RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SEM-M02

The Marriage of Threat Intelligence and Risk Assessment

Wade Baker

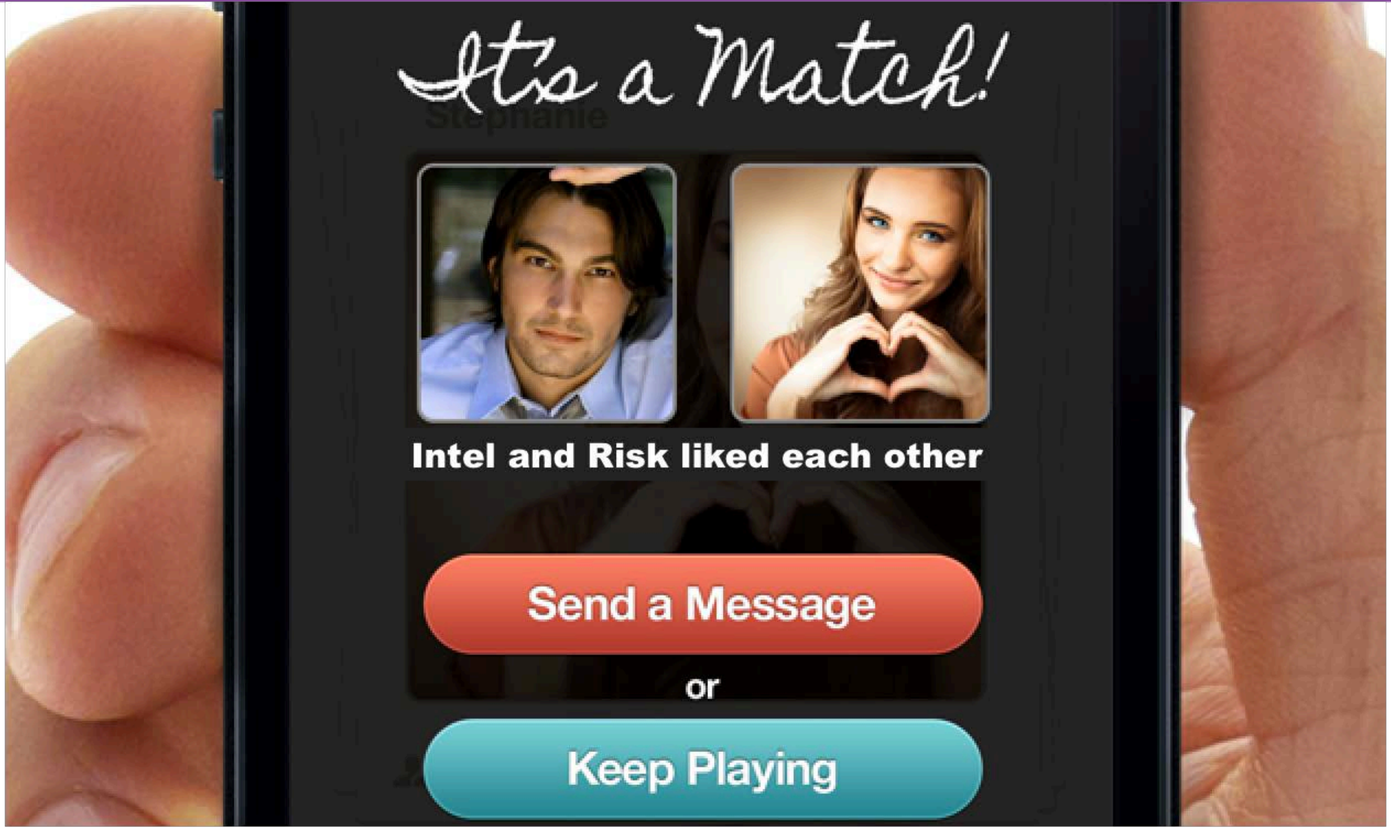
VP, Strategy & Risk Analytics
ThreatConnect
@wadebaker

#RSAC

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**.

Intel & Risk: Those two should hook up…



It's a Match!

Intel and Risk liked each other

…but they haven’t quite hit it off…

Threat Intelligence

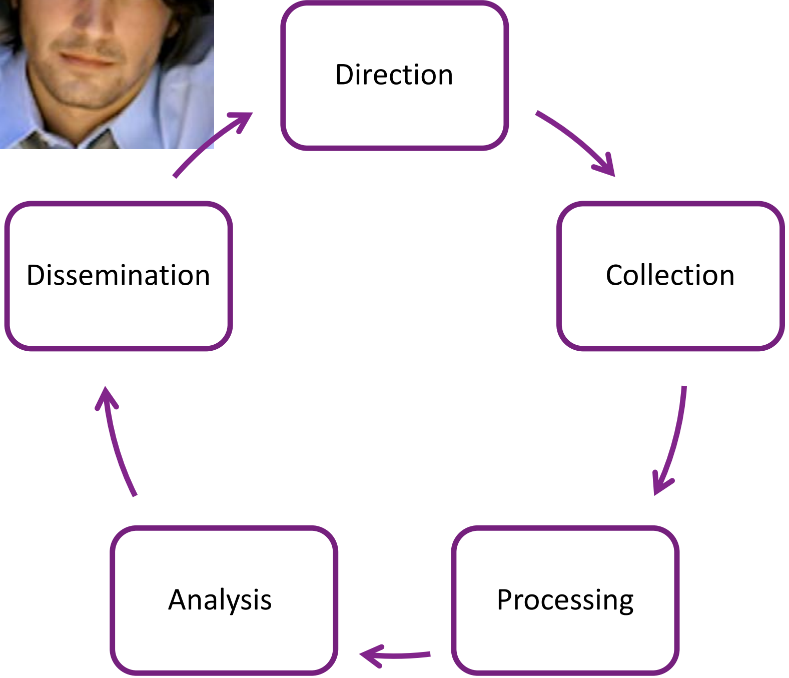
- “There’s way too much uncertainty in her life. I need something predictable.”
- “I’m a simple guy from the STIX and drive a TAXII; she’s a one-percenter by nature.”
- “Everything’s an assessment with her; I don’t want to be managed!”
- “Sure, she’s a great model now, but I worry about overfitting as she gets older.”

