mimecast

Risk Profiling: Foundation of Transformative Security

PURCO 2023

Johan Nepgen

Principal Sales Engineer

33 billion

electronic records are expected to be stolen

$8 trillion

Cybercrime is expected to cost the world $8 trillion. In economic terms, this is greater than the GDP of any country except the U.S. and China

$4.35 million

Globally, the average cost of a data breach is $4.35 million. The average cost in the U.S. is more than double that, at $9.44 million

13%

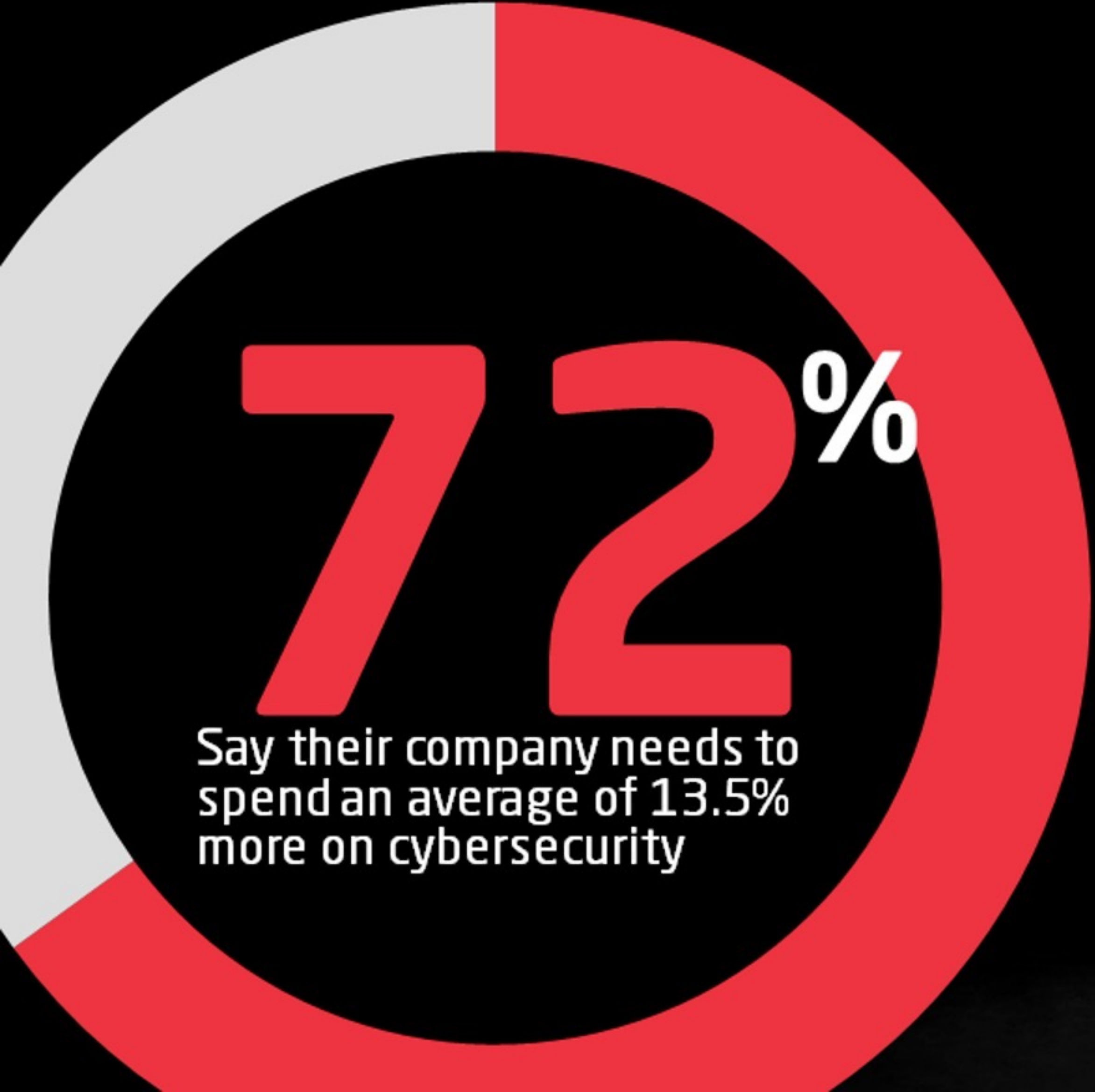
Rise in ransomware in 2022 — an increase as big as the past five years combined

