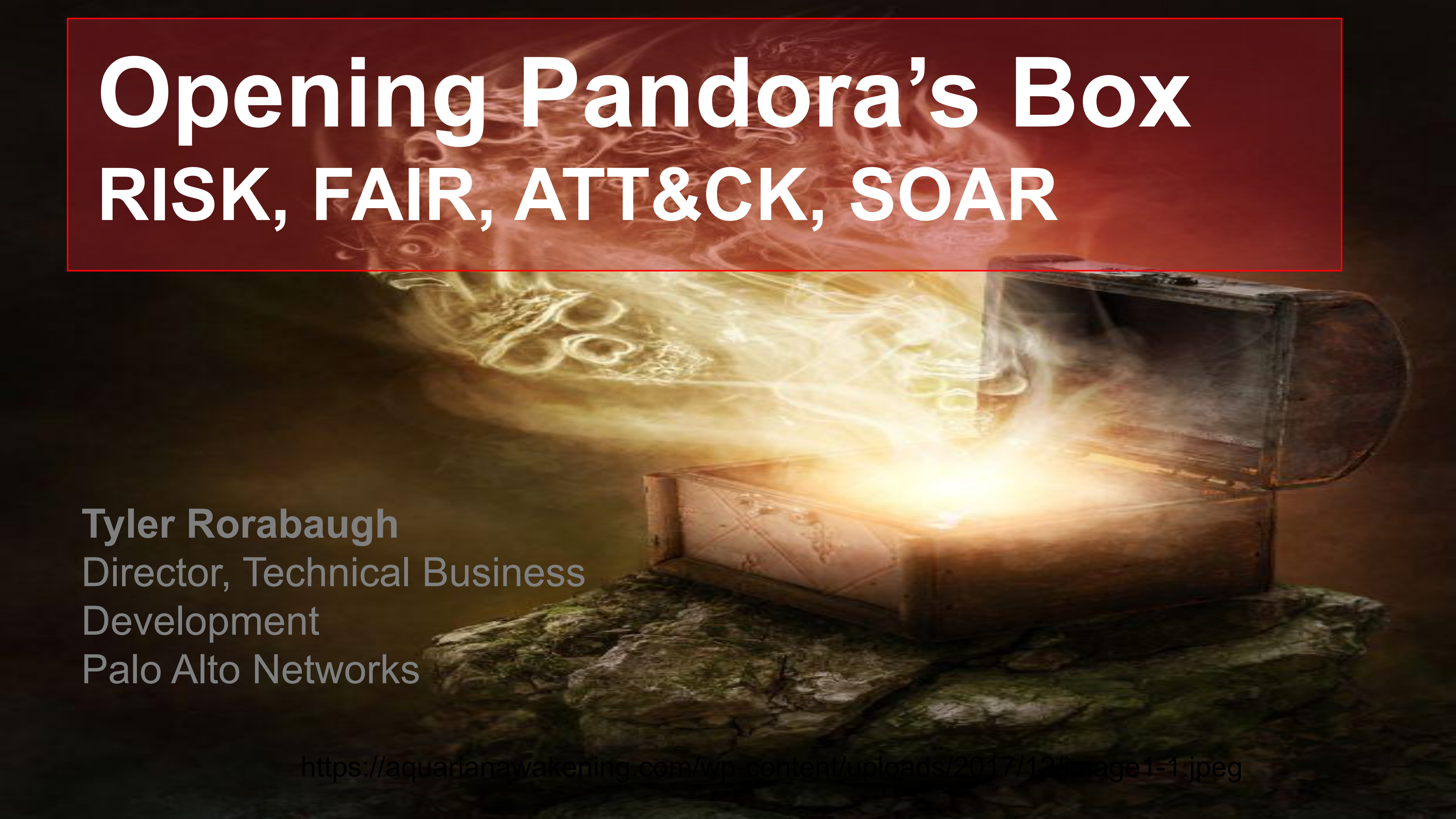
Opening Pandora's Box

RISK, FAIR, ATT&CK, SOAR



Tyler Rorabaugh
Director, Technical Business Development
Palo Alto Networks

https://aquarianawakening.com/wp-content/uploads/2017/12/image1-1.jpeg

Agenda (In Hacker Green Of Course)

- ➔ Story Time
- ➔ What is RISK? No seriously, What is RISK?
- ➔ FAIR Overview
- ➔ Mitre ATT&CK
- ➔ SOAR at a glance
- ➔ Modeling a scenario RISK + ATT&CK + SOAR
- ➔ Questions

Story Time

What 4 Simple Questions Did I Ask?

#1

What is the largest cyber security RISK to your organization?

#2

What are the ASSETS that hold the most value in your organization?

#3

If ______ was breached, how do you RESPOND today?

#4

If ________ was breached, what is the financial or reputational **LOSS** that could occur?

How did they RESPOND?

Over 40% →

Only 1 Great Answer

“We know exactly what percentage and where the financial losses come from, they come from Fraud Events”

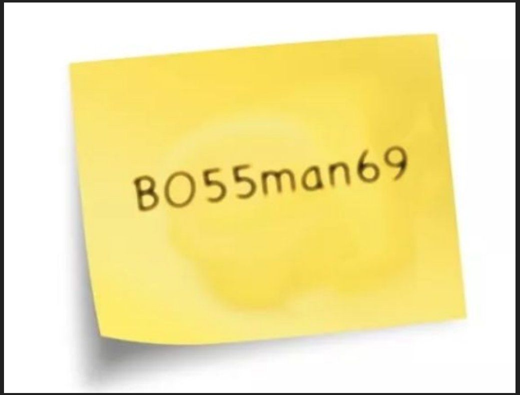
What is RISK?

LIBERTAS
AEQVITAS
FELICITAS
PAX
CONCORDIA
VIRTVS
SPES
Iulio Bonasone f.

RISK = Loss Exposure

In business that generally means financial loss...

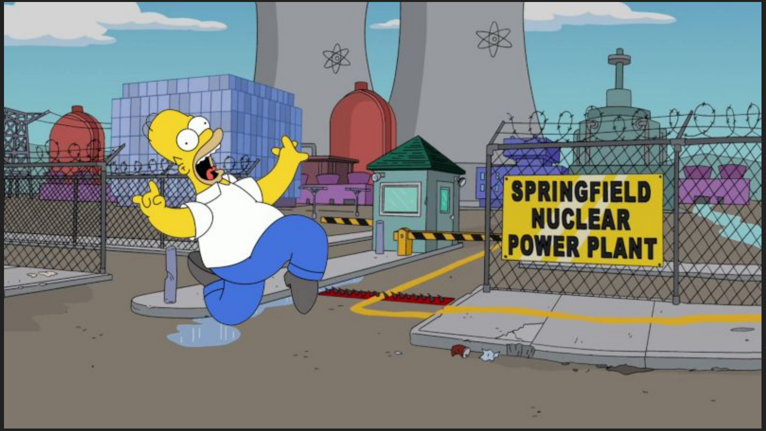
When thinking
in terms of RISK…
is this password
an Asset or a Control?



If the password opens a door to this →

Then in terms of RISK it is probably not an Asset

But if the password opened a door to an energy plant or shut it down...then someone, somewhere would definitely consider the password to be an Asset!



If a password is an asset, from a RISK perspective….

Are you concerned about the passwords?