Risk Management

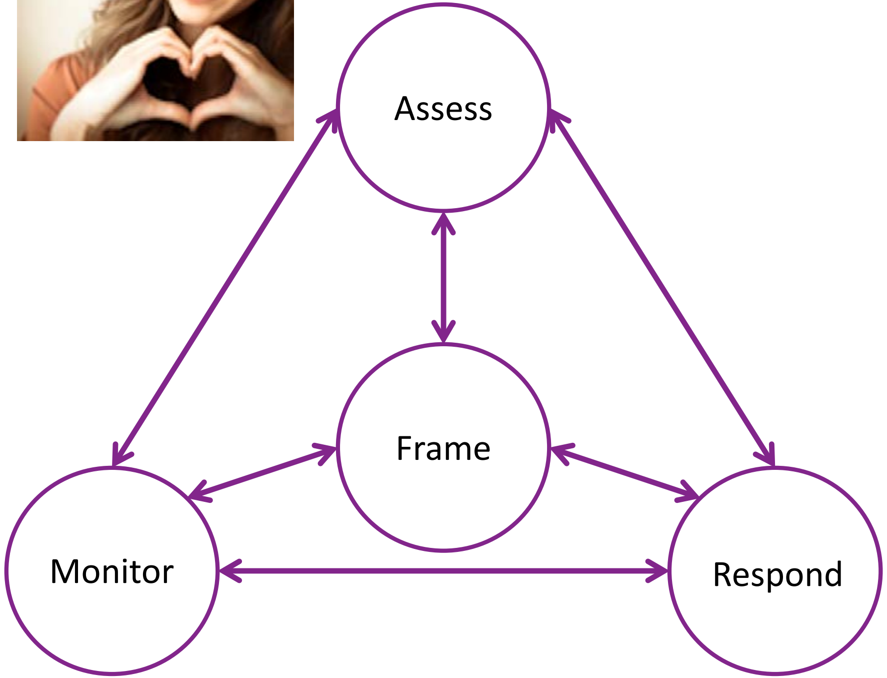
- “I feel like I’m under constant surveillance; he tries to control my private domain.”
- “I don’t like the way he treats me; he needs to just accept me as I am.”
- “He won’t open up and never shares. I swear, if he TLP-Red’s me one more time…”
- “What’s his deal with China, anyway? It’s uncomfortable around my Asian friends.”