212 days

On average, it takes 212 days to detect a data breach and another 75 days to contain it

mimecast

Cyber Preparedness | **Budget**

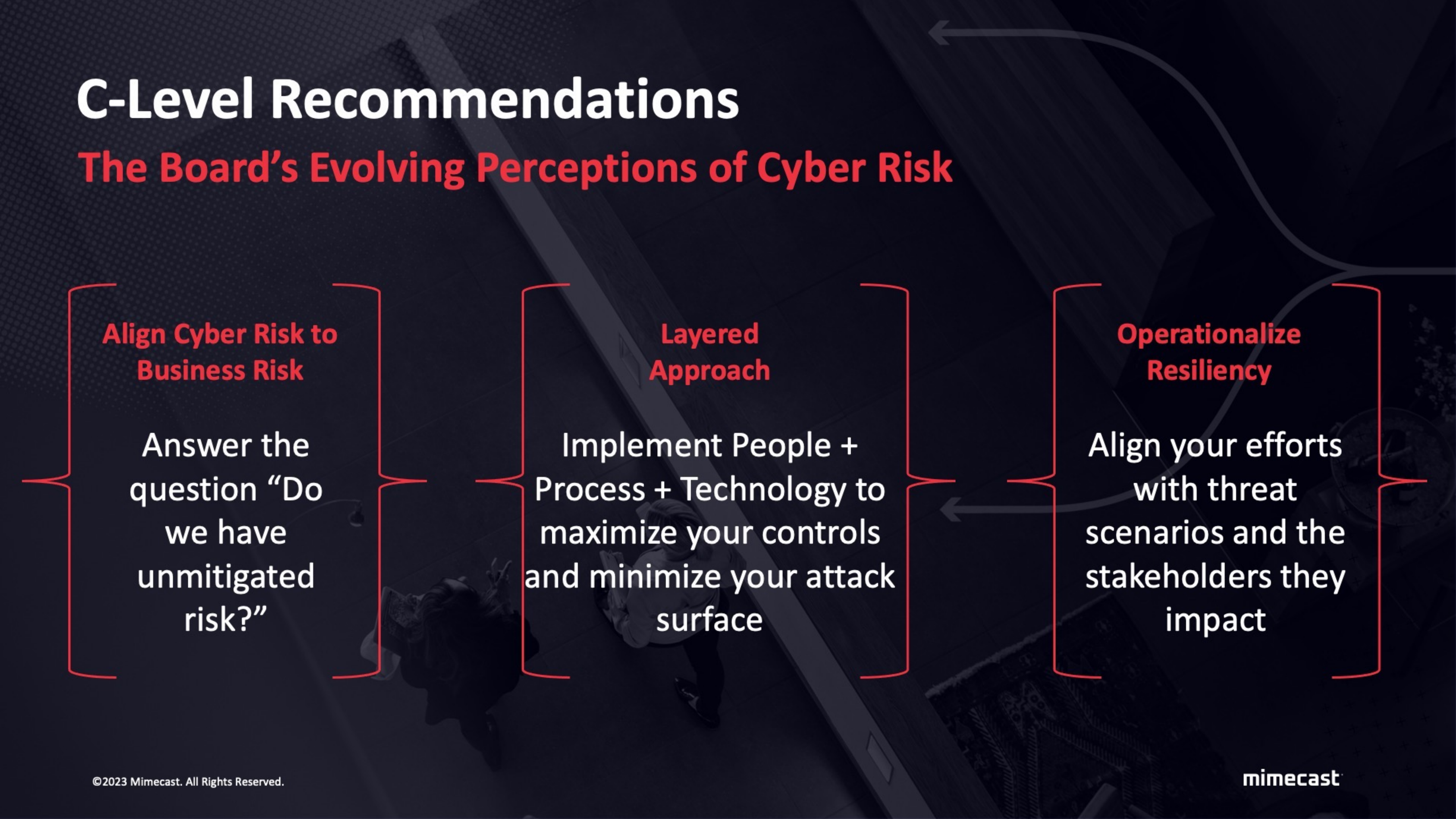


72%

Say their company needs to spend an average of 13.5% more on cybersecurity

Priorities

- Prevention
- Operationalise
- Integrate
- Automate



C-Level Recommendations

The Board’s Evolving Perceptions of Cyber Risk

Align Cyber Risk to Business Risk

Answer the question “Do we have unmitigated risk?”

