods over time



**All Figures from Verizon DBIR

Building Understanding

What is threat intelligence?

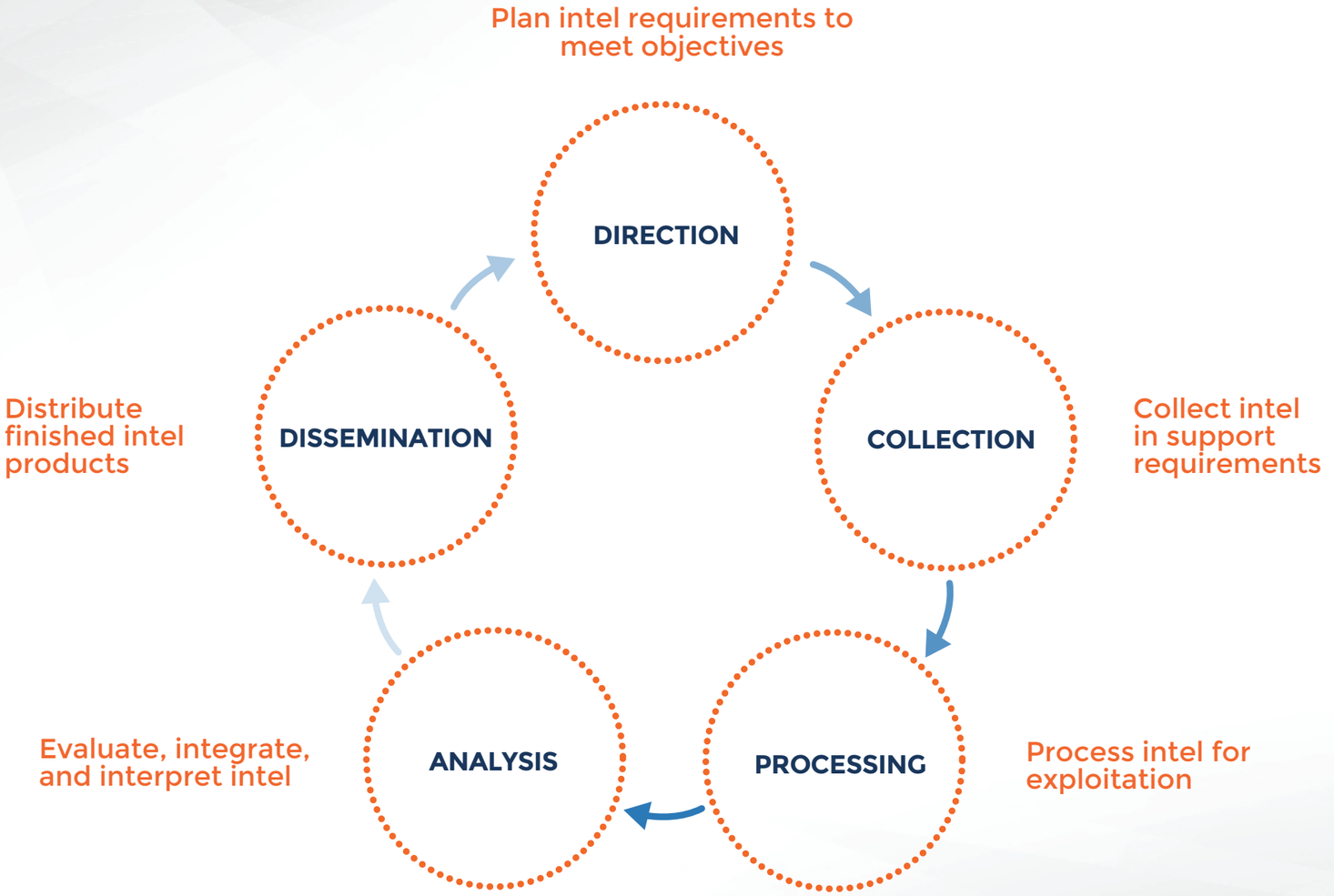
"Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."

Gartner®

"The details of the motivations, intent, and capabilities of internal and external threat actors. Threat intelligence includes specifics on the tactics, techniques, and procedures of these adversaries. Threat intelligence's primary purpose is to inform business decisions regarding the risks and implications associated with threats."