...& they run in such different circles

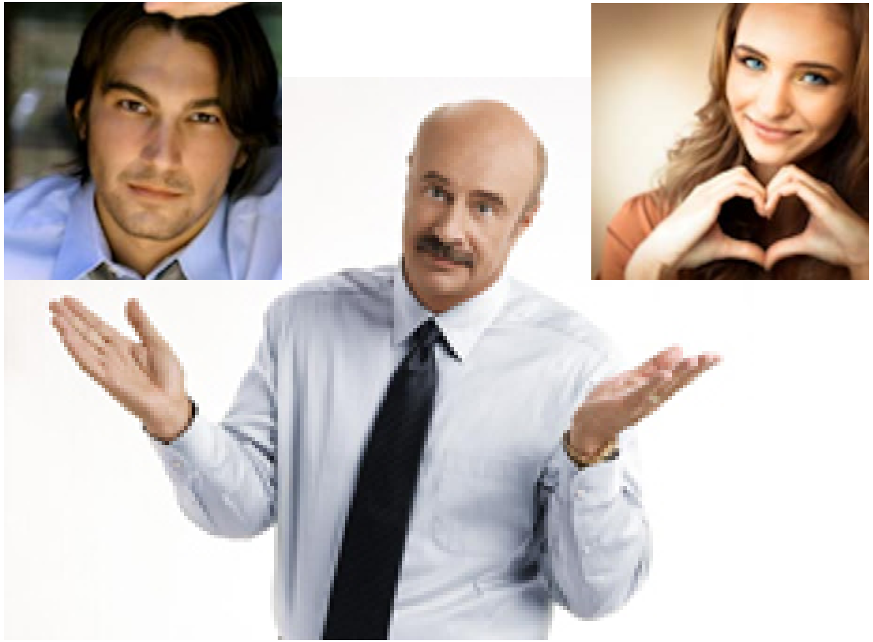
Threat Intelligence



Risk Management



Let’s help this young couple find love



Intel

Risk

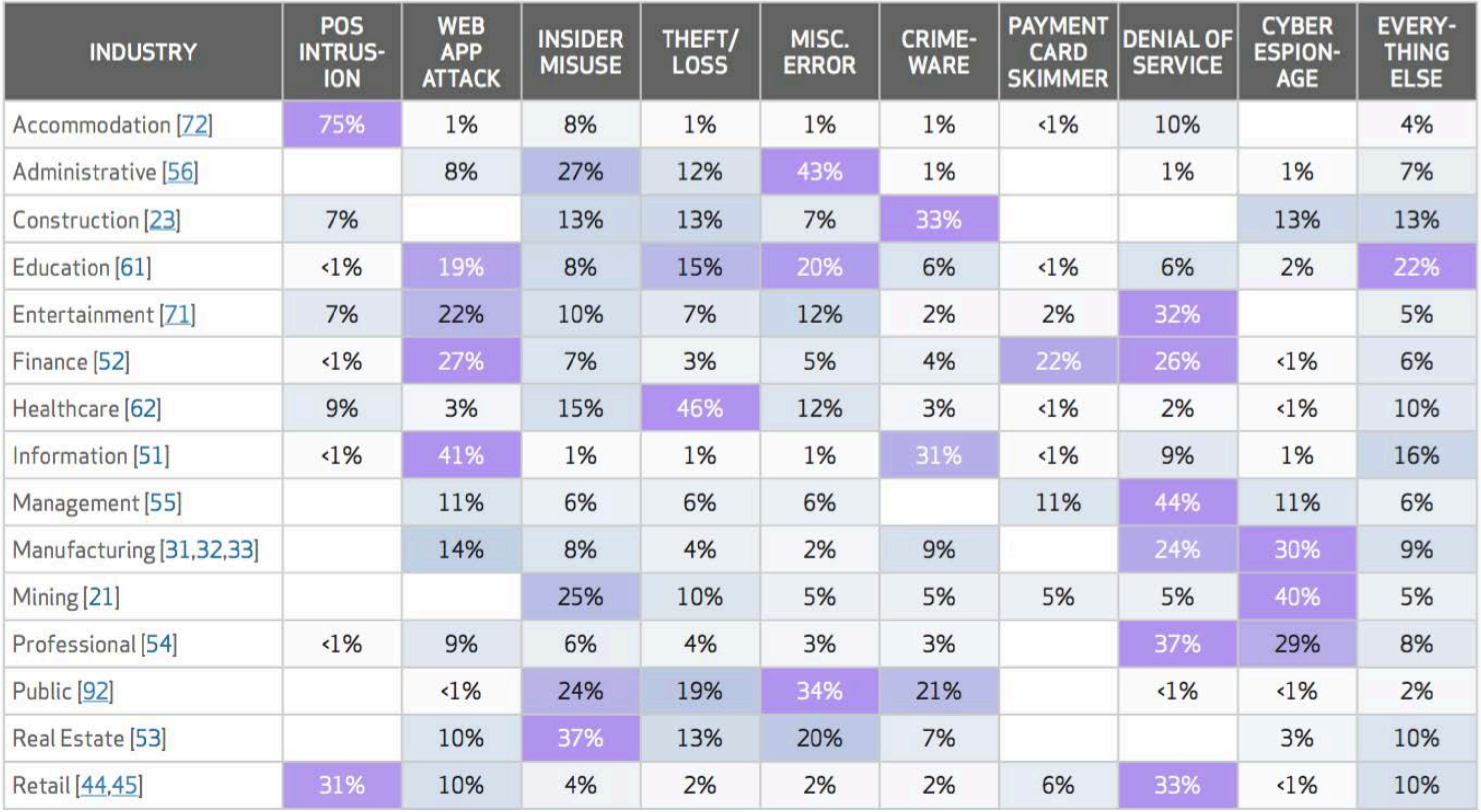
Agenda

- Marriage of Risk & IR in Verizon’s DBIR.
- *Dating*: Let’s get to know each other.
- *Love*: There’s something special here.
- *Marriage*: How does this actually work?

The Marriage of Risk and IR in Verizon's DBIR

Risk + IR = Love

Frequency of incident classification 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 [72]	75%	1%	8%	1%	1%	1%	<1%	10%		4%
Administrative [56]		8%	27%	12%	43%	1%		1%	1%	7%
Construction [23]	7%		13%	13%	7%	33%			13%	13%
Education [61]	<1%	19%	8%	15%	20%	6%	<1%	6%	2%	22%
Entertainment [71]	7%	22%	10%	7%	12%	2%	2%	32%		5%
Finance [52]	<1%	27%	7%	3%	5%	4%	22%	26%	<1%	6%
Healthcare [62]	9%	3%	15%	46%	12%	3%	<1%	2%	<1%	10%
Information [51]	<1%	41%	1%	1%	1%	31%	<1%	9%	1%	16%
Management [55]		11%	6%	6%	6%		11%	44%	11%	6%
Manufacturing [31,32,33]		14%	8%	4%	2%	9%		24%	30%	9%
Mining [21]			25%	10%	5%	5%	5%	5%	40%	5%
Professional [54]	<1%	9%	6%	4%	3%	3%		37%	29%	8%
Public [92]		<1%	24%	19%	34%	21%		<1%	<1%	2%
Real Estate [53]		10%	37%	13%	20%	7%			3%	10%
Retail [44,45]	31%	10%	4%	2%	2%	2%	6%	33%	<1%	10%

Figure from Verizon 2014 DBIR

Dating:
Let’s get to know each other

What is threat intelligence?

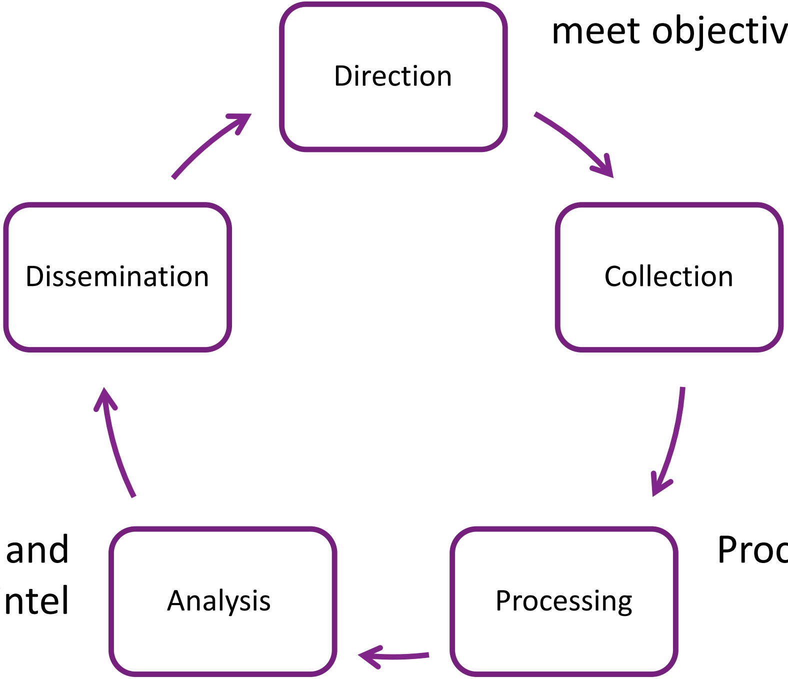
“Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject’s response to that menace or hazard.”