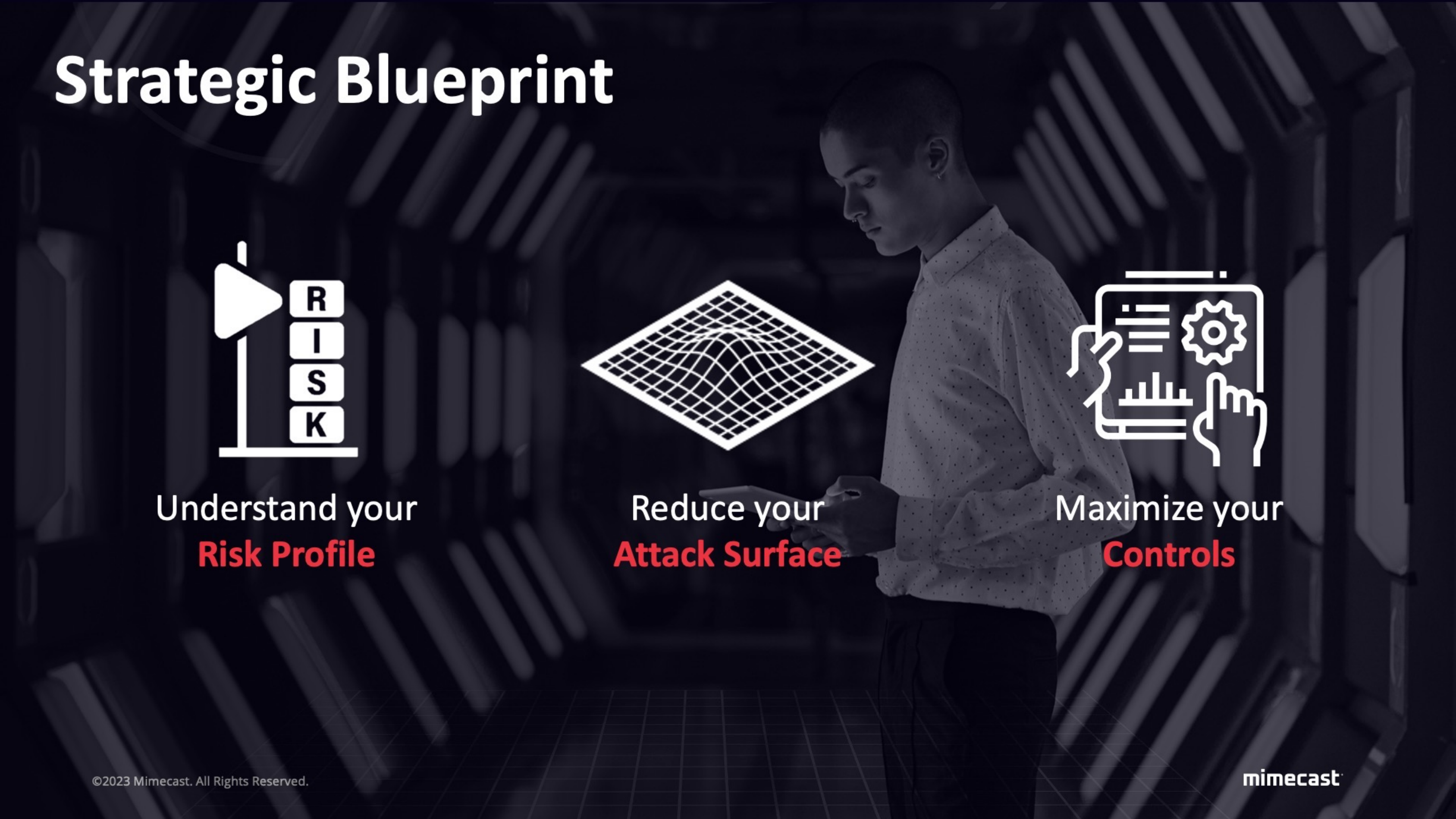
Layered Approach

Implement People + Process + Technology to maximize your controls and minimize your attack surface