FORRESTER®

Classic intelligence cycle

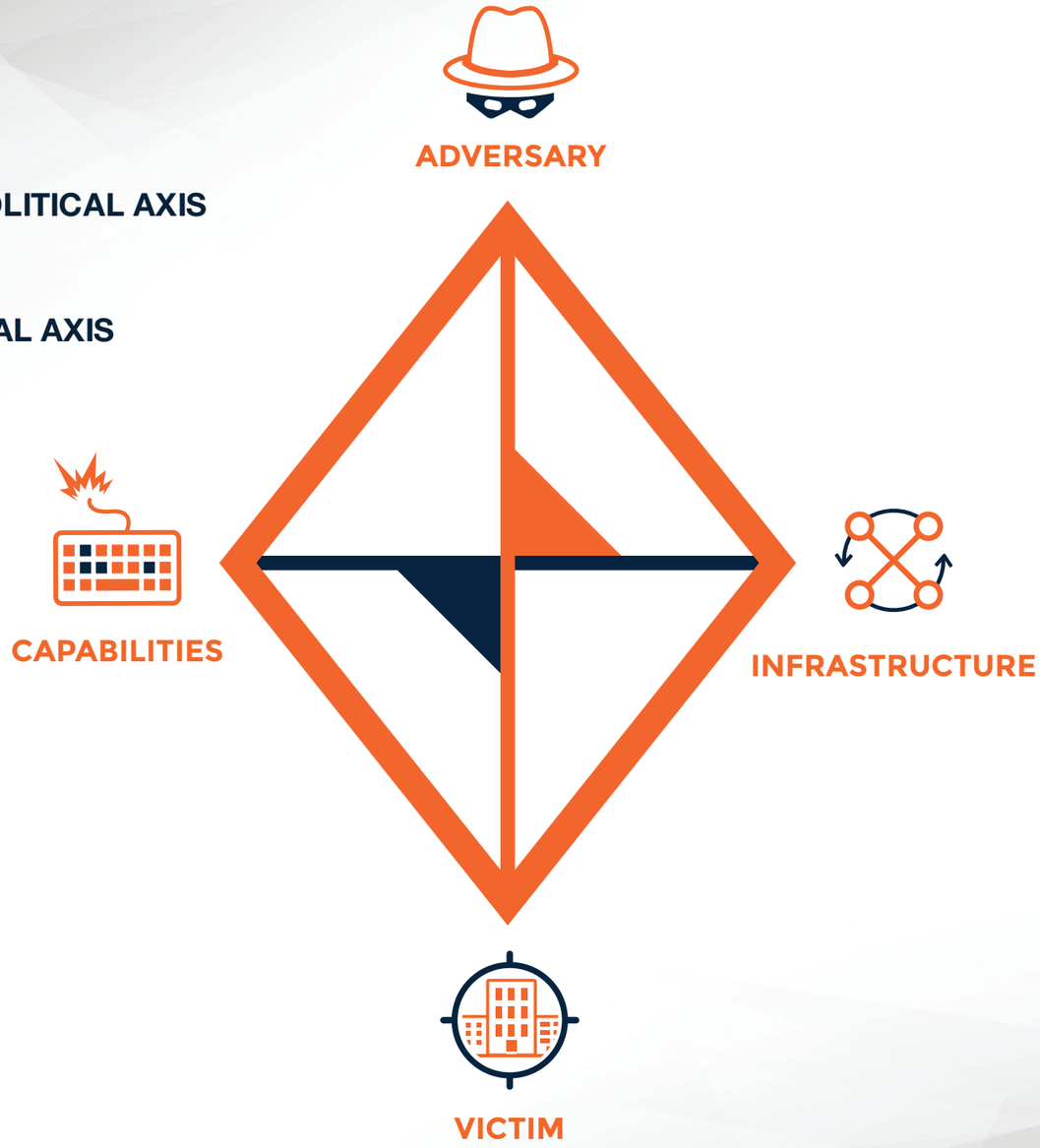


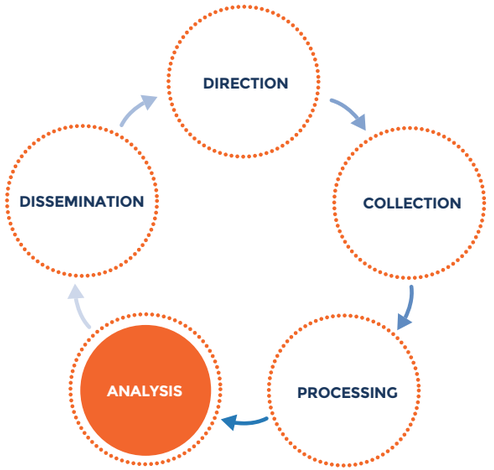
Threat intelligence process

The Diamond Model of Intrusion Analysis

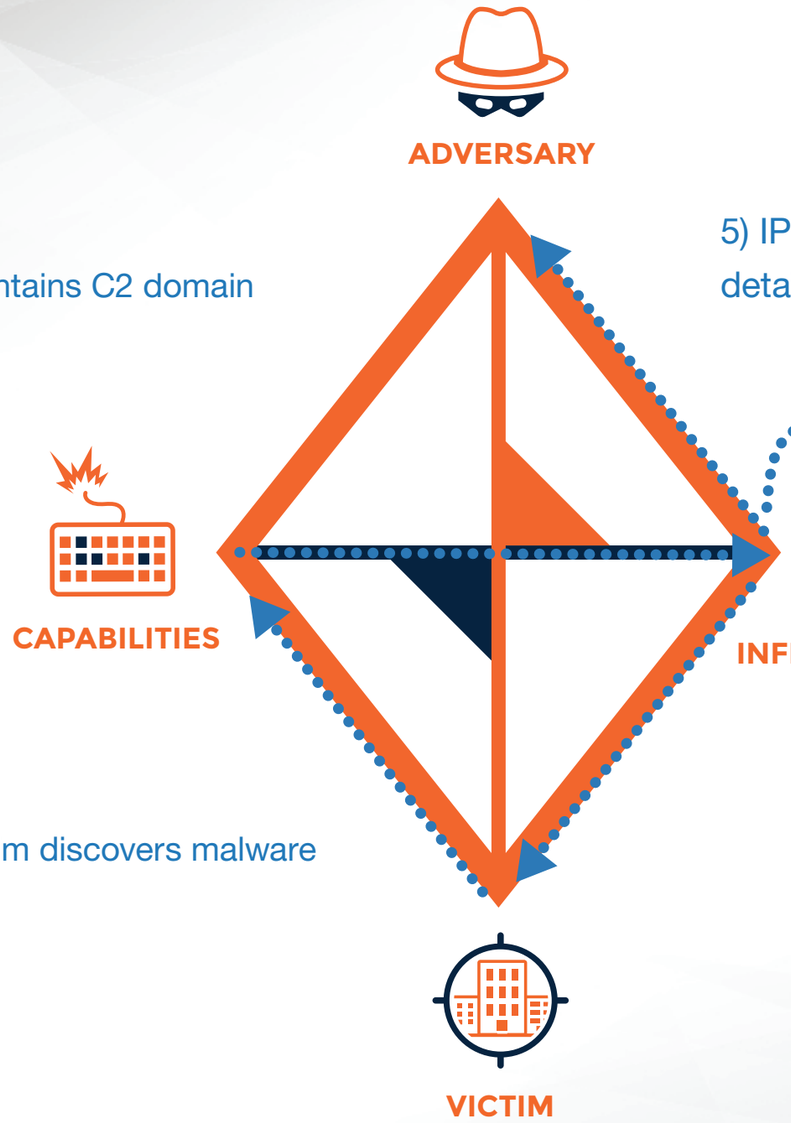
1 SOCIO-POLITICAL AXIS

2 TECHNICAL AXIS





Threat intelligence process



What is risk?