Or the places, data, and applications, the passwords provide access to?

Or about the effects or loss that could occur?

When you think about RISK, you must be crystal clear on what you consider a real Asset.

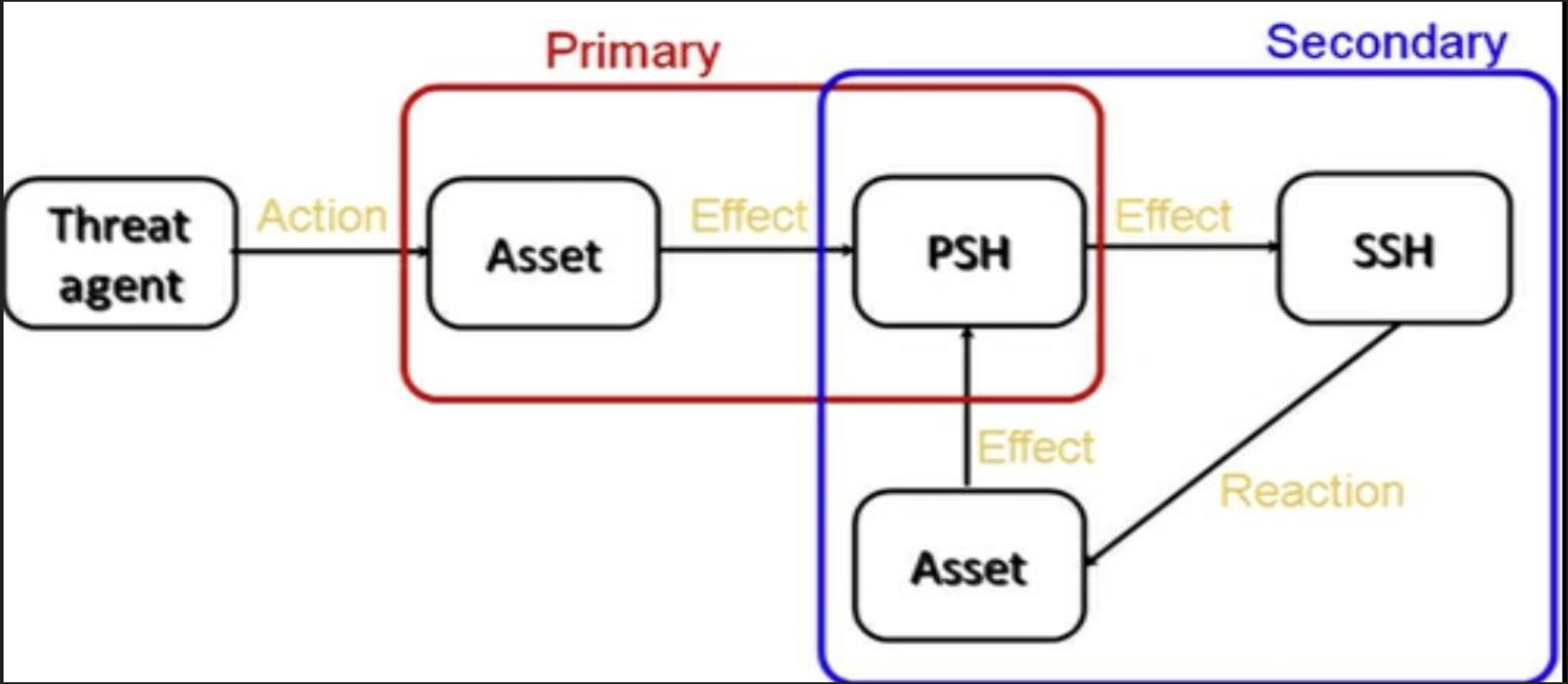
Without being crystal clear on what we consider an Asset...

We can not think or calculate the potential or probability of Loss Exposure!

When Zeus created pandora's box as a gift and the gift was opened evil poured out…almost like lava burning and covering everything in its path

LIBERTAS
AEQVITAS
CONCORDIA
FELICITAS
PAX
SALVS
VIRTVS
SPES
Iulio Bonaſone f.

That’s Kind Of How Loss Flow Works



What Types Of Loss Flows Are There?

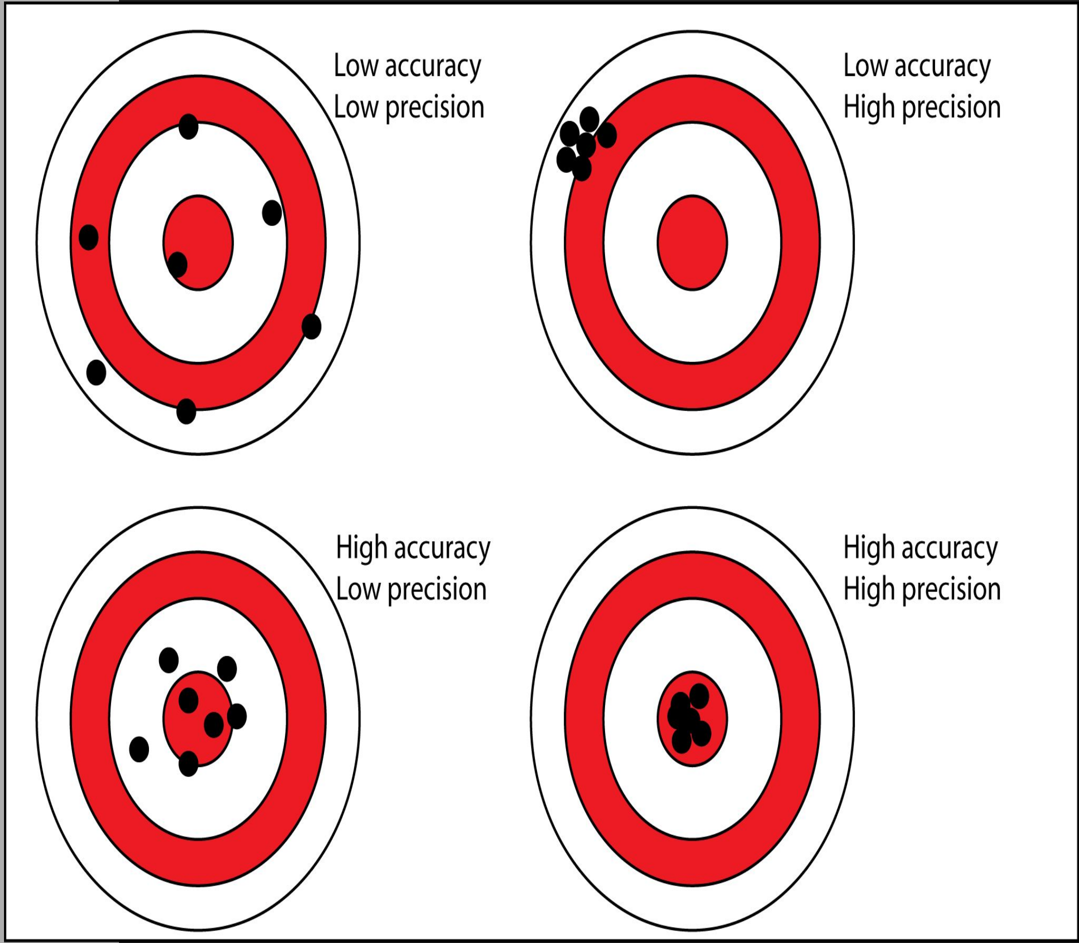
In RISK frameworks like FAIR, Loss for both primary and secondary stakeholders include:

- **Loss in productivity**
- **Response costs**
- **Replacement costs**
- **Competitive advantage**
- **Fines and judgments**
- **Reputational Damage**

What Is FAIR?
Factor Analysis of Information Risk

FAIR
INSTITUTE

In FAIR,
Accuracy is better
than Precision



FAIR - Its A Way Of Measuring Risk

Explained as a recipe

1 pt Ontology / Taxonomy

1 pt Risk Terminology (TE, TEF, LE, LEF, CF, POA......)