Operationalize Resiliency

Align your efforts with threat scenarios and the stakeholders they impact

Strategic Blueprint



Understand your **Risk Profile**

Reduce your **Attack Surface**

Maximize your **Controls**

Education Sector is a Target

Personal Data

Faculty and Students

Infrastructure

Data + Disruption

Digitized Classrooms

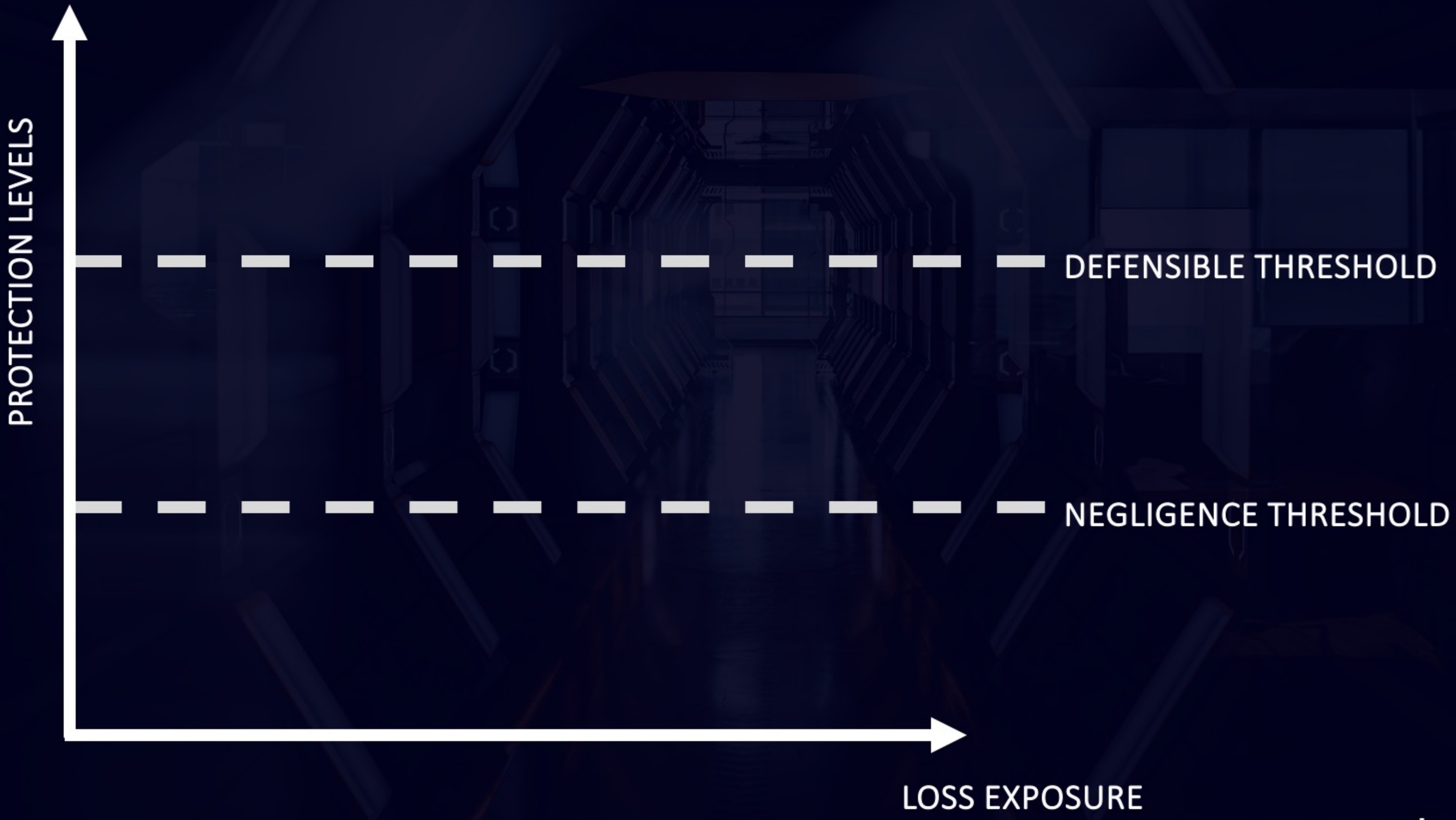
Increased attack vector

Defensible vs Negligent?