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



Direction

Plan intel requirements to meet objectives

Collection

Collect intel in support of requirements

Processing

Process intel for exploitation

Analysis

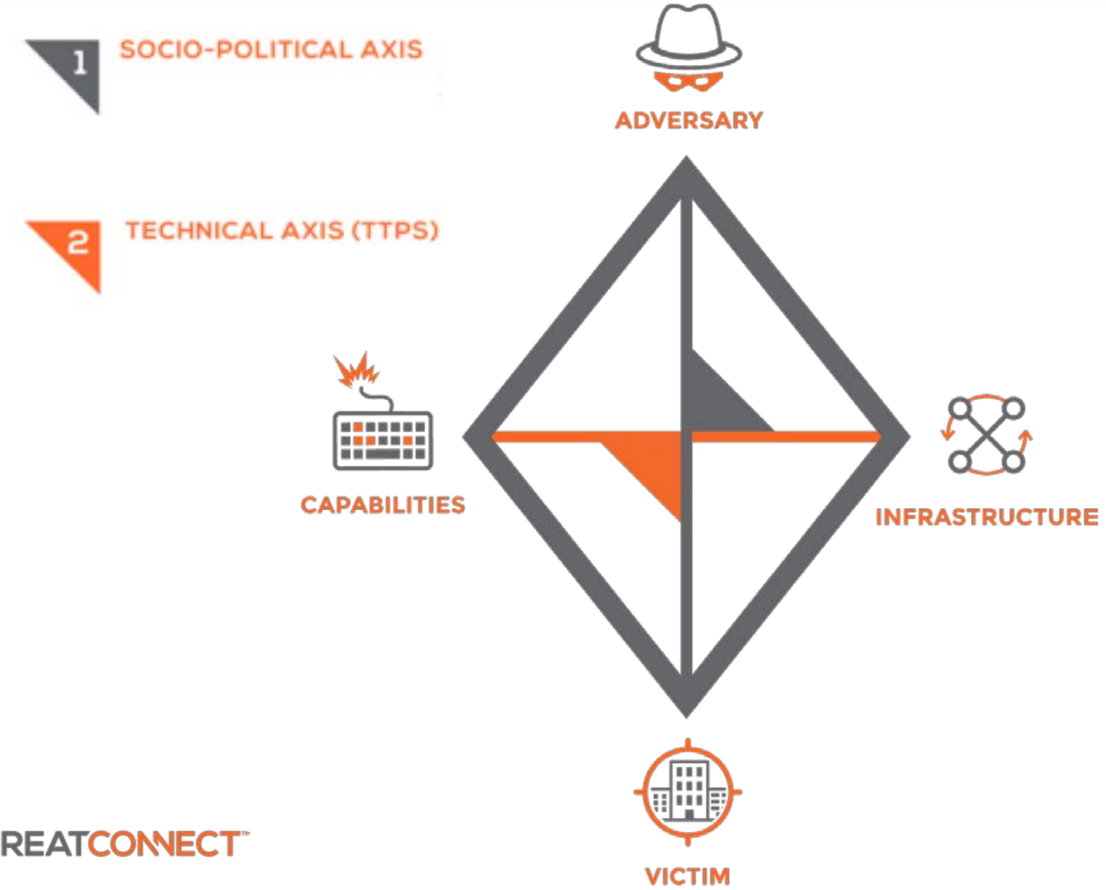
Evaluate, integrate, and interpret intel

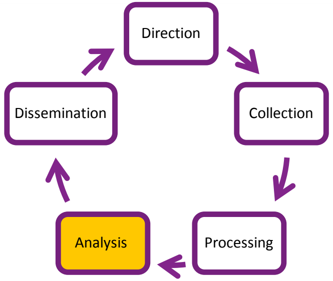
Dissemination

Distribute finished intel products

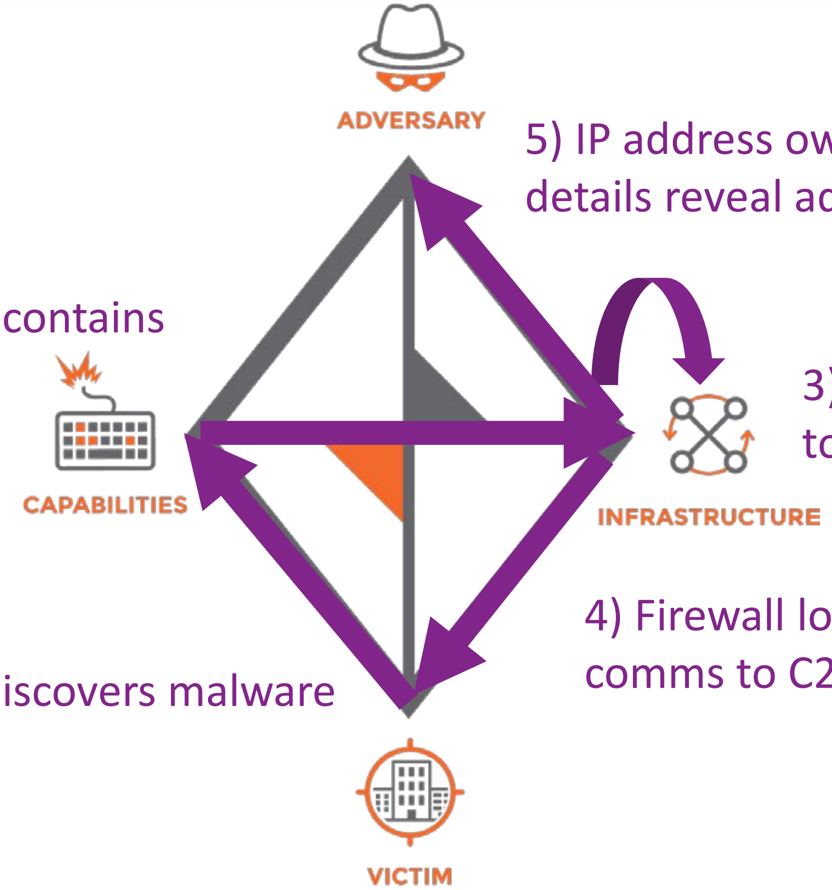
Threat intelligence process

The Diamond Model of Intrusion Analysis





Threat intelligence process



5) IP address ownership details reveal adversary

2) Malware contains C2 domain

3) C2 domain resolves to IP address

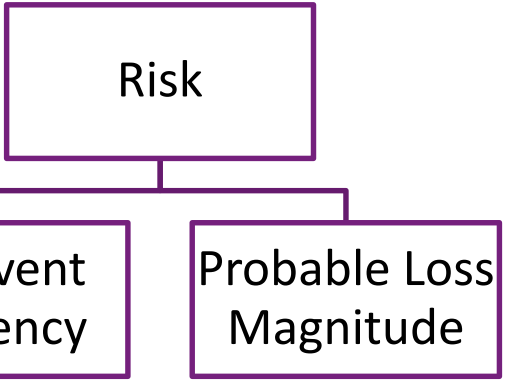
4) Firewall logs reveal more comms to C2 IP

1) Victim discovers malware

What is risk?

“The probable frequency and probable magnitude of future loss”