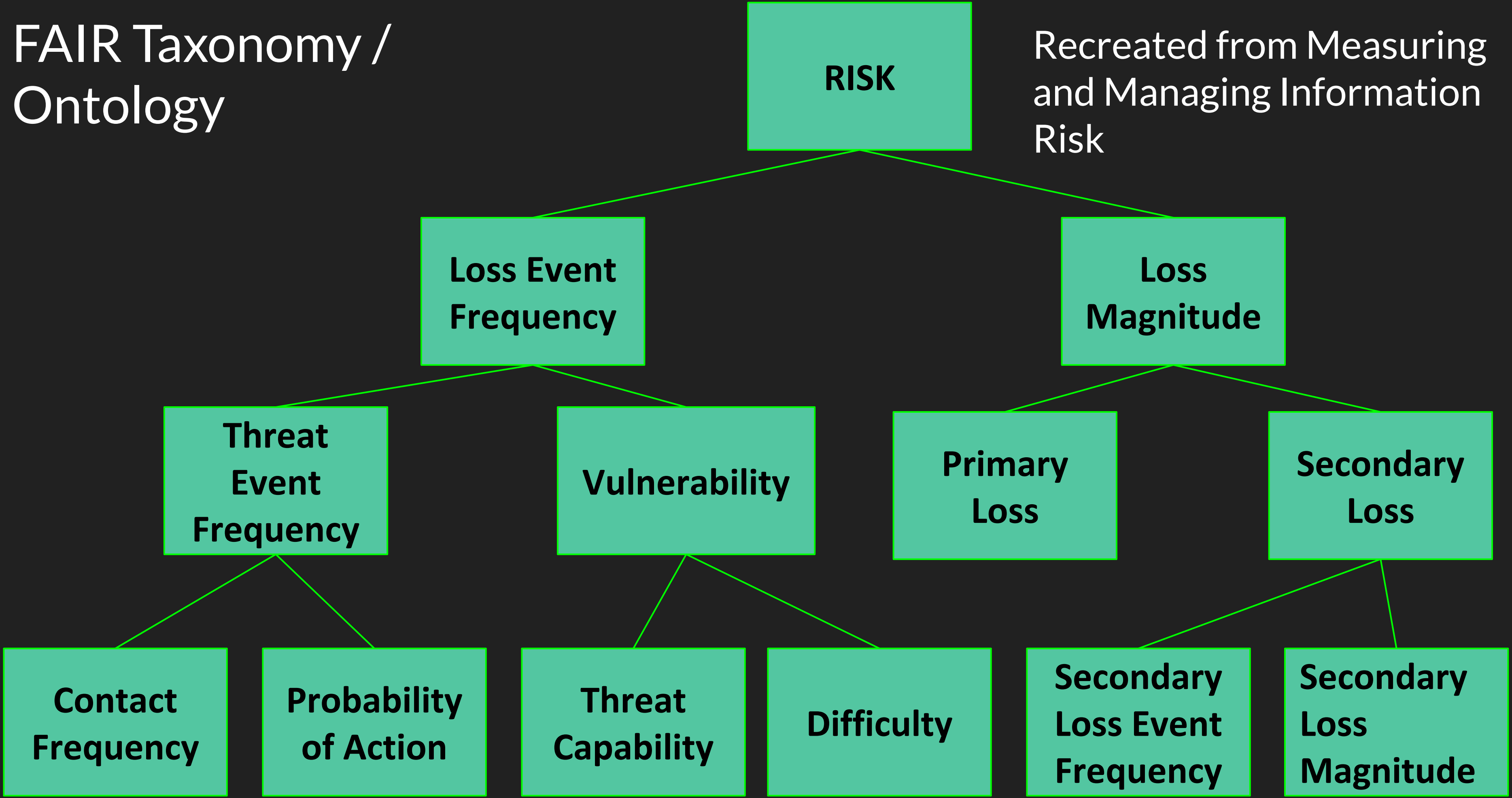
1 pt Data Gathering

1 pt Probability, Normalized Distributions

- **½ pt PERT Formula using 3 point estimates (spread between minimum, most likely, to least likely)**
- **½ pt Monte Carlo Simulation**

FAIR Taxonomy / Ontology

Recreated from Measuring and Managing Information Risk



Slimmed Down Version (Not Full Process)

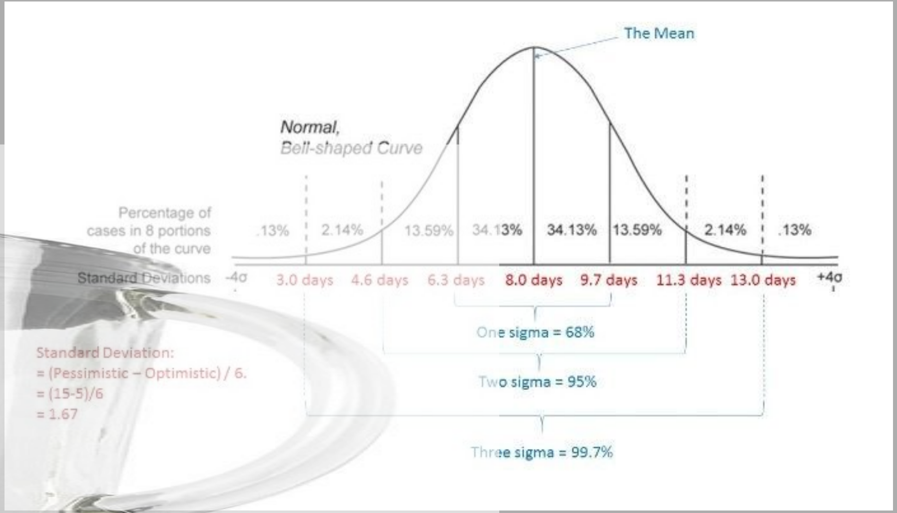
- Identify Scenario
  - Asset
  - Threat Community
- Evaluate Loss Event Frequency (LEF)
  - Estimate Threat Event Frequency (TEF)
  - Estimate Threat Capabilities (TCAP)
  - Estimate Difficulty
  - Determine Vulnerability
  - Determine Primary Loss Event Frequency (PLEF)
  - Determine Secondary Loss Event Frequency (SLEF)
- Estimate Probability Loss Magnitude (PLM)
- Estimate Probability Secondary Loss Magnitude (SLM)
- Determine Primary and Secondary Risk
- Determine overall RISK