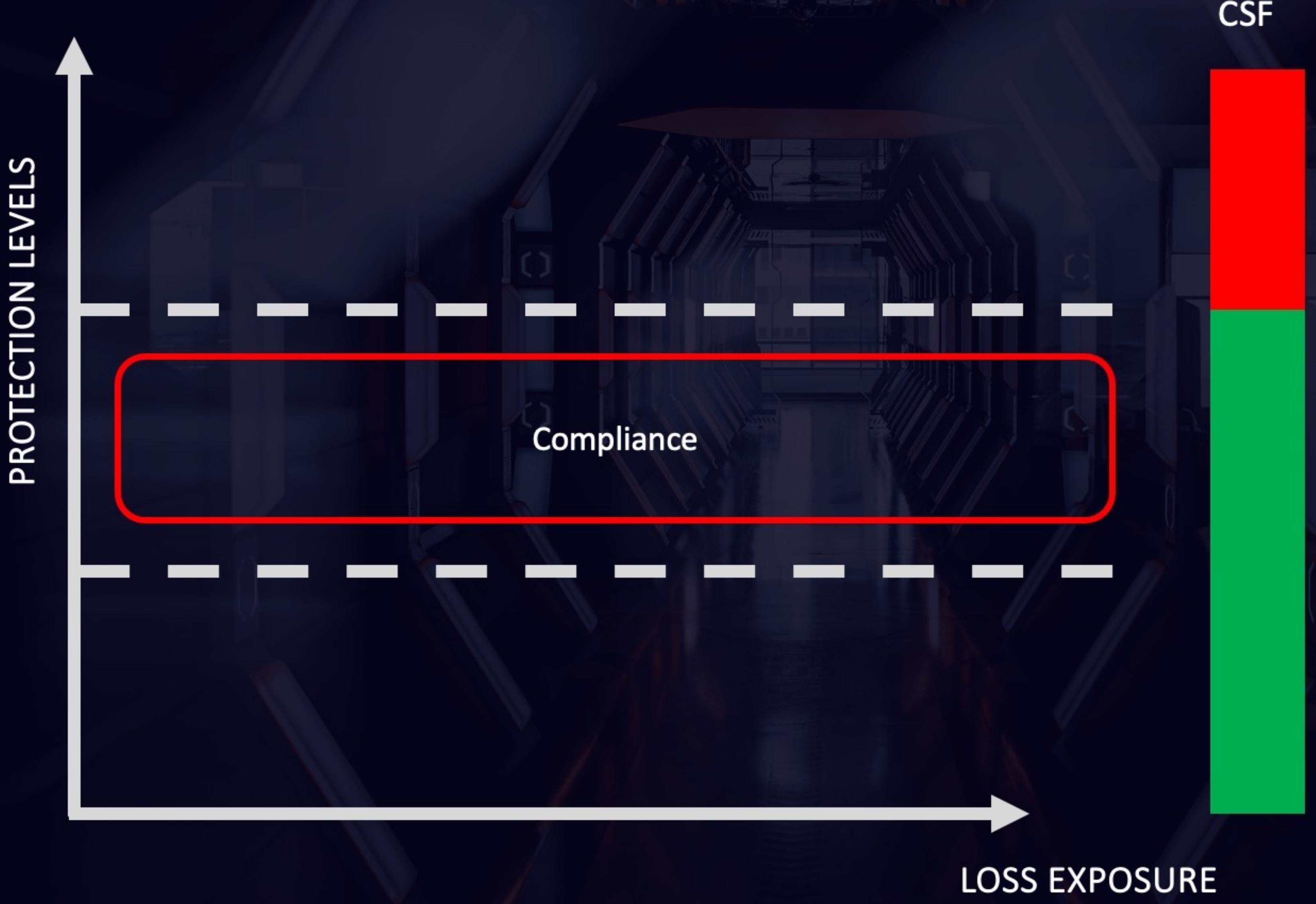
DEFENSIBLE THRESHOLD

NEGLIGENCE THRESHOLD

Protection Levels & Loss Exposure



Compliant Doesn't Mean Secure



Today, 73% of CSF audit standard questions relate to the existence of controls, not their performance

Gartner

Risk Tolerance

What business outcomes do you want?
How much are you willing to pay to achieve them?