"The probable frequency and probable magnitude of future loss."

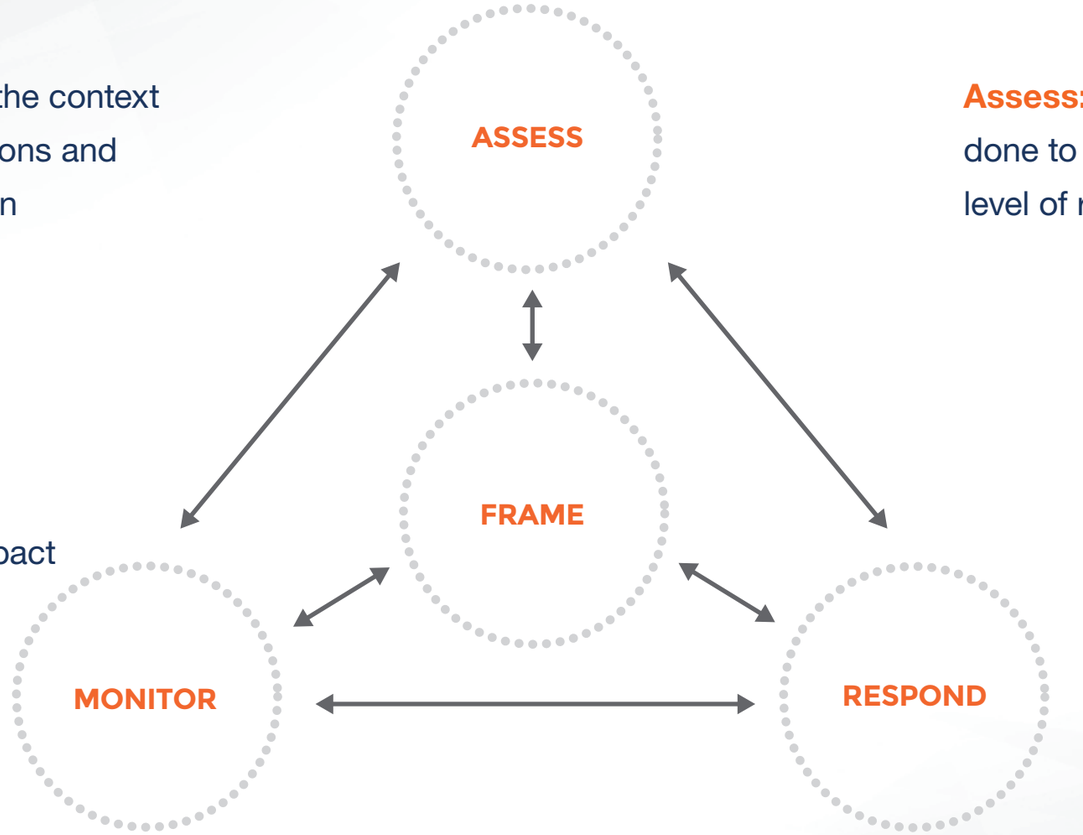
– Factor Analysis of Information Risk (FAIR)

Risk management process

(NIST 800-39)

Frame: establishes the context for risk-based decisions and strategy for execution

Assess: encompasses everything done to analyze and determine the level of risk to the organization