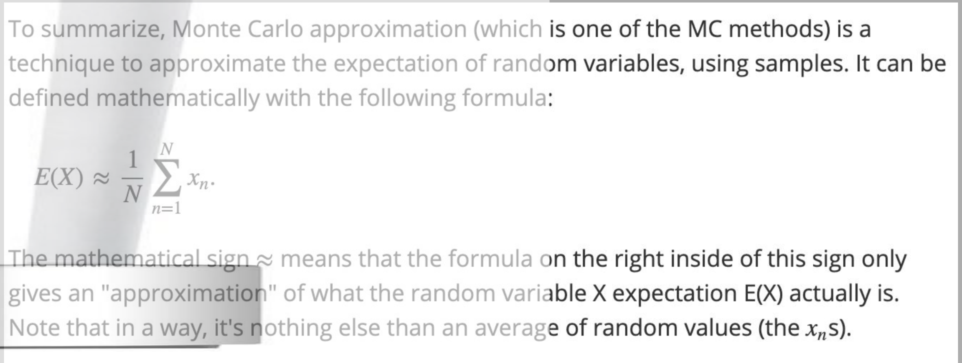
Credit: Measuring and Managing Information Risk

FAIR - Stick All Of This In The FAIR Blender

LEF Min	LEF Most Likely	LEF Max	Data Gathering Confidence
0.3 once every 3 years	0.5 once every 2 years	3 three times a year	Low
TEF Min	TEF Most Likely	TEF Max	Data Gathering Confidence
0.015	0.05	0.6	Low

LOSS MAGNITUDE	MIN RESPONSE COST	MIN REPLACEMEN T	Data Gathering Confidence
PRIMARY	$500,000	$2900	Low
SECONDARY	$1,300,00	$30,600,000	Medium





To summarize, Monte Carlo approximation (which is one of the MC methods) is a technique to approximate the expectation of random variables, using samples. It can be defined mathematically with the following formula:

$$E(X) \approx \frac{1}{N} \sum_{n=1}^{N} x_n.$$

The mathematical sign ≈ means that the formula on the right inside of this sign only gives an "approximation" of what the random variable X expectation E(X) actually is. Note that in a way, it's nothing else than an average of random values (the x_ns).

Stop... This All Seems Too Complicated...

Basically FAIR allows us to COMMUNICATE in the terms of RISK and understand potential financial loss...

To

BUSINESS PEOPLE!

What is Mitre Att&CK

Pew Pew Pew…….

MITRE | ATT&CK™

Mitre Att&CK

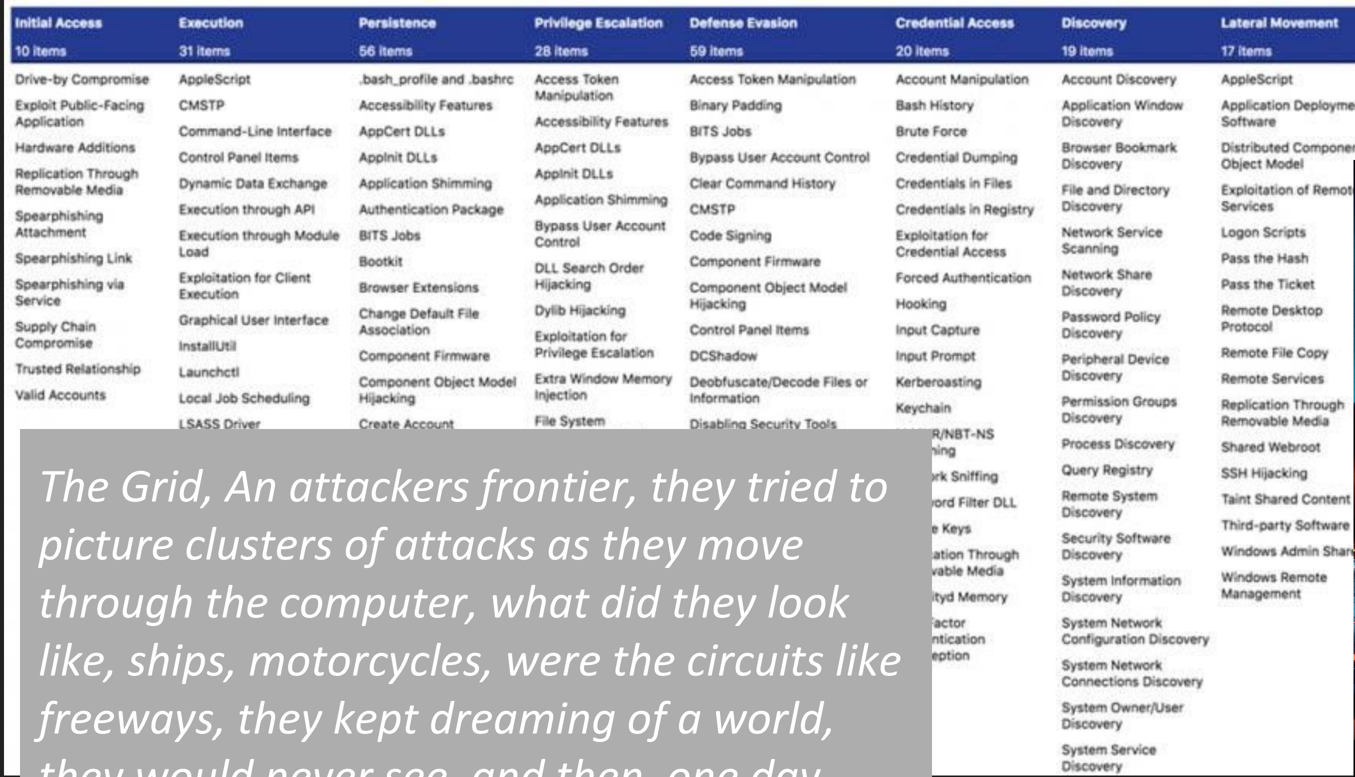
Book Definition….

MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

Recipe

Attacker/ threat taxonomy/ontology:
1pt Tactics
1pt Techniques
1pt Procedures
Mix in numbers, with a coverage matrix