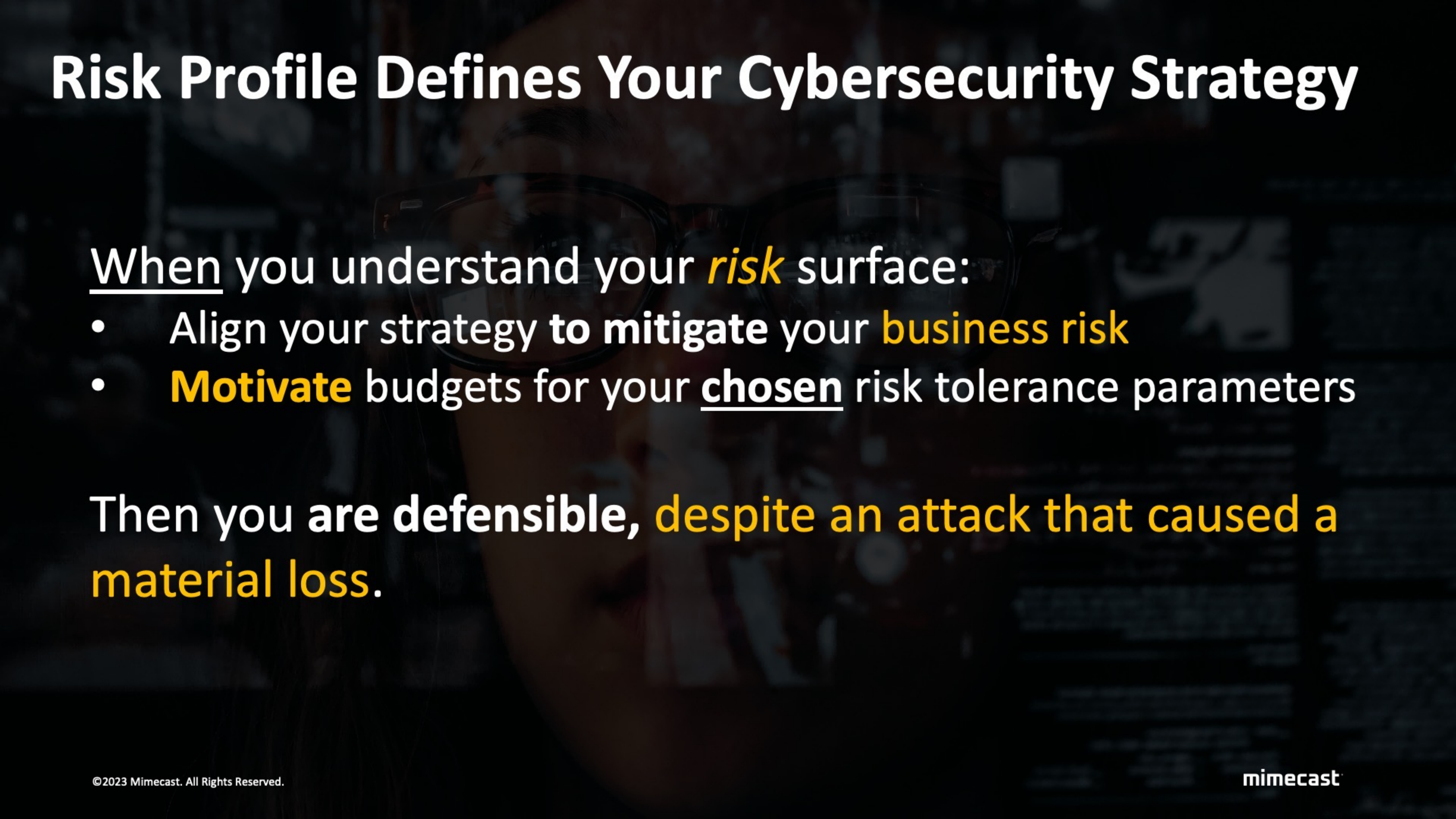
Protection level agreements

15 minutes to investigate-remediate

15 minutes to investigate-remediate

15 minutes to investigate-remediate

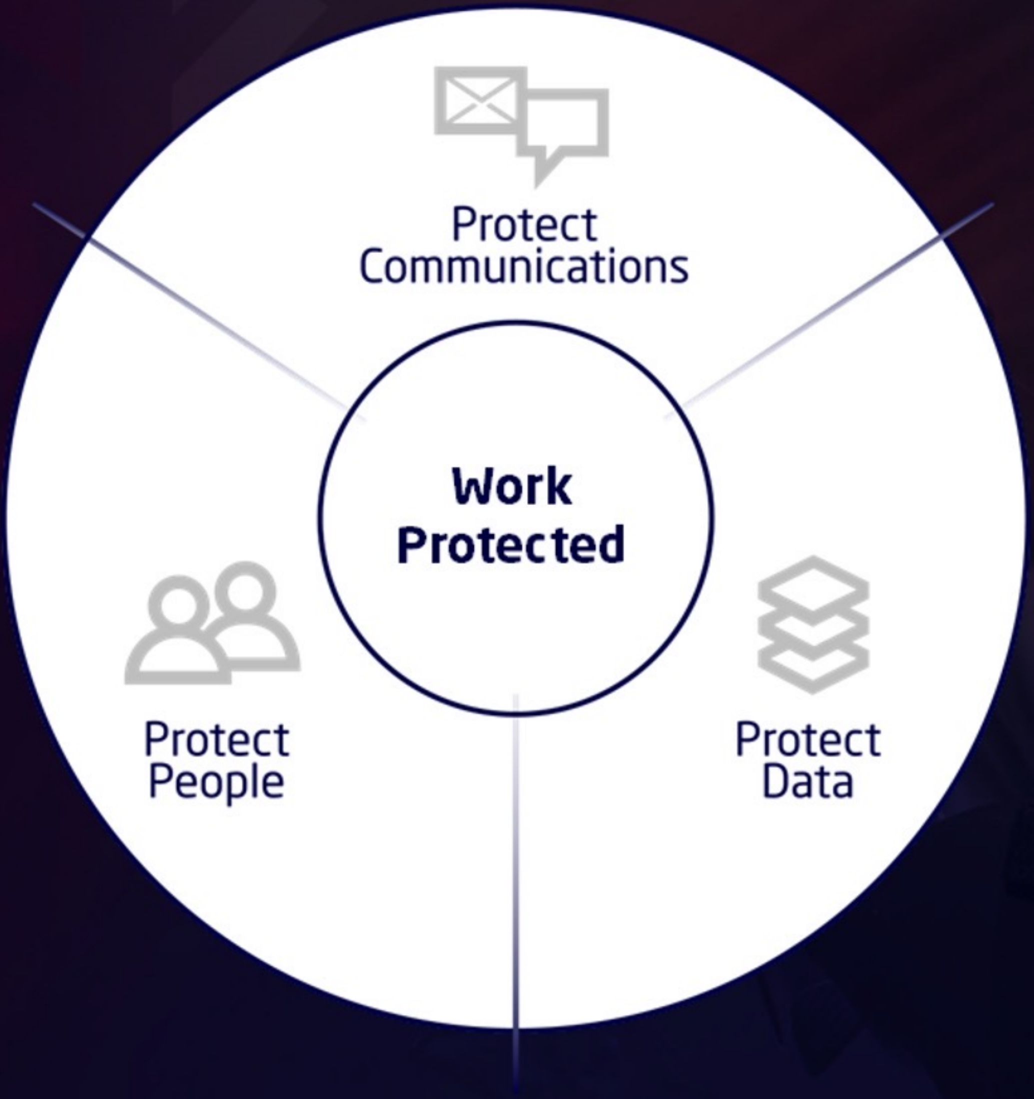
Risk Profile Defines Your Cybersecurity Strategy



When you understand your *risk* surface:

- Align your strategy **to mitigate** your business risk
- **Motivate** budgets for your **chosen** risk tolerance parameters

Then you **are defensible,** despite an attack that caused a material loss.