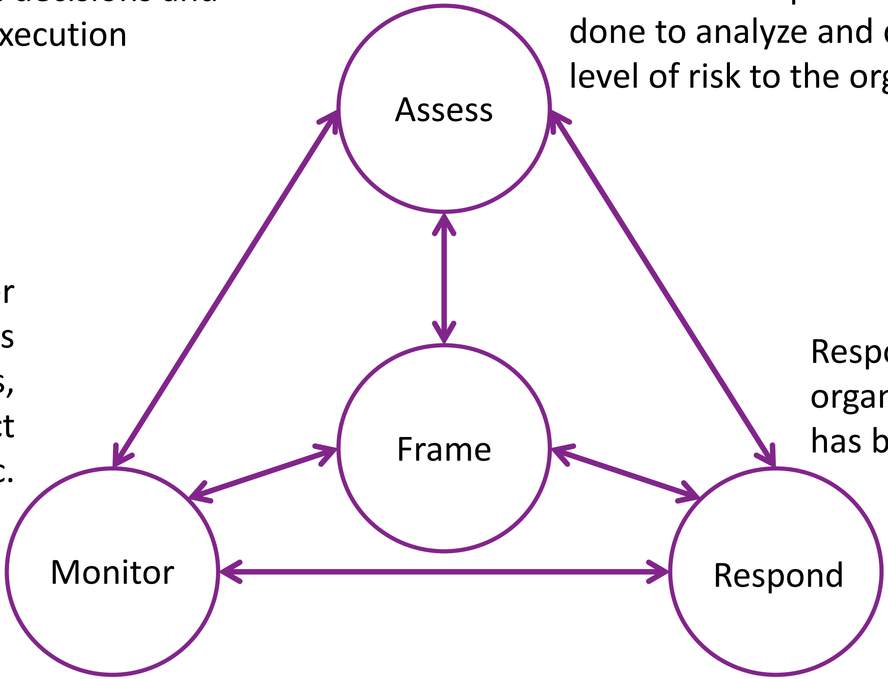
- Factor Analysis of Information Risk (FAIR)



Risk management process (NIST 800-39)

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

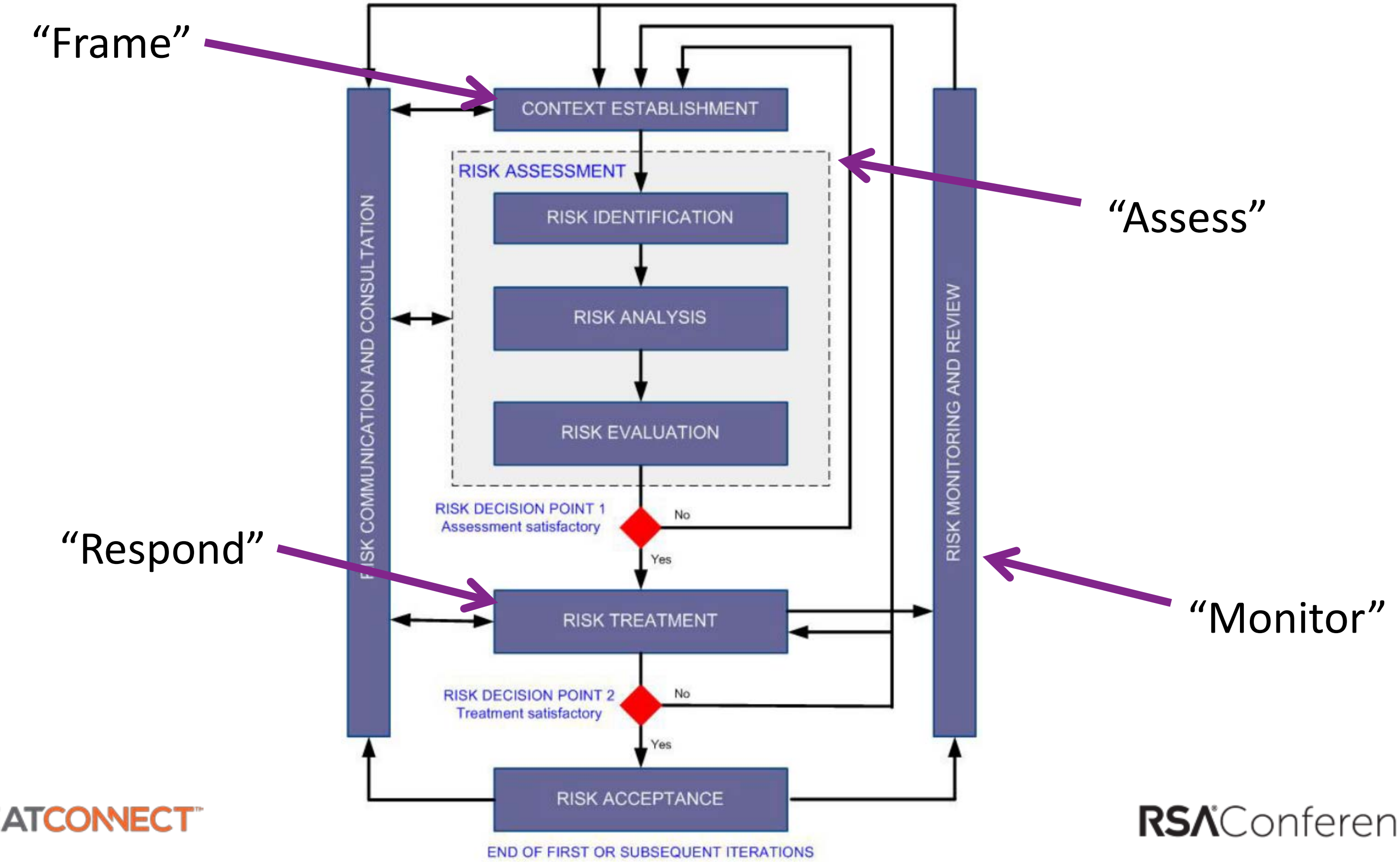
Assess: encompasses everything done to analyze and determine the level of risk to the organization.



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)



Love:

There’s something special here

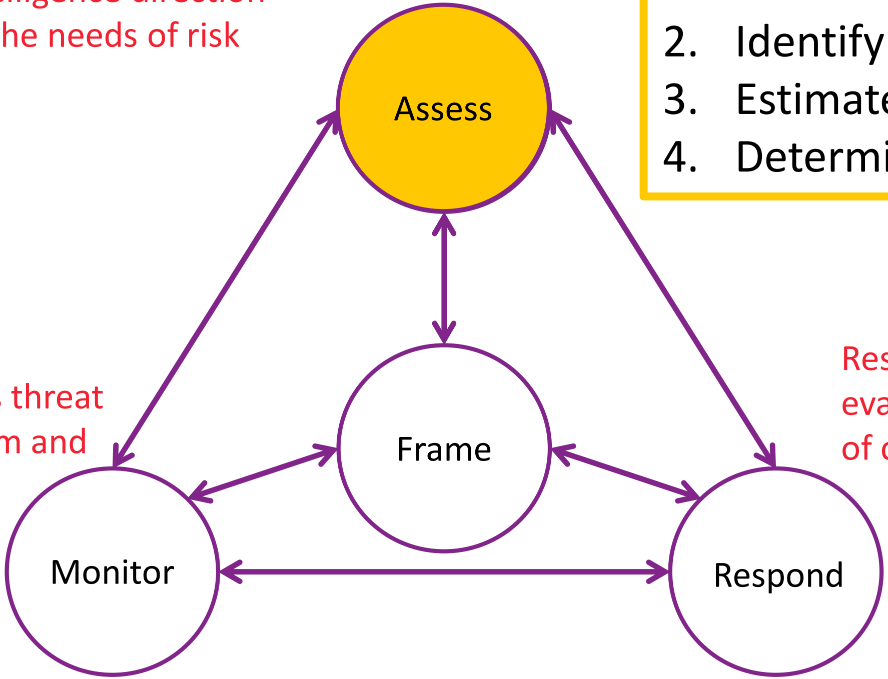
Risky questions needing intelligent answers