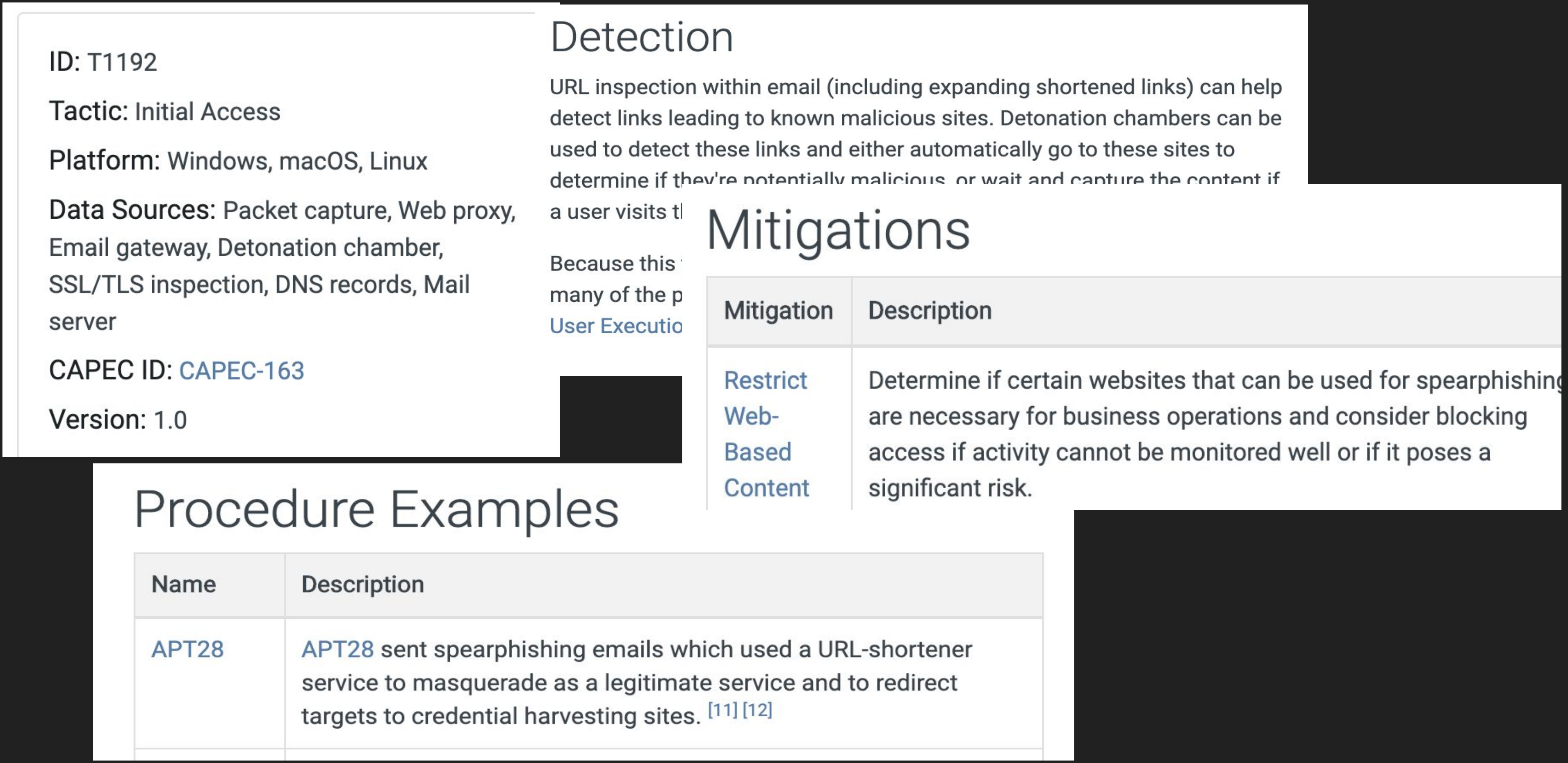
The Grid (Reminds me of the movie Tron)



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remot	Data from Information	Data Transfer Size	
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts			
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash			
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket			
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol			
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy			
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services			
	Launchctl	Component Firmware	File System	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media			
	Local Job Scheduling	Component Object Model Hijacking		Deobfuscate/Decode Files or Information	Kerberoasting	Remote System Discovery	Shared Webroot			
	LSASS Driver	Create Account		Disabling Security Tools	Keychain	Security Software Discovery	SSH Hijacking			
					R/NBT-NS ning	System Information Discovery	Taint Shared Content			
					rk Sniffing	System Network Configuration Discovery	Third-party Software			
					ord Filter DLL	System Network Connections Discovery	Windows Admin Shar			
					e Keys	System Owner/User Discovery	Windows Remote Management			
					ation Through vable Media	System Service Discovery				
					ityd Memory					
					Factor ntication eption					

The Grid, An attackers frontier, they tried to picture clusters of attacks as they move through the computer, what did they look like, ships, motorcycles, were the circuits like freeways, they kept dreaming of a world, they would never see, and then, one day, they got in...

Quick Example



ID: T1192

Tactic: Initial Access

Platform: Windows, macOS, Linux

Data Sources: Packet capture, Web proxy, Email gateway, Detonation chamber, SSL/TLS inspection, DNS records, Mail server

CAPEC ID: CAPEC-163

Version: 1.0

Detection

URL inspection within email (including expanding shortened links) can help detect links leading to known malicious sites. Detonation chambers can be used to detect these links and either automatically go to these sites to determine if they're potentially malicious, or wait and capture the content if a user visits tl

Because this
many of the p
User Executio

Mitigations

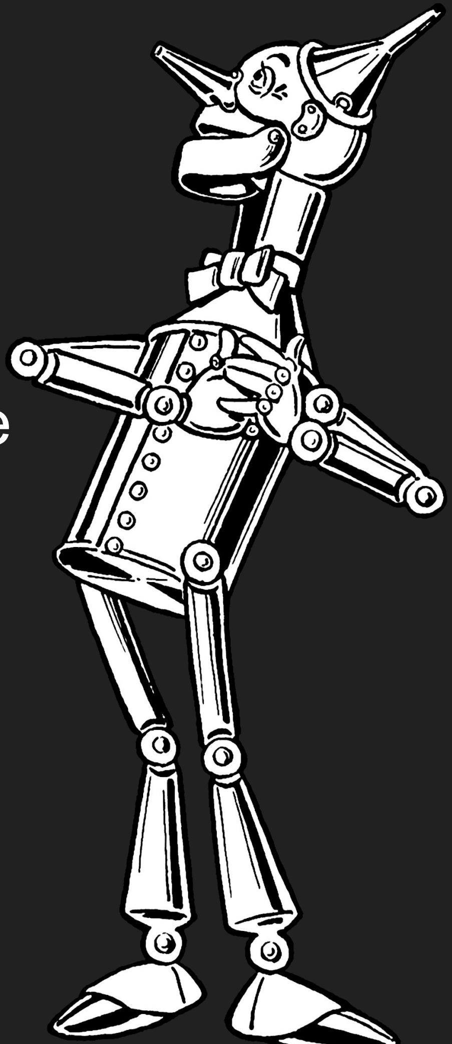
Mitigation	Description
Restrict Web-Based Content	Determine if certain websites that can be used for spearphishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk.

Procedure Examples

Name	Description
APT28	APT28 sent spearphishing emails which used a URL-shortener service to masquerade as a legitimate service and to redirect targets to credential harvesting sites. [11] [12]