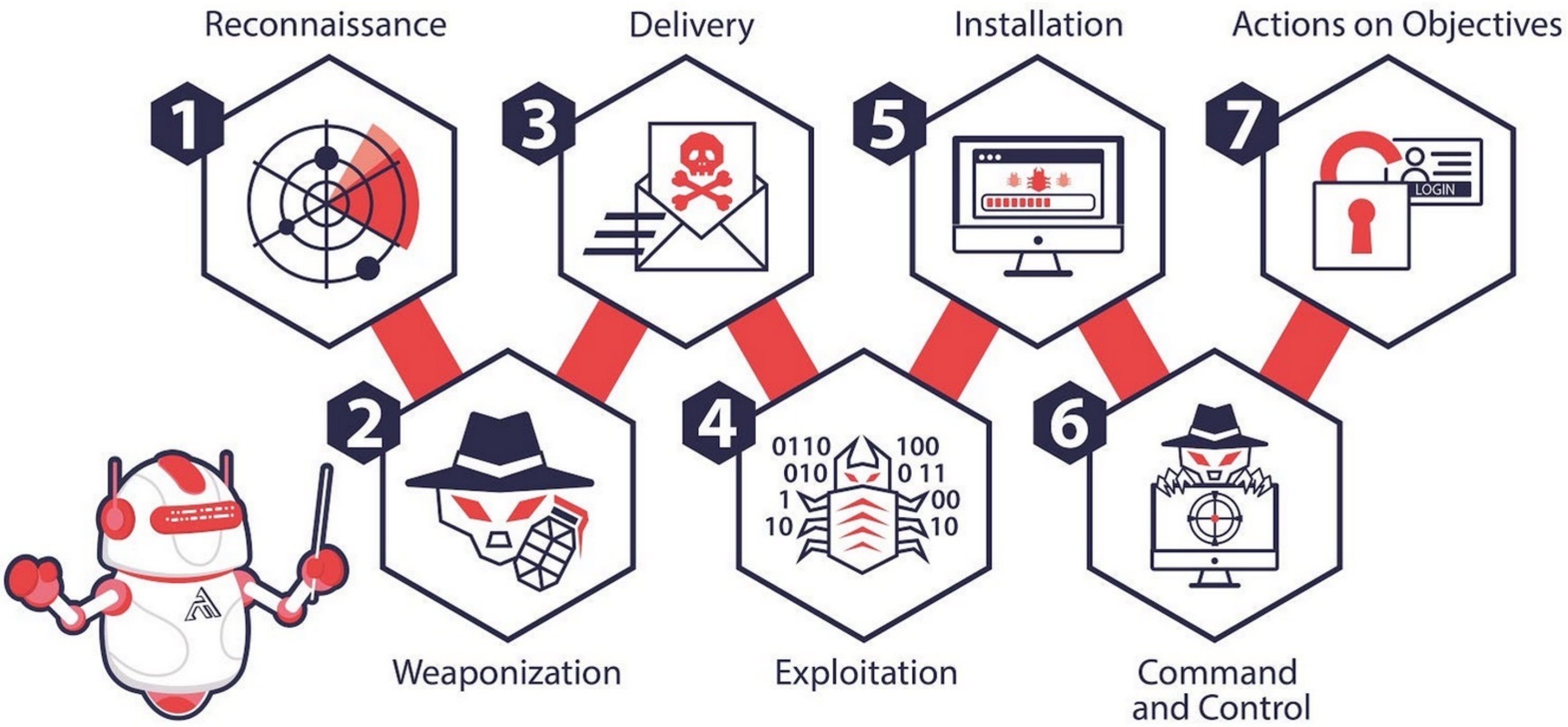
The Work Protected Methodology

mimecast

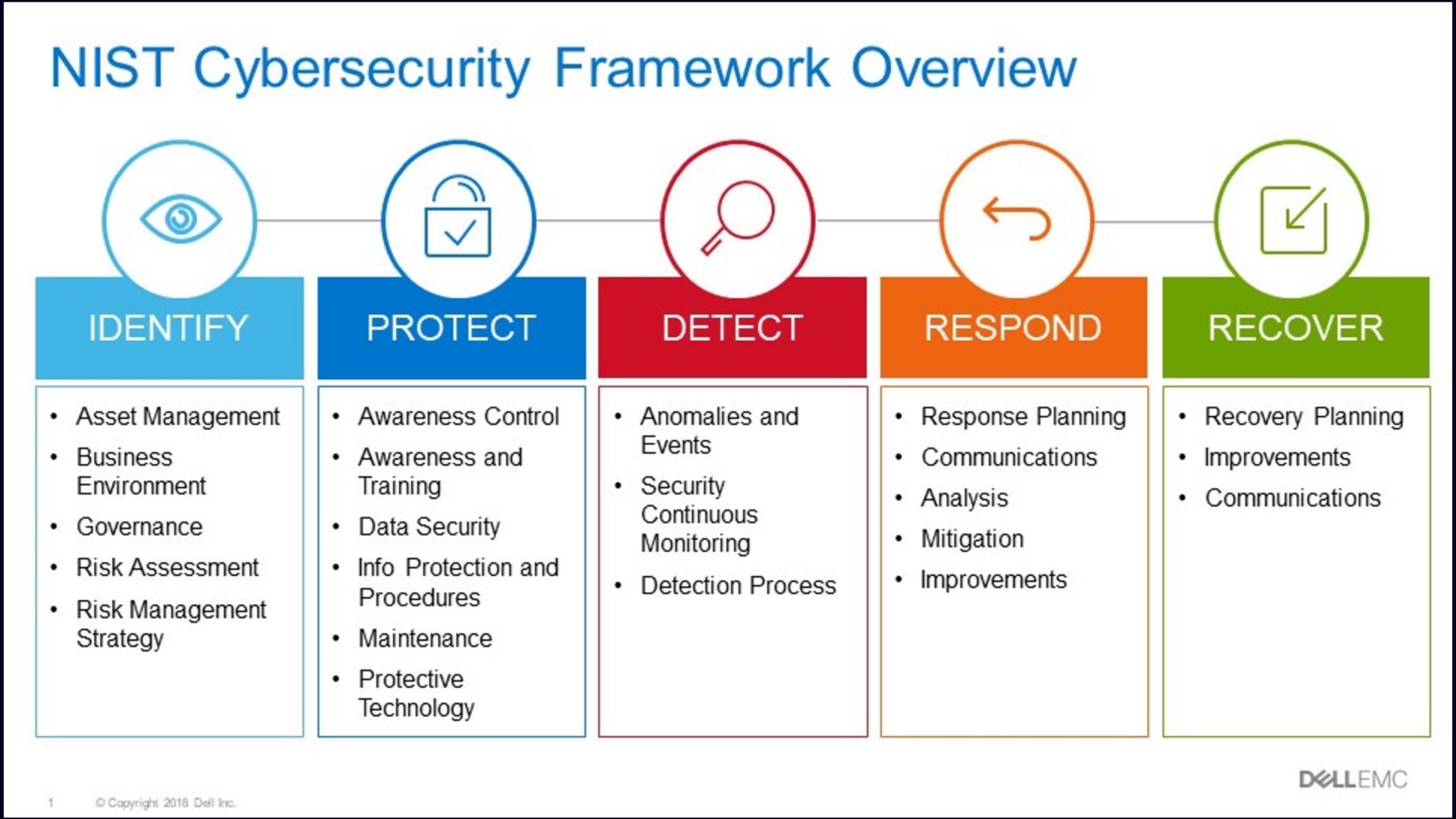
Cyber Risk Strategies:

Budget, Procurement,
Increased Risk

Understanding the Modern Cyber Kill Chain



GOOD: Cyber Defense Matrix Assessment



NIST Cybersecurity Framework Overview

IDENTIFY

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

