How to Prioritize NIST CSF Controls with FAIR

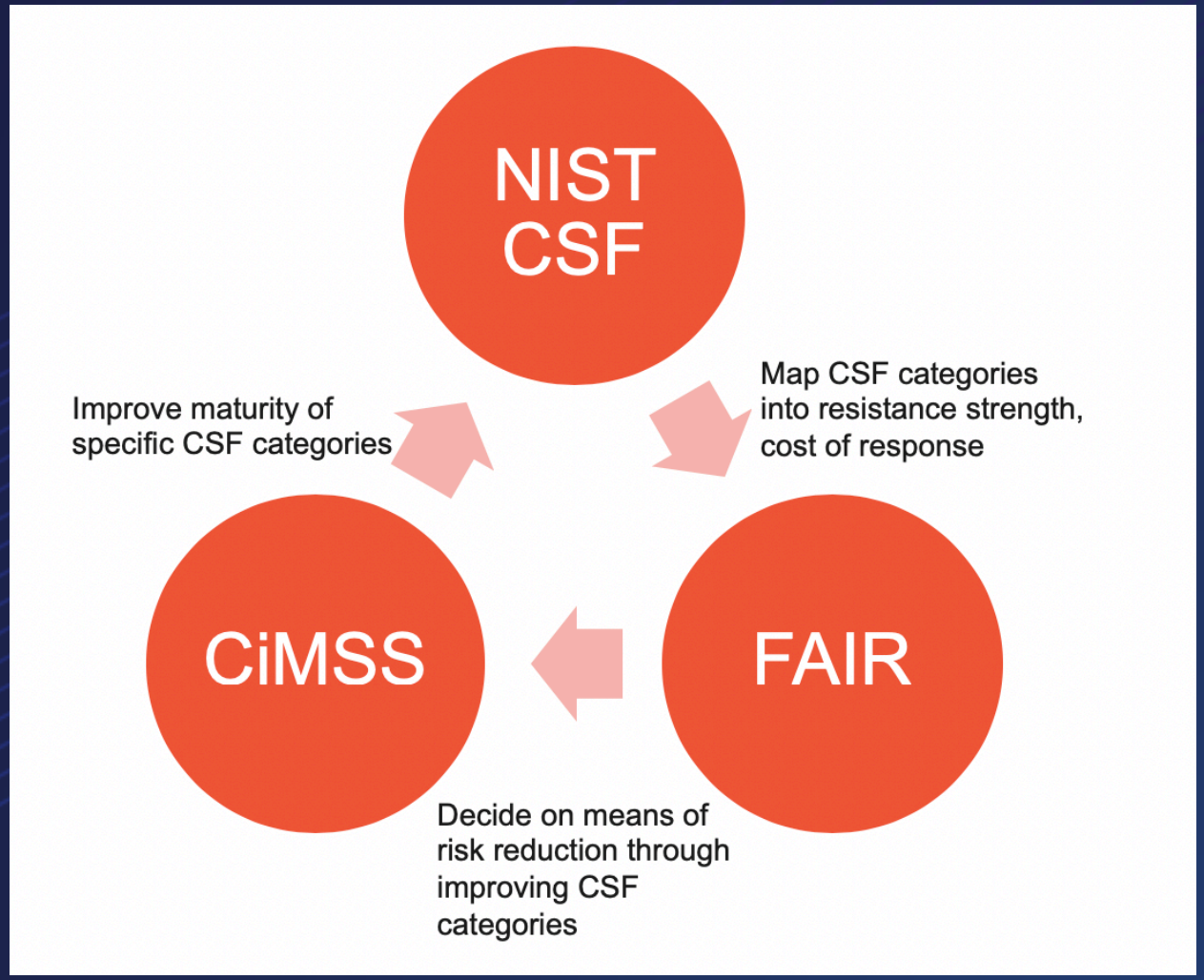
Richard Barretto
Manager of Security Operations


@richardbarretto

Agenda

- Cimpress' journey with FAIR
- What worked and what didn't ?
- How can FAIR work with NIST CSF?
- Prototype mapping and measurement
- How to prove security value?