- 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

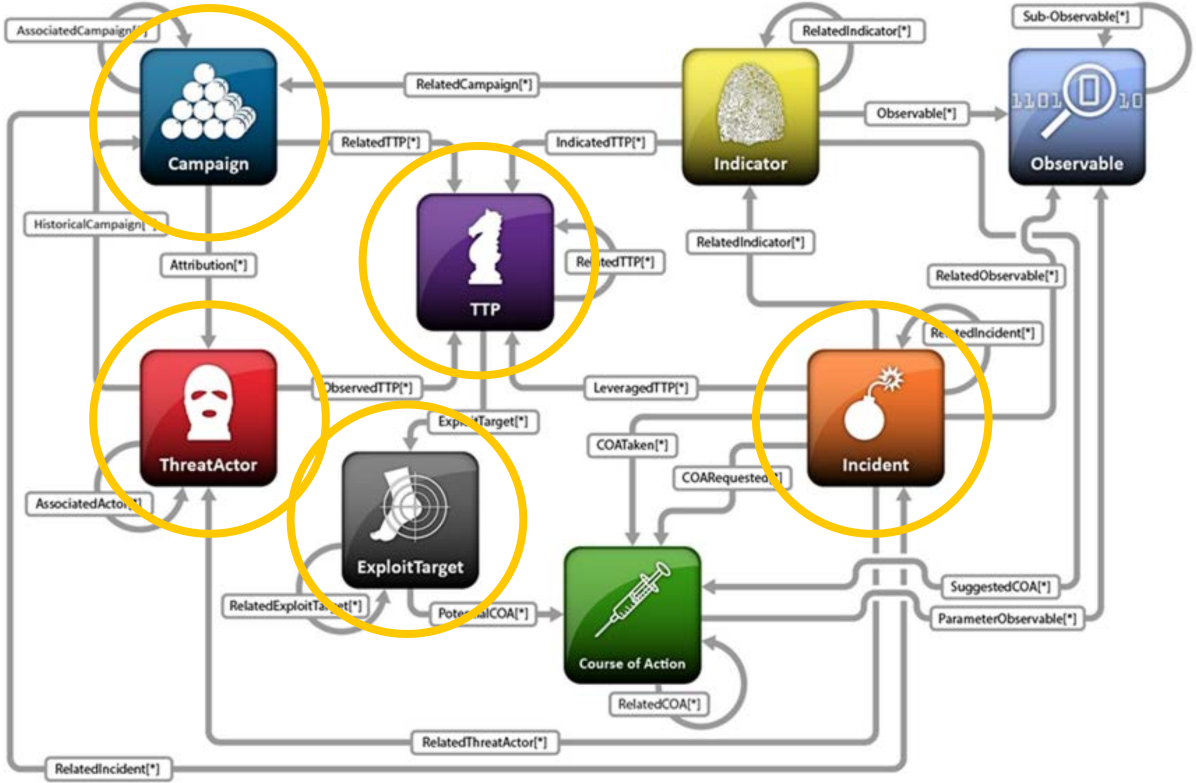


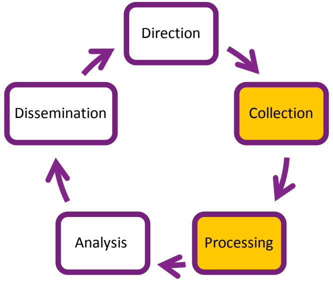
Monitor: intelligence tracks threat changes that warrant system and control changes

Respond: intelligence supports evaluation and implementation of courses of action

Building a model relationship

Structured Threat Information eXpression (STIX)