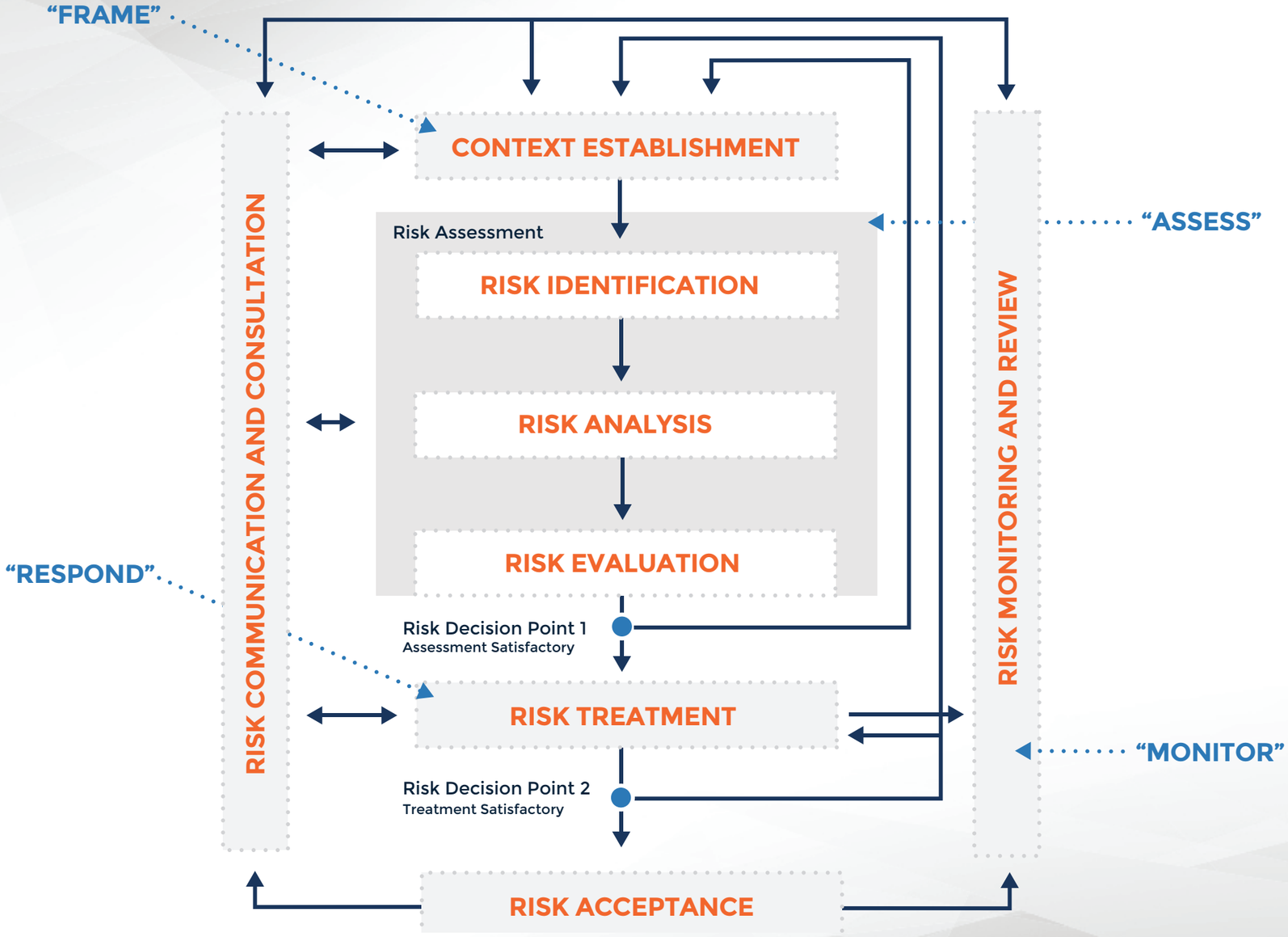


Monitor: verifies proper implementation, measures ongoing effectiveness, tracks changes that impact effectiveness or risk, etc.

Respond: addresses what organizations choose to do once risk has been assessed and determined

Risk management process

(ISO 27005)



Finding Common Ground

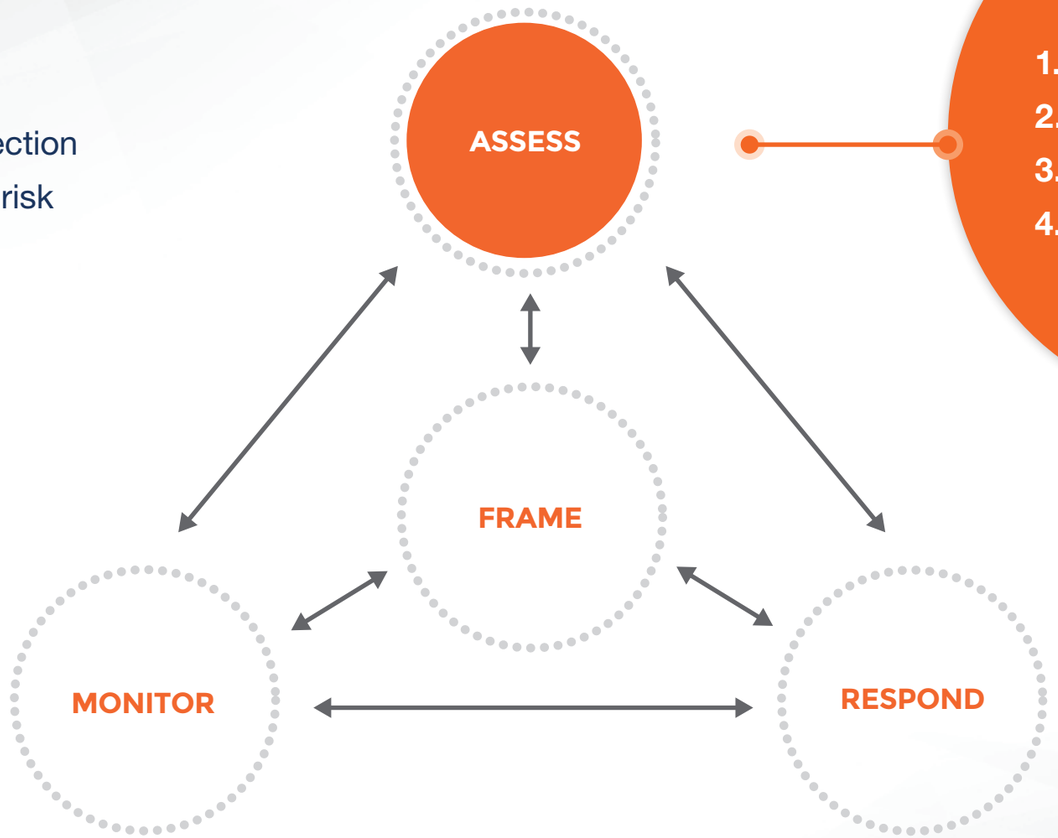
Risky questions needing intelligence answers

- What types of threats exist?
- Which threats have occurred?
- How often do they occur?
- How is this changing over time?
- What threats affect my peers?
- Which threats could affect us?
- Are we already a victim?
- Who’s behind these attacks?
- Would/could they attack us?
- Why would they attack us?
- Are we a target of choice?
- How would they attack us?