PROTECT

- Awareness Control
- Awareness and Training
- Data Security
- Info Protection and Procedures
- Maintenance
- Protective Technology

DETECT

- Anomalies and Events
- Security Continuous Monitoring
- Detection Process

RESPOND

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

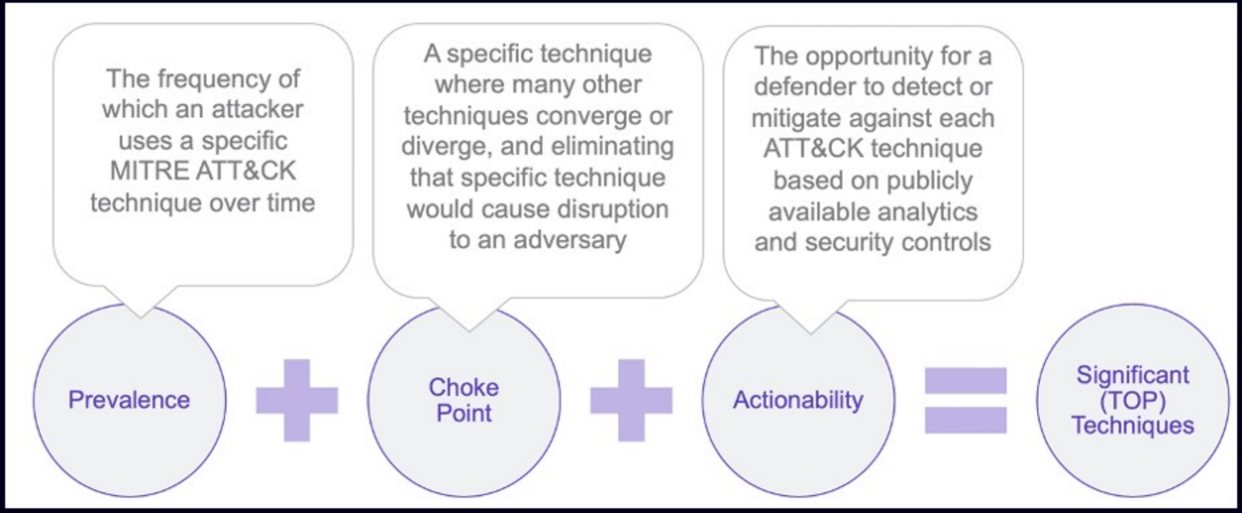
RECOVER