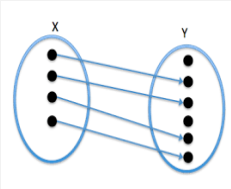
Our Journey



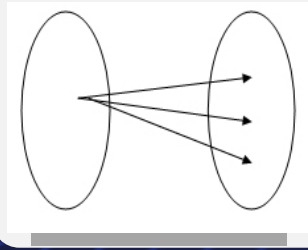
Challenges

- How could we back up the rationale for Resistance Strength?
- Which controls gave the best value?
- Transparency between Risks and Controls

FAIR and NIST Mapping Model



1:1: Risk Scenario to mitigating controls can map directly to a FAIR element such as Resistance Strength.



1:Many – Risk Scenario to mitigating controls can map to more than one NIST Control

Risk Scenario: Malware

MITGATIONS:

- Account Use Policies
- Active Directory Configuration
- Antivirus/Antimalware
- Data Backup
- Disable or Remove Feature or Program
- Encrypt Sensitive Information
- Execution Prevention

PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes

PR.AC-3: Remote access is managed

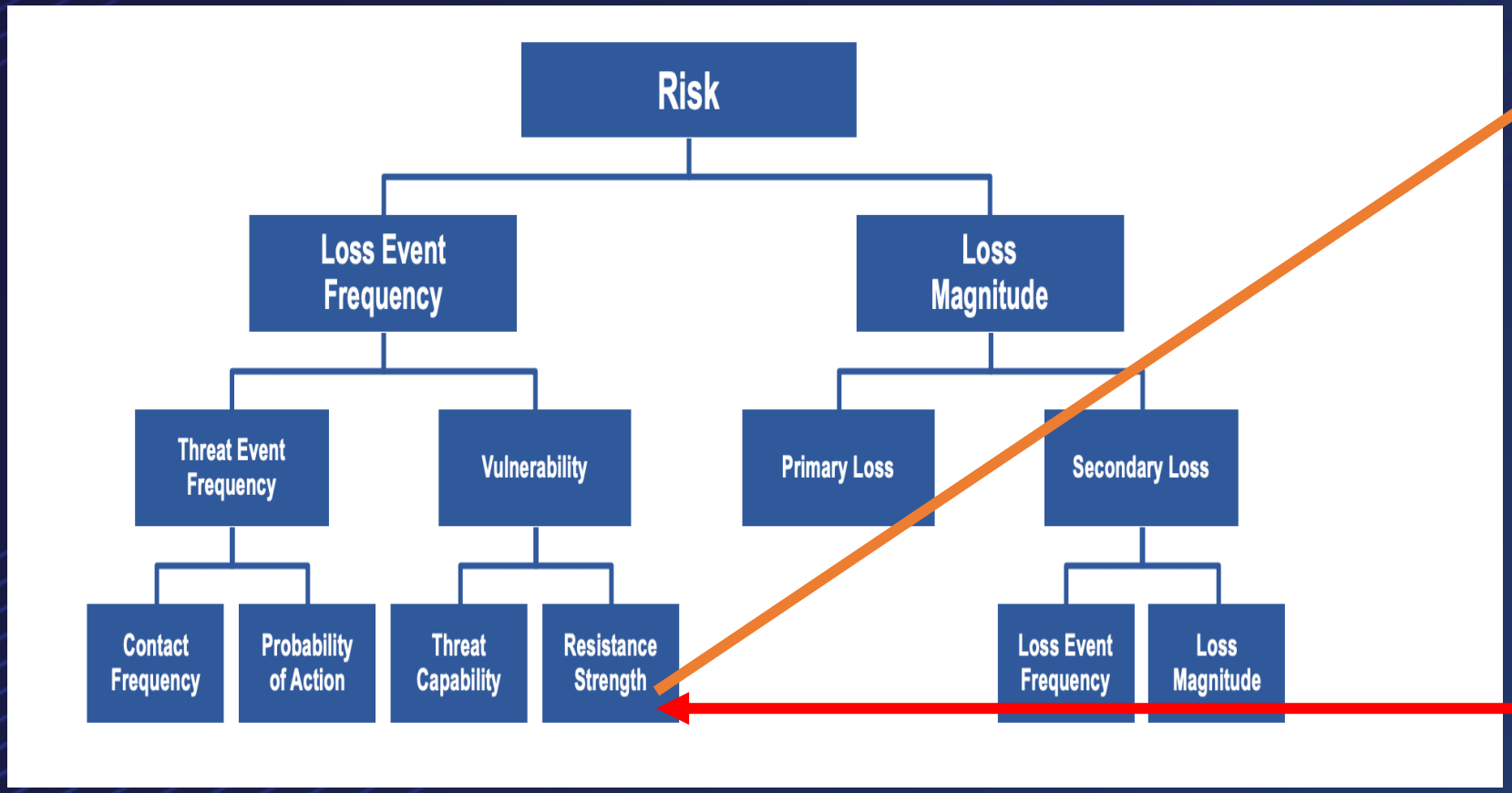
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties

PR.AC-6: Identities are proofed and bound to credentials, and asserted in interactions when appropriate

PR.DS-5: Protections against data leaks are implemented

PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating appropriate security principles (e.g. concept of least functionality)

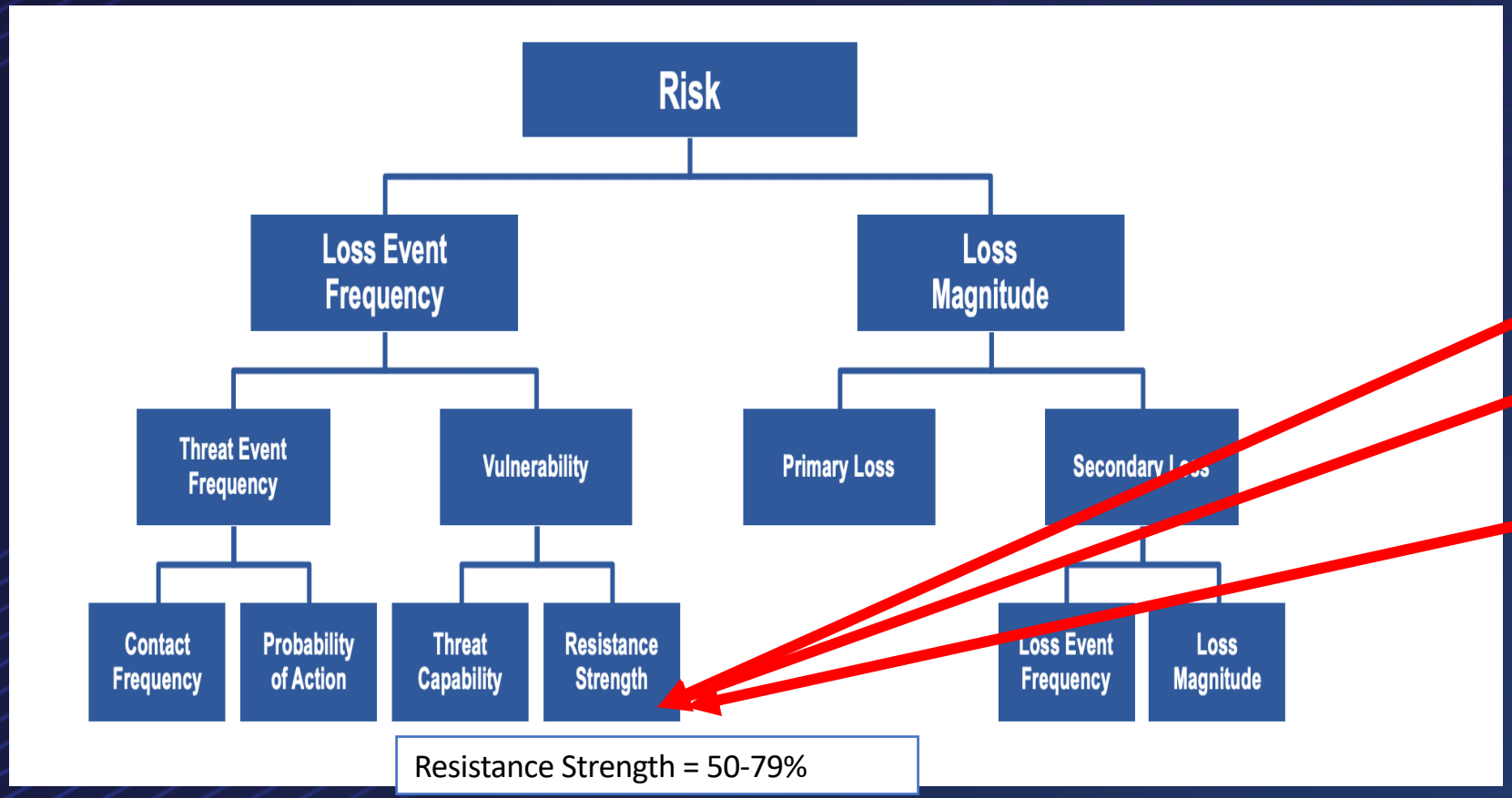
NIST Maturity Score 1:1



PR.IP-12: A vulnerability management plan is developed and implemented

Maturity Average	Resistance Strength
0 – None	0-20%
1 - AdHoc	20-50%
2 - Repeatable	50-79%
3 - Managed	80-95%

NIST Maturity Score 1: Many



DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	2
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	2
		DE.AE-5: Incident alert thresholds are established	2
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	2
		DE.CM-8: Vulnerability scans are	3
		DE.DP-1: Roles and responsibilities for	3
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-2:** Detection activities comply with all applicable requirements	3
		DE.DP-3: Detection processes are tested	3
		DE.DP-4: Event detection information is communicated to appropriate parties	3
		DE.DP-5: Detection processes are	2

Maturity Average	Resistance Strength
0 – None	0-20%
1 - AdHoc	20-50%
2 - Repeatable	50-79%
3 - Managed	80-95%