- Could we detect those attacks?
- Are we vulnerable to those attacks?
- Do our controls mitigate that vulnerability?
- Are we sure controls are properly configured?
- What happens if controls do fail?
- Would we know if controls failed?
- How would those failures impact the business?
- Are we prepared to mitigate those impactS?
- What’s the best course of action?
- Were these actions effective?
- Will these actions remain effective?

Intel in the risk management process

Frame: adjust intelligence direction and ops to meet the needs of risk management



1. Select asset(s) at risk
2. Identify risk scenarios
3. Estimate risk factors
4. Determine risk level

Monitor: intelligence tracks threat changes that warrant system and control changes

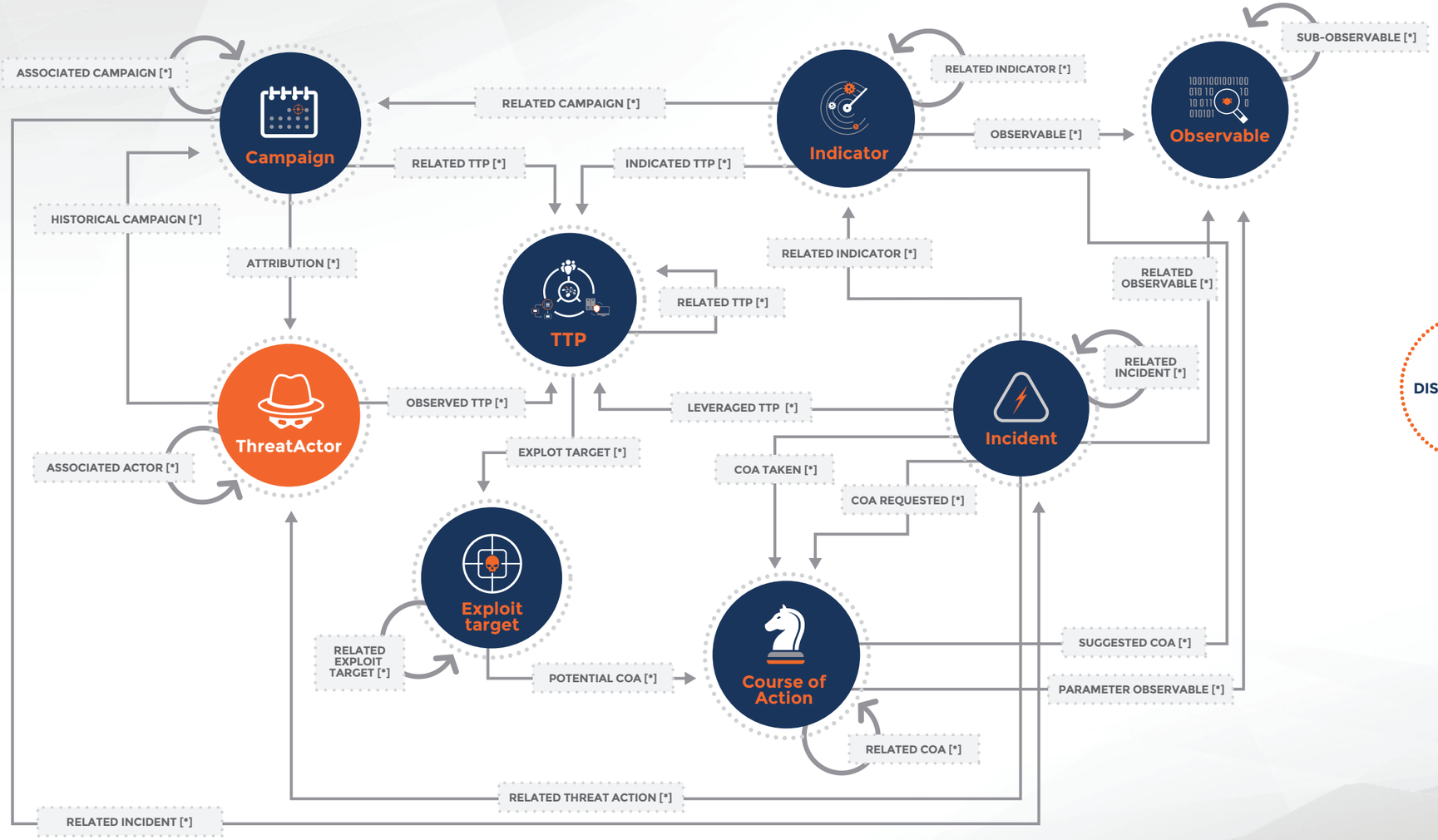
Respond: intelligence supports evaluation and implementation of courses of action

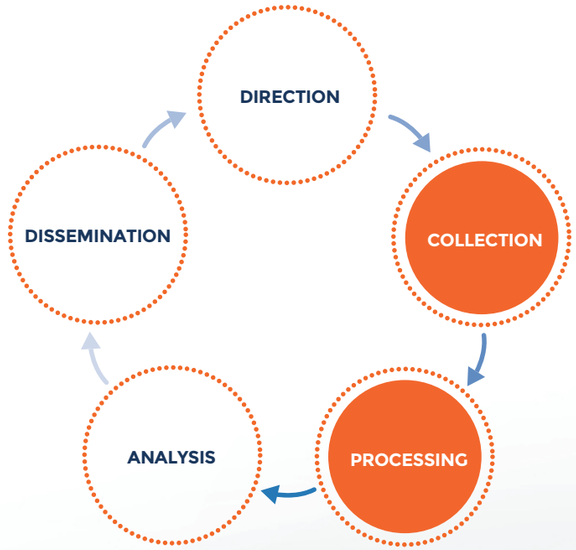
Finding some common ground

Factor Analysis of Information Risk (FAIR)