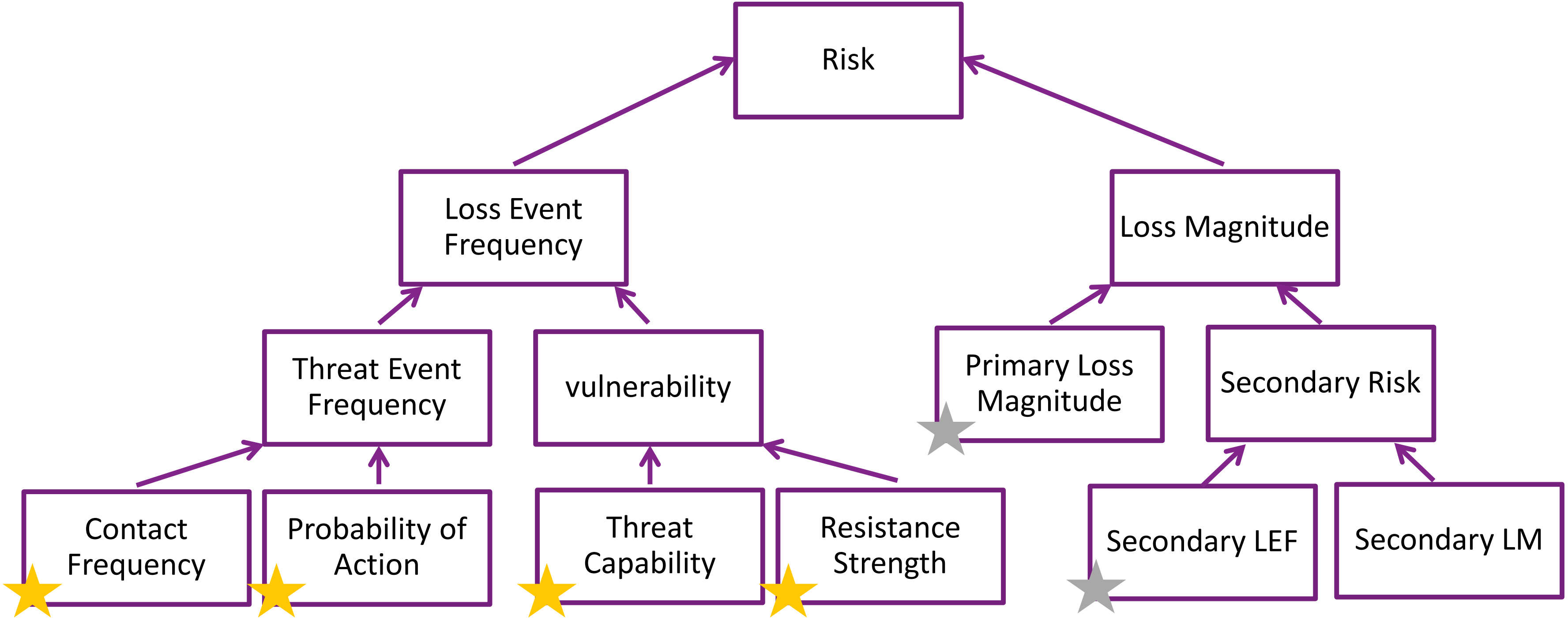
Source: https://stixproject.github.io/

THREATCONNECT™

RSAConference2016

Building a model relationship

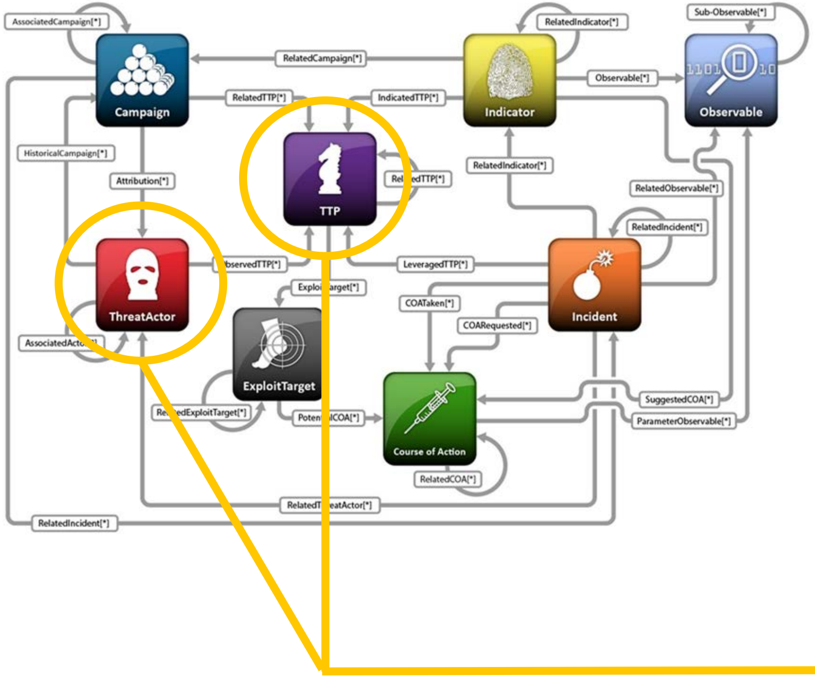
Factor Analysis of Information Risk (FAIR)



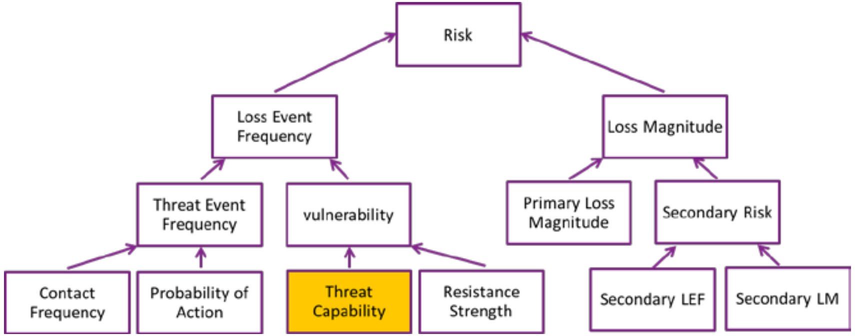
Building a model relationship

Finding mutual interests and activities

Threat Intel (STIX)



Risk Analysis (FAIR)


Risk

Loss Event Frequency

Loss Magnitude

Threat Event Frequency

vulnerability

Primary Loss Magnitude

Secondary Risk

Contact Frequency

Probability of Action

Threat Capability

Resistance Strength

Secondary LEF

Secondary LM

- *Type* *Behavior*
- *Resources* *Sophistication*
- *Kill_Chain_Phases* *Planning_And_Support*
- *Exploit_Target* *Intended_Effect*
- *Observed_TTPs*

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

And they lived happily ever after!

Marriage:

How does this actually work?

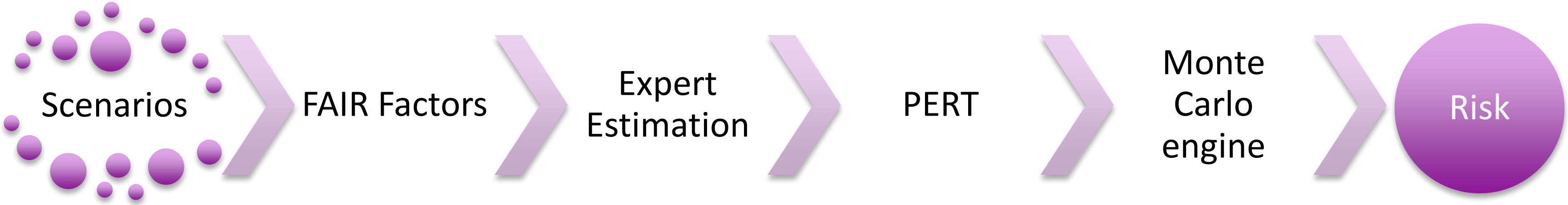
Example risk assessment project

“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

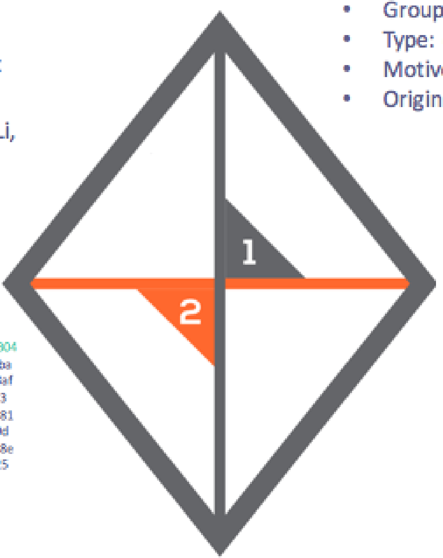
Example intelligence-driven adversary profile