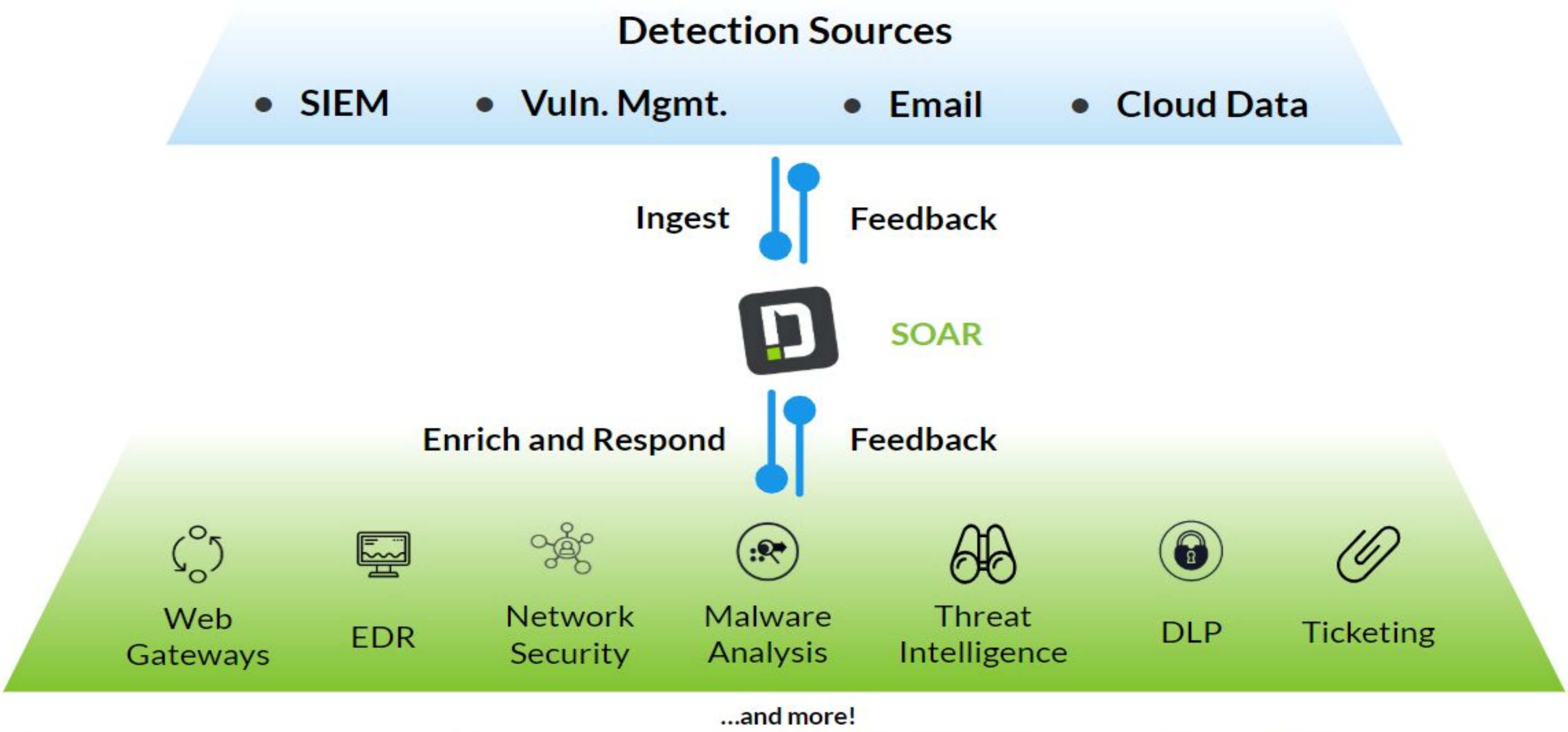
What is SOAR?

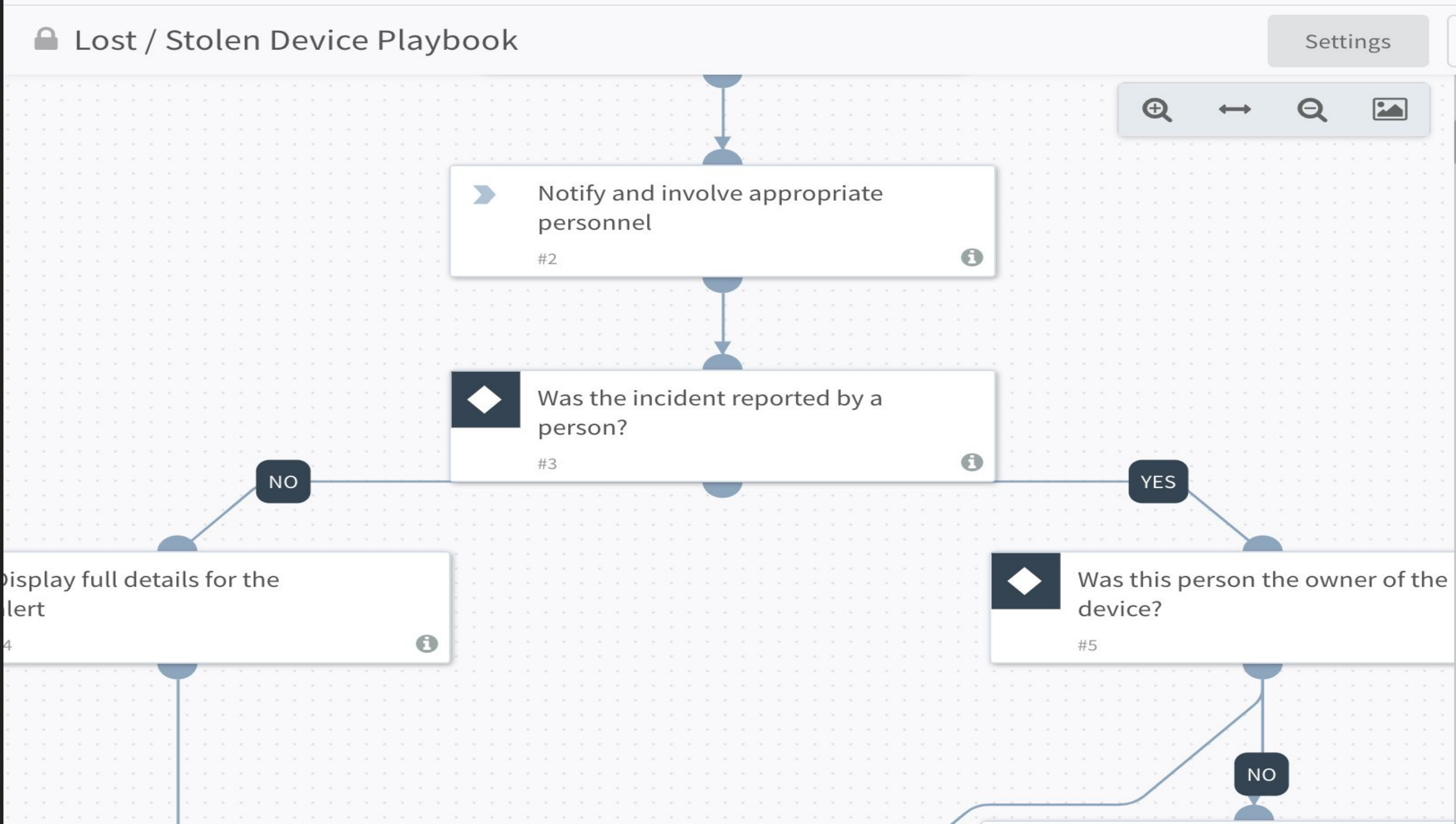
Security Orchestration Automation & Response



Security Orchestration Automation & Response

How SOAR works





Lost / Stolen Device Playbook

Notify and involve appropriate personnel

#2

Was the incident reported by a person?

#3

)isplay full details for the
lert

4

Was this person the owner of the device?