Finding some common ground

Structured Threat Information eXpression (STIX)

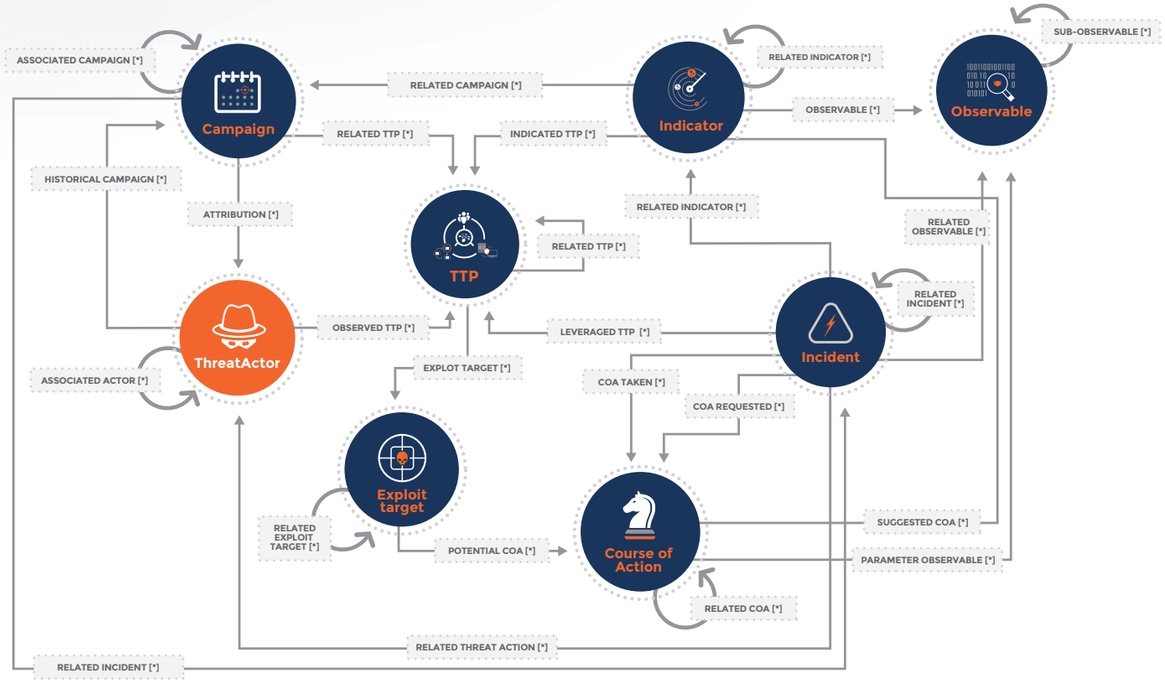




Finding some common ground

A FAIR-ly intelligent approach

Threat Intel (STIX)



Risk Analysis (FAIR)

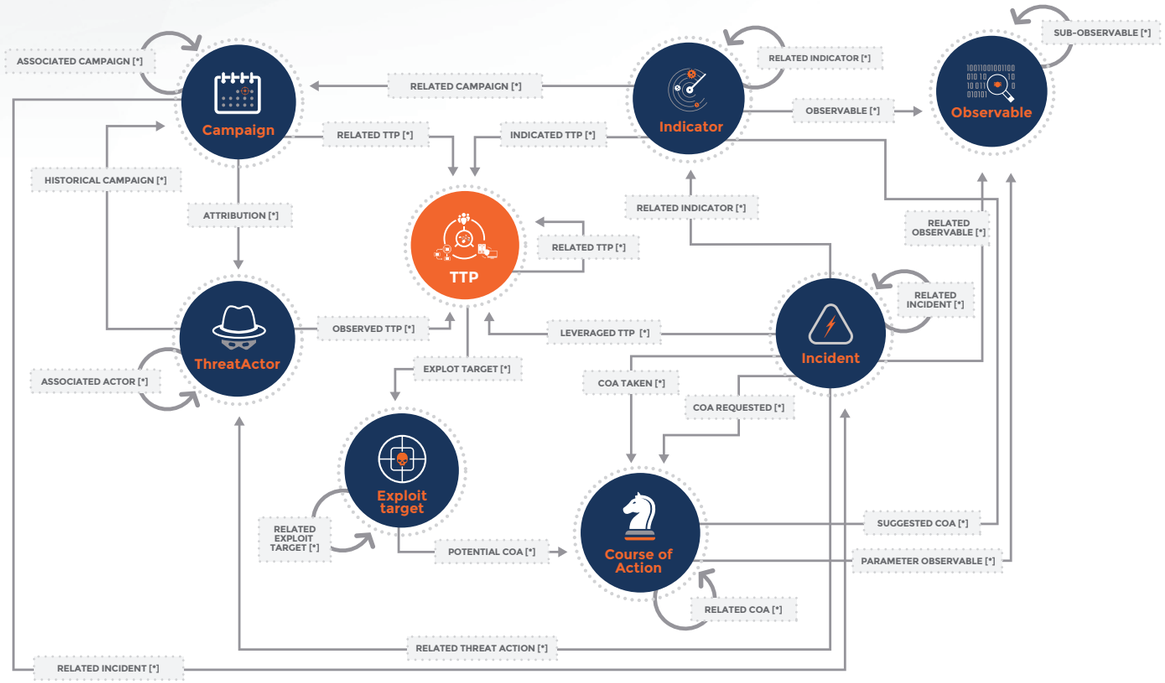
- Type
- Sophistication
- Planning and Support
- Intended Effect
- Observed TTPs

** Initial map: threatconnect.com/threat-intelligence-driven-risk-analysis/*

Finding some common ground

A FAIR-ly intelligent approach

Threat Intel (STIX)



Risk Analysis (FAIR)

- Behavior
- Resources
- Kill Chain Phases
- Exploit Target

** Initial map: threatconnect.com/threat-intelligence-driven-risk-analysis/*

Bridging the Gap

Example risk assessment project

"During a recent audit, it was discovered that there were active accounts in a customer service application with inappropriate access privileges. These accounts were for employees who still worked in the organization, but whose job responsibilities no longer required access to this information. Internal audit labeled this a high risk finding."

From: Measuring and Managing Information Risk by Jack Freund and Jack Jones (p. 123)

Example risk assessment project

FAIR analysis process flow

From: *Measuring and Managing Information Risk* by Jack Freund and Jack Jones (p. 93)

Example risk assessment project

Scenarios associated with inappropriate access privileges

Asset at Risk	Threat Community	Threat Type	Effect
Customer PII	Privileged insiders	Malicious	Confidentiality
Customer PII	Privileged insiders	Snooping	Confidentiality
Customer PII	Privileged insiders	Malicious	Integrity
Customer PII	Cyber criminals	Malicious	Confidentiality

FAIR estimations relevant to the cyber criminal scenario

TEF Min	TEF M/L	TEF Max	TCap Min	TCap M/L	TCap Max
0.5 / year	2 / year	12 / year	70	85	95

From: *Measuring and Managing Information Risk* by Jack Freund and Jack Jones (p. 127)

Example risk assessment project

Standard cyber criminal threat profile

Factor	Description
Motive	Financial, intermediary.
Primary intent	Engage in activities legal or illegal to maximize their profit.
Sponsorship	Non-state sponsored or recognized organizations (illegal organizations or gangs).
Targets	Financial services and retail organizations.
Capability	Professional hackers. Well-funded, trained, and skilled.
Risk Tolerance	Relatively high; however, willing to abandon efforts that might expose them. Prefer to keep their identities hidden.
Methods	Malware, stealth attacks, and Botnet networks.

From: *Measuring and Managing Information Risk* by Jack Freund and Jack Jones (p. 54)

Example risk assessment project

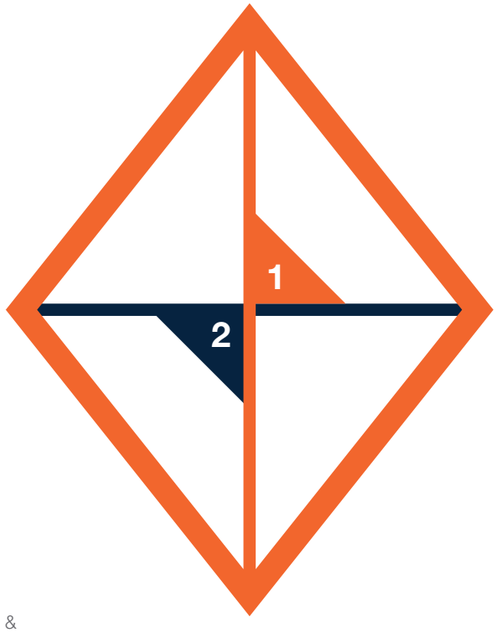
Example intelligence-driven adversary profile

1 SOCIO-POLITICAL AXIS
Intent: High
Target Geo: US, RU
Target Sector: FinSrv
Timeline: 2014 to present

2 TECHNICAL AXIS
Spear phishing, CSRF, SQLi
DNS hijack, paremeter tampering
ATM withdrawals

GROUP: Anunak/carbanak, **TYPE:** eCrime
MOTIVE: Financial or economic, **ORIGIN:** Russia

ADVERSARY



CAPABILITIES

FILES

6FF3AE5BA4E9A312602C8D44A398A02AB04
37378,58318739e970bbfa3ef45673f47b09ba
3fe3f20b,833a8d88be11807aae966d56a28af
7b3cc34dbcd,fb434ba4f1eaf9f7f20fe6449e43
75e90fa98069,af7564ee7959142c3b0d9eb81
29605c2ae582cb7,dcc932b878b374d47540d
43a2dee97f37d68267f,32aa4911bc5ab8098e
496cd88790ff7147ec6ac3,3d1cd366ffe90e25
c36c849d720ba6c7329dde7b

VIRLOCK

EXPLOITS
CVE-2012-2539,
CVE-2012-0158

TOOLS
Mimikatz, MBR Eraser, Network Scanner, Cain & Abel, SSHD backdoor, Ammy Admin, Team Viewer