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

2 TECHNICAL AXIS (TTPS)
- Spear phishing, CSRF, SQLi, DNS hijack, Paremeter tampering
- ATM withdrawals

ADVERSARY

- Group: Anunak/Carbanak
- Type: eCrime
- Motive: Financial or economic
- Origin: Russia



CAPABILITIES

- Files
  - 6FF3AE5BA4E9A312602CBD44A398A02AB0437378,58318739e970bbfa3ef45673f47b09ba3fe3f20b,833a8d88be11807bae966d56b28af7b3cc34dbcd,fb434ba4f1eaf9f7f20fe6f49c4375e90fa98069,af7564ee7959142c3b0d9eb8129605c2ae582cb7,dcc932b878b374d47540d43a2dee97f37d682671,32aa4911bc6ab8098e496cd88790ff7147ec6ac3,3d1cd366ffe90e25c36c849d720ba6c7329dde7b
- VIRLOCK
- Exploits
  - CVE-2012-2539,CVE-2012-0158
- Tools
  - Mimikatz, MBR Eraser, Network Scanner, Cain & Abel, SSHD backdoor, Ammy Admin, Team Viewer

INFRASTRUCTURE

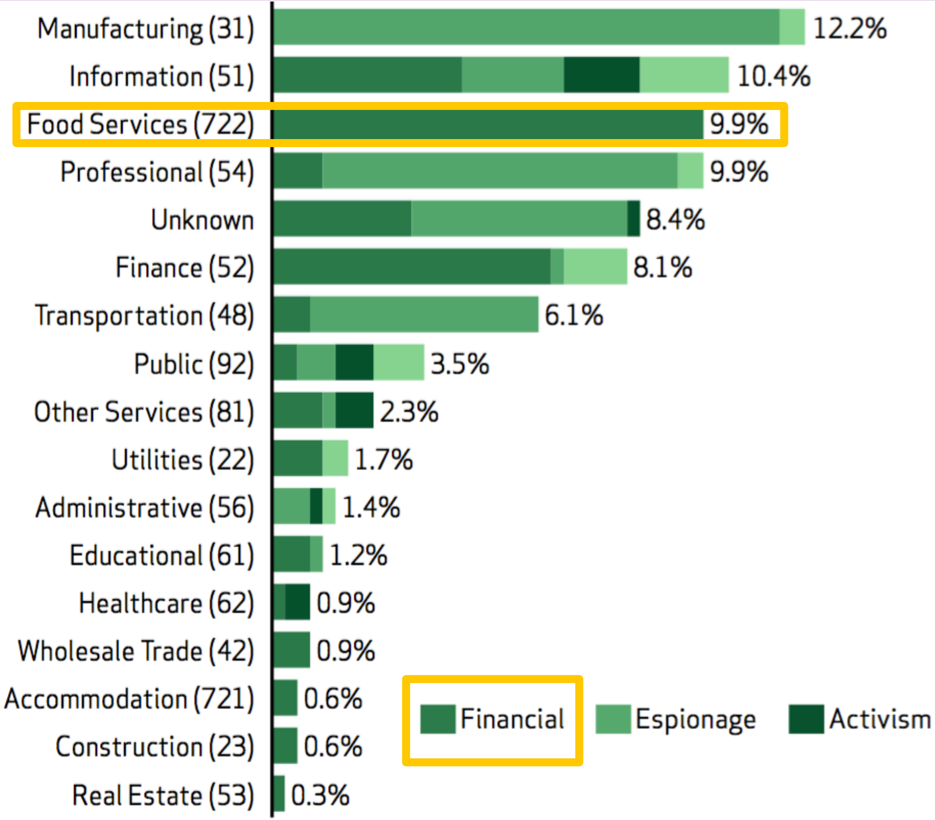
- IPs
  - 78.128.92[.]117
  - 176.31.157[.]62
- Hosts
  - login.collegefan[.]org
  - login.loginto[.]me
  - img.in-travelusa[.]com
- Known to rent adversary infr

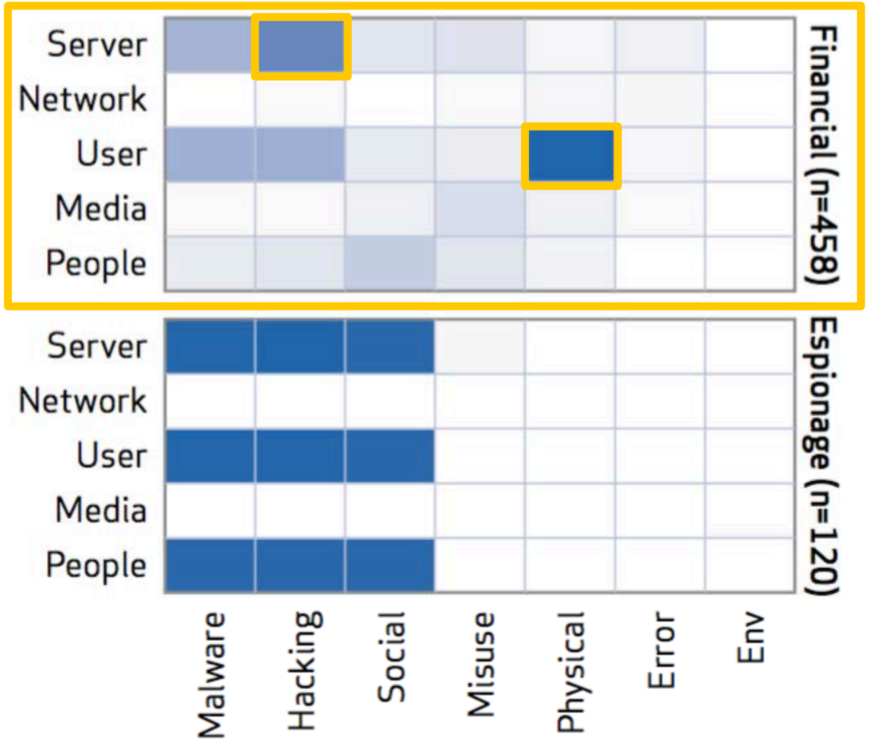
VICTIM

- 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





Making it work in your organization

1. Initiate communication between intel & risk teams
2. Orient intel processes & products around desired risk factors
3. Identify threat communities of interest and create profiles
4. Establish guidelines & procedures for risk assessment projects
5. Encourage ongoing coordination & 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**.

RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SEM-M02

The Marriage of Threat Intelligence and Risk Assessment

THANK YOU!!

Wade Baker

VP, Strategy & Risk Analytics
ThreatConnect
@wadebaker

#RSAC