Control Average = 2.44

Cimpress Journey

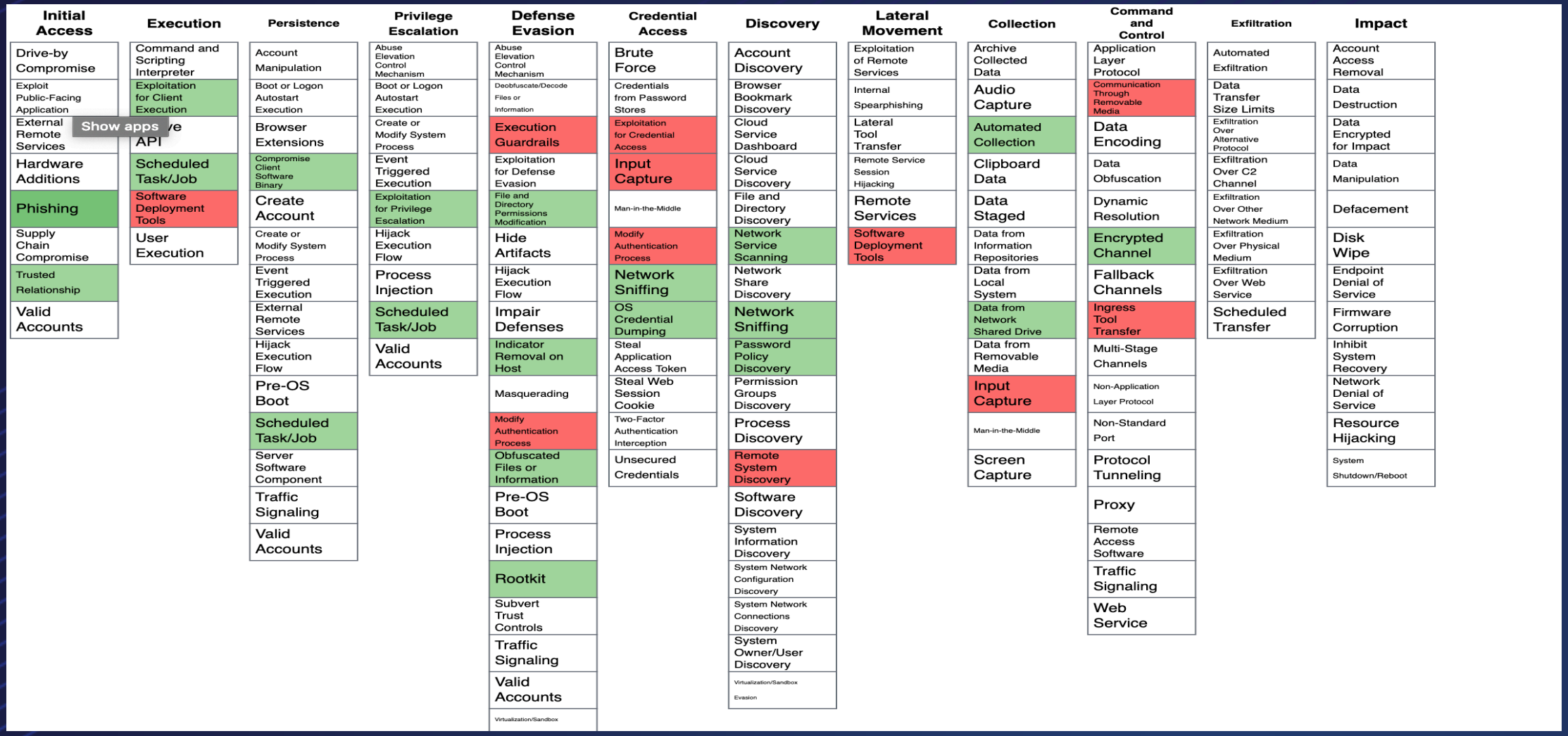
NIST CSF

FAIR

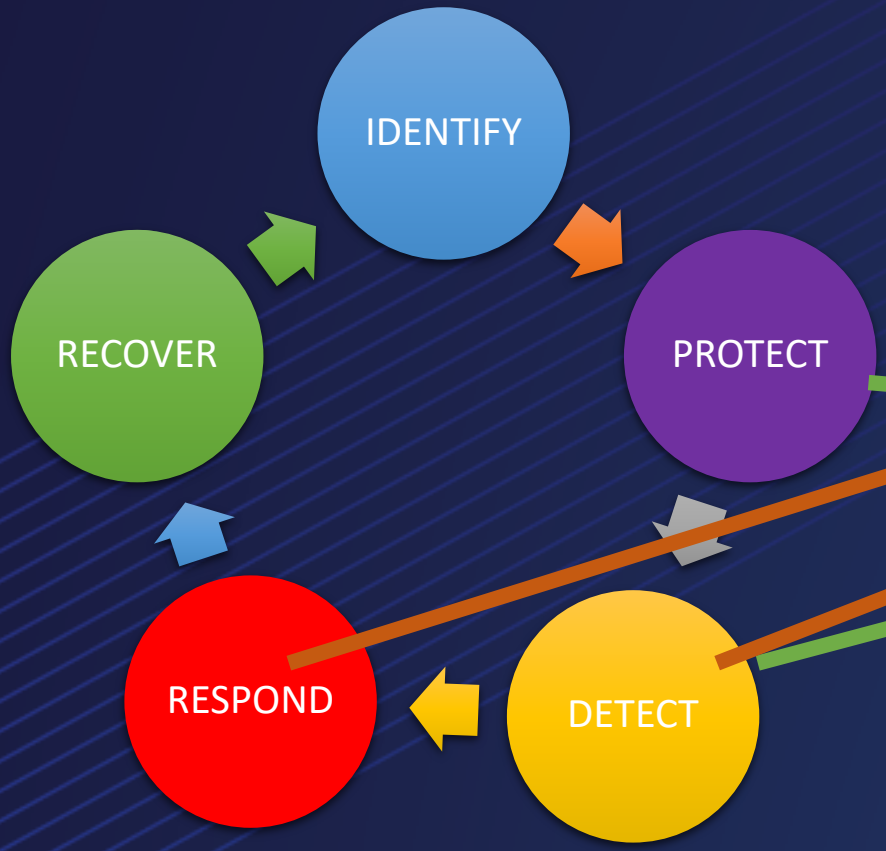
Red Team Test

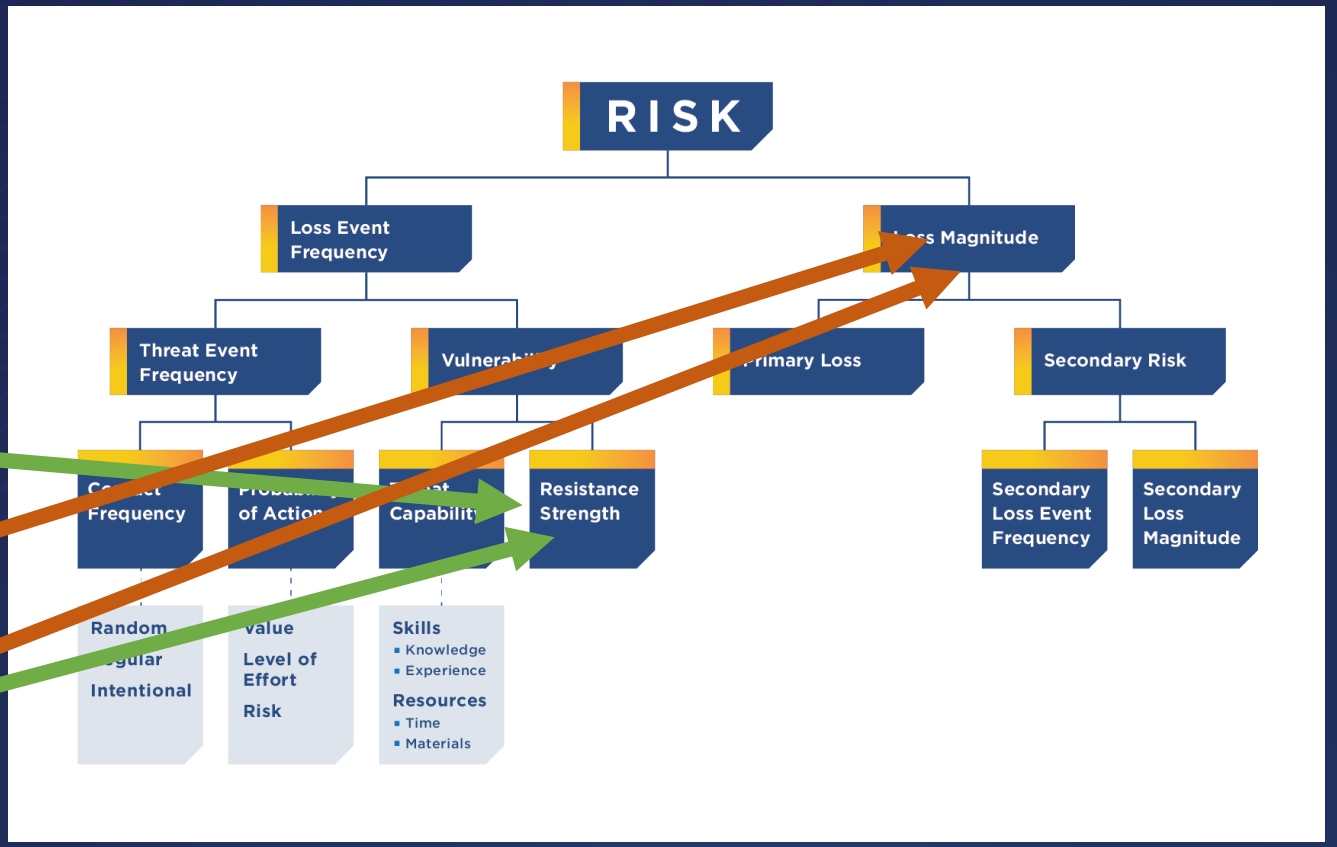
MITRE ATT&CK™

MITRE ATT&CK Coverage Heat Map

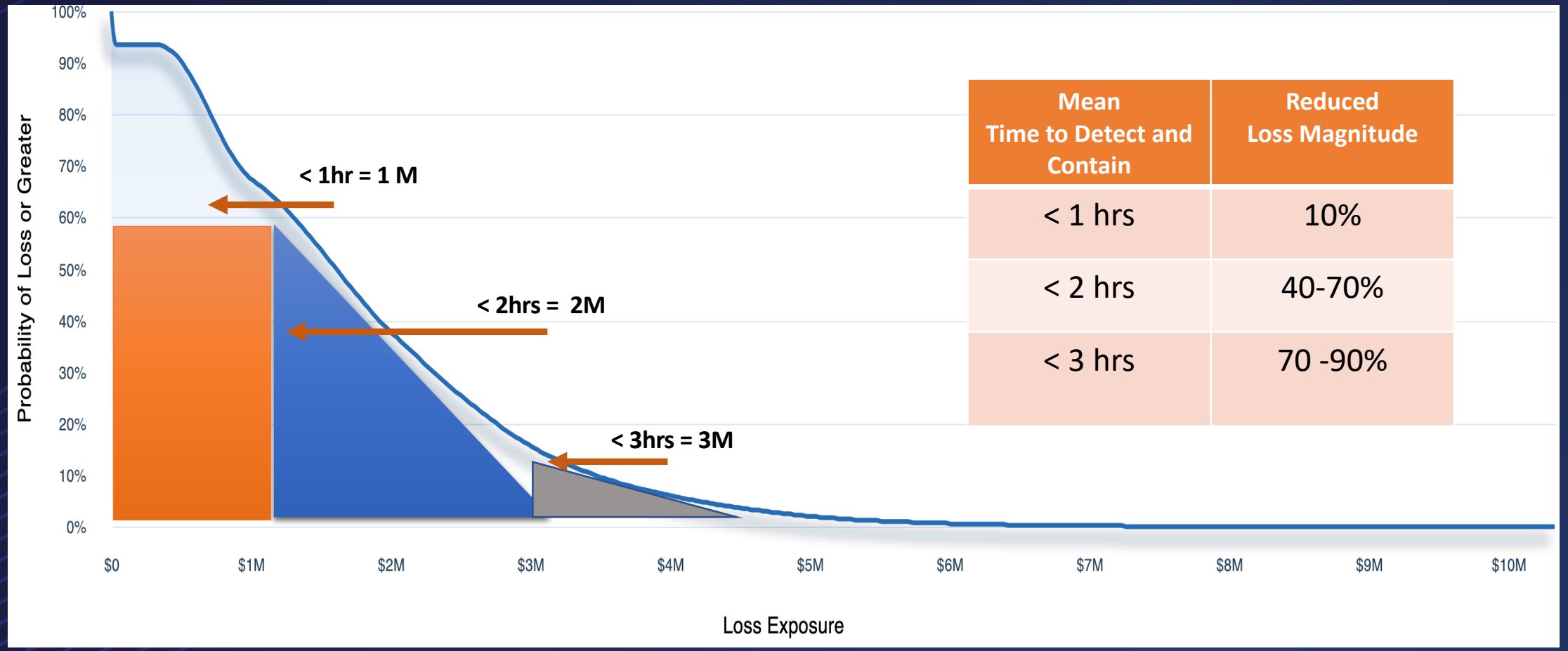


Two Sides to Every Story





Impact Reduction



Mean Time to Detect and Contain	Reduced Loss Magnitude
< 1 hrs	10%
< 2 hrs	40-70%
< 3 hrs	70 -90%

Metrics to consider

Measuring	Insights
• **Mean time to retrieve logs for investigation**	Point of attack contact to initial log availability
• **Mean time to get logs and produce detections**	Log entry to initial security alert
• **Mean time to produce alert from point of attack**	Security alert to SOC notification
• **Mean time to validate true or false positive to point of escalation**	SOC notification to escalation to relevant business
• **Mean time to response**	Escalation to initial Incident Response
• **Mean time to containment**	IR start to establishing containment and impact scope (IOCs, TTPs, root cause)
• **Mean time to eradicate**	Containment to Eradication and closure

Different Scopes for Different Folks

Clear as Glass

- Build test plans
- Clear road map of controls
- Prioritization of controls, tests, and, investments

Thank you