INFRASTRUCTURE

IPS
78. 128.92(.)117
176.31.157(.)62

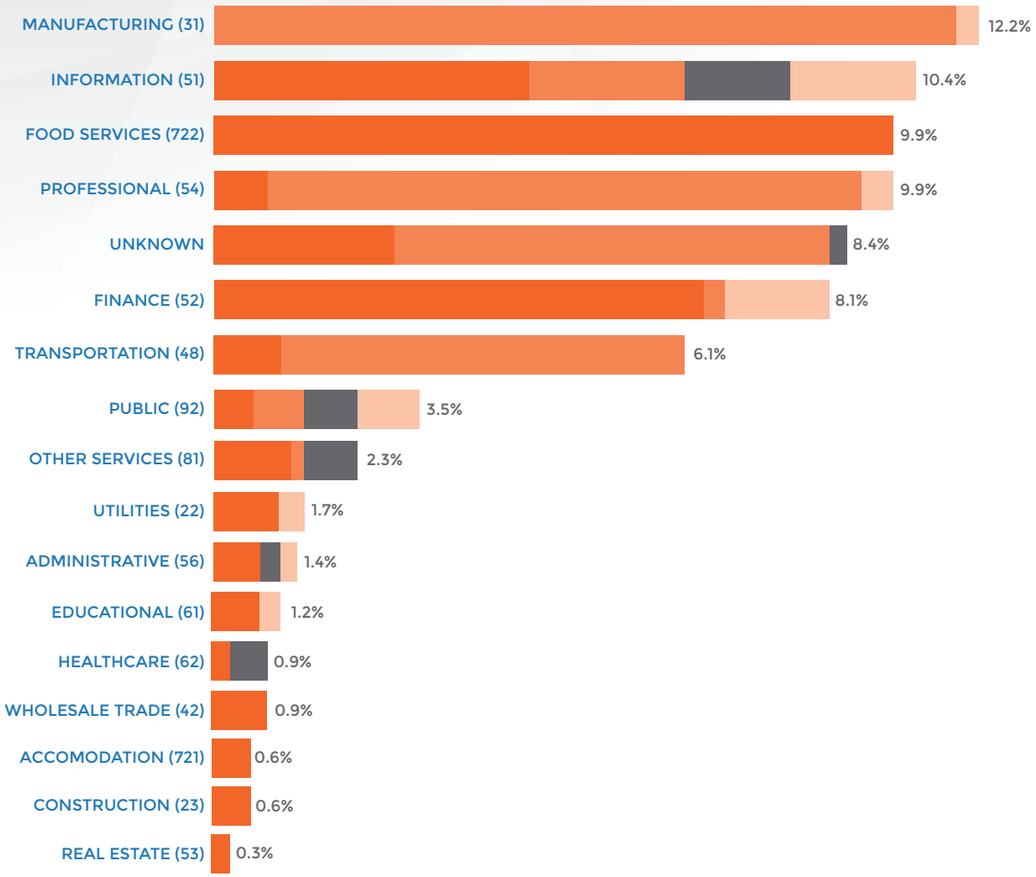
HOSTS
login.collegefa n[.]org
login. loginto[.]me
img. in-travelusa [.]com

KNOWN TO RENT ADVERSARY INFR

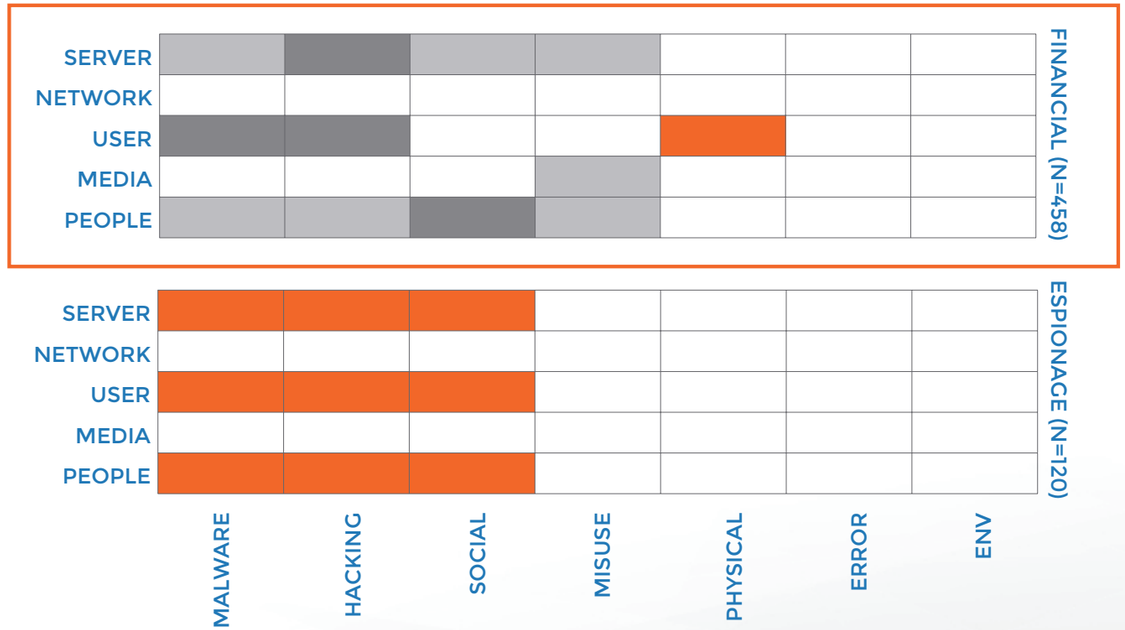
VICTIM

ORGANIZATIONS: Acme Corp (that's us), 50 Russian banks , British bank
ASSETS: Endpoints, servers, ATMs, SWIFT network

Example risk assessment project



Example intelligence-driven threat community profile **.... OVER TIME**



Crossing the Divide

Making it work in your organization

1. Initiate communication between intel and risk teams
2. Orient intel processes and products around desired risk factors
3. Identify threat communities of interest and create profiles
4. Establish guidelines and procedures for risk assessment projects
5. Encourage ongoing coordination and collaboration
   - Create centralized tools/repositories

~~Underlying assumption~~

Motivating conviction

Good **intelligence** makes smarter **models**;
Smarter models inform **decisions**;
Informed decisions drive better **practice**;
Better practice improves **risk** posture;
which, done efficiently,
Makes a successful security **program**.

www.ThreatConnect.com

THREAT CONNECT™

THANK YOU!

Bridging the Gap Between Threat Intelligence and Risk Management

Toni Gidwani
Director of Research Operations

ThreatConnect
@ThreatConnect