#5

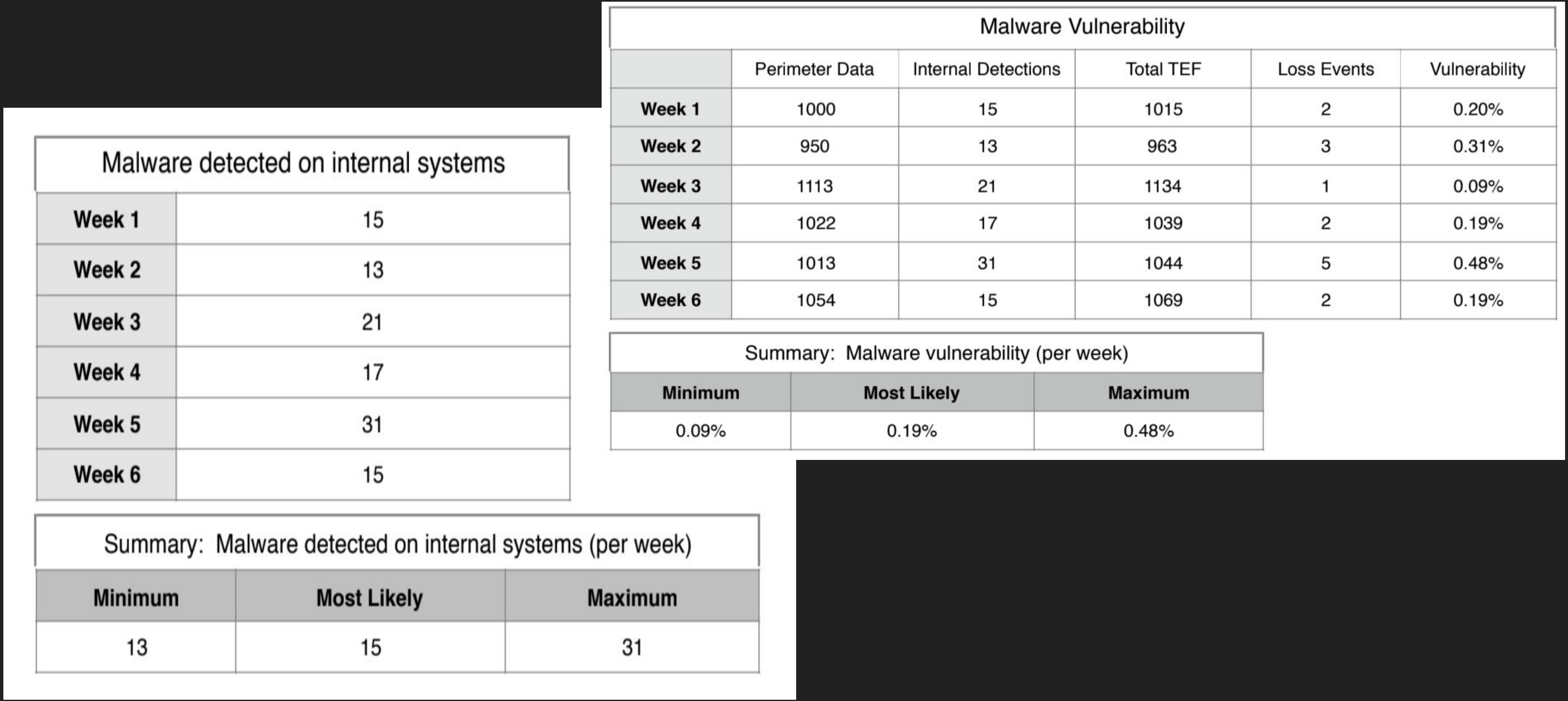
Modeling a RISK Scenario with FAIR + ATT&CK + SOAR

Model a Scenario

- Determine Asset
- Threat Community
- Threat Type / Capability
- Effect? Confidentiality, Integrity, Availability
- Apply FAIR (TE, TEF, LE, LEF, CF, POA……)
- Assoc. Mitre Att&CK TTPs
- Determine Priority For Responses

Asset	**Employee Or Corporate Laptop/Endpoints**
Threat Community	**Cyber Criminals**
Threat Type	**Malicious Activity**
Effect	**Confidentiality**
Assoc. TTPS	**T1192….**

FAIR & ATT&CK - Dirty Example



Malware detected on internal systems

Week 1	15
Week 2	13
Week 3	21
Week 4	17
Week 5	31
Week 6	15

Summary: Malware detected on internal systems (per week)

Minimum	Most Likely	Maximum
13	15	31

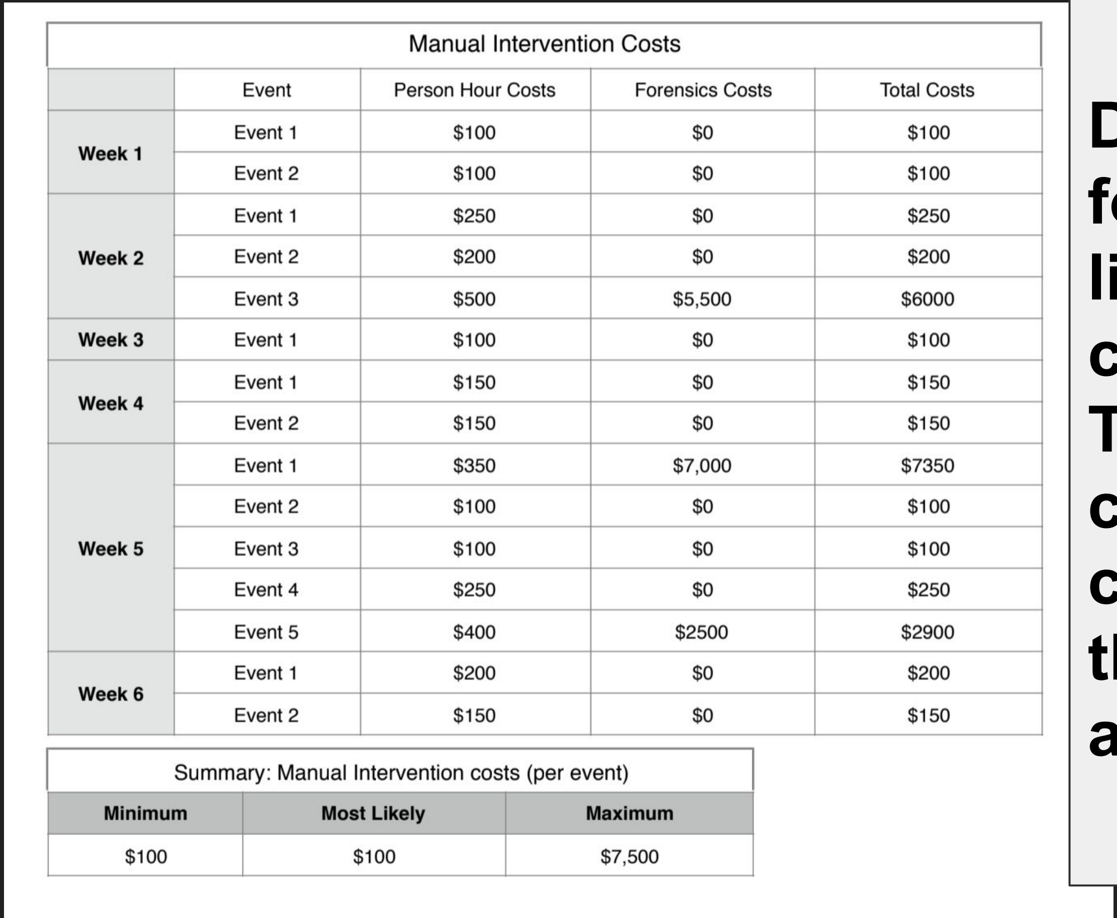
Malware Vulnerability

	Perimeter Data	Internal Detections	Total TEF	Loss Events	Vulnerability
Week 1	1000	15	1015	2	0.20%
Week 2	950	13	963	3	0.31%
Week 3	1113	21	1134	1	0.09%
Week 4	1022	17	1039	2	0.19%
Week 5	1013	31	1044	5	0.48%
Week 6	1054	15	1069	2	0.19%

Summary: Malware vulnerability (per week)

Minimum	Most Likely	Maximum
0.09%	0.19%	0.48%

Dirty Example



Manual Intervention Costs

	Event	Person Hour Costs	Forensics Costs	Total Costs
Week 1	Event 1	$100	$0	$100
	Event 2	$100	$0	$100
Week 2	Event 1	$250	$0	$250
	Event 2	$200	$0	$200
	Event 3	$500	$5,500	$6000
Week 3	Event 1	$100	$0	$100
Week 4	Event 1	$150	$0	$150
	Event 2	$150	$0	$150
Week 5	Event 1	$350	$7,000	$7350
	Event 2	$100	$0	$100
	Event 3	$100	$0	$100
	Event 4	$250	$0	$250
	Event 5	$400	$2500	$2900
Week 6	Event 1	$200	$0	$200
	Event 2	$150	$0	$150

Summary: Manual Intervention costs (per event)

Minimum	Most Likely	Maximum
$100	$100	$7,500

Depending on results for the minimum, most likely, and maximum costs, the ATT&CK TTP’s associated and coverage of TTP’s we can then PRIORITIZE the response accordingly.

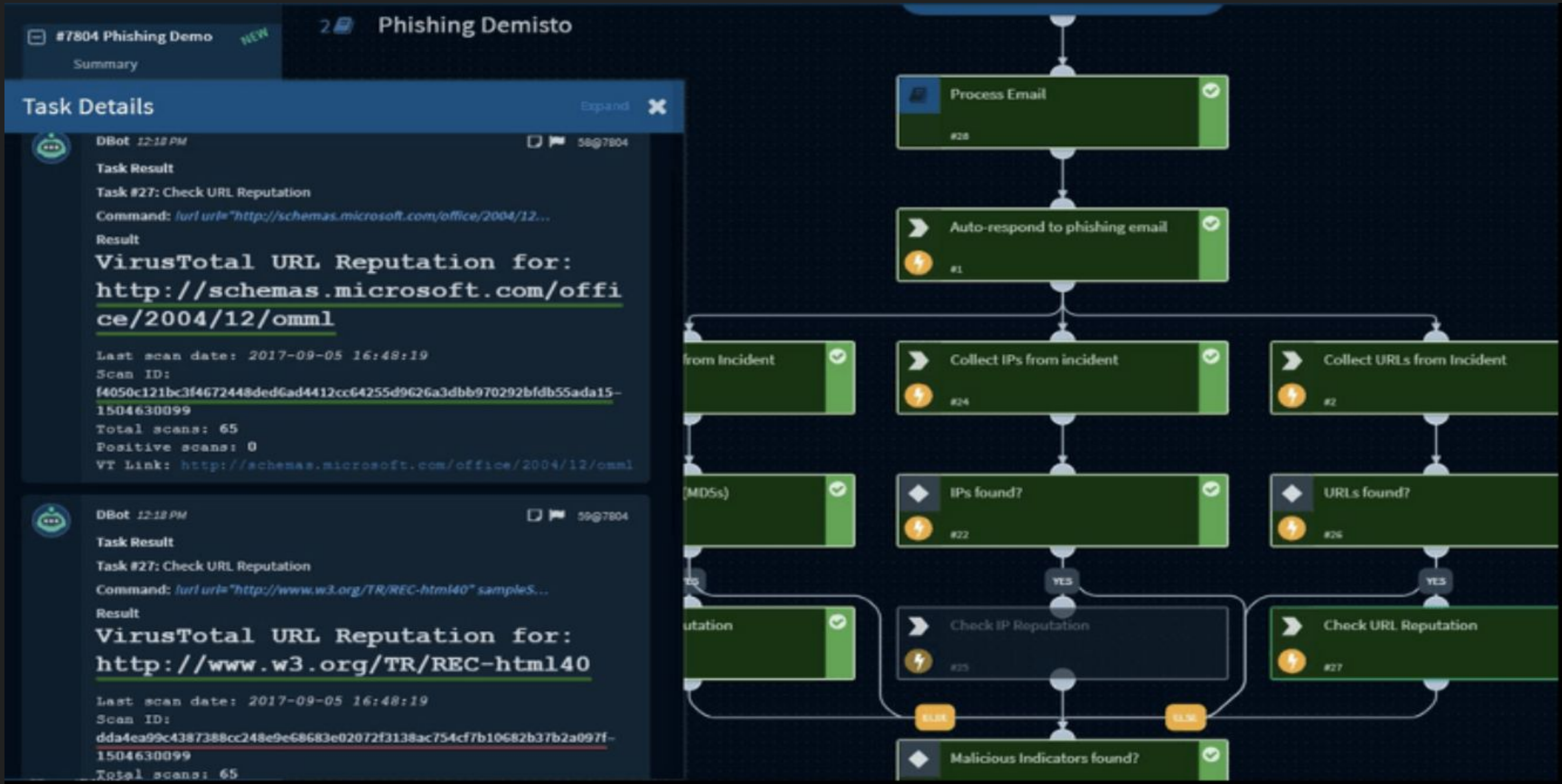
SOAR Activity

- Design/Develop
  - Use cases by aligning TTP’s and RISK (Loss Exposure)

- Prevention/Detection
  - Align detection and automated actions
  - Patch / Automate blocking

- Post breach
  - Measure and Automate what costs the most…
    - Time
    - Resources
    - Manual Intervention
  - Automate Evidence Collection

Dirty Example



Task Details

DBot 12:18 PM 58@7804

Task Result

Task #27: Check URL Reputation

Command: /url url="http://schemas.microsoft.com/office/2004/12...

Result

```
VirusTotal URL Reputation for:
http://schemas.microsoft.com/offi
ce/2004/12/omml

Last scan date: 2017-09-05 16:48:19
Scan ID:
f4050c121bc3f4672448ded6ad4412cc64255d9626a3dbb970292bfdb55ada15-
1504630099
Total scans: 65
Positive scans: 0
VT Link: http://schemas.microsoft.com/office/2004/12/omml
```

DBot 12:18 PM 59@7804

Task Result

Task #27: Check URL Reputation

Command: /url url="http://www.w3.org/TR/REC-html40" sampleS...

Result

```
VirusTotal URL Reputation for:
http://www.w3.org/TR/REC-html40

Last scan date: 2017-09-05 16:48:19
Scan ID:
dda4ea99c4387388cc248e9e68683e02072f3138ac754cf7b10682b37b2a097f-
1504630099
Total scans: 65
```

In Summary

By applying FAIR + Att&CK + SOAR we can ask questions like

- Raise or Lower priority of Use Case?
- Measure Automate Or Manual Intervention?
- What response metrics are req?
- Does the responses align with the TTP's and the FAIR estimates?
- Is the Att&CK and SOAR coverage we have for this RISK enough to reduce the RISK / Loss Exposure, or Financial Loss that could occur?
- Finally....

Thank You!

Resources:

Measuring and Managing Information Risk A Fair Approach

By Jack Freund and Jack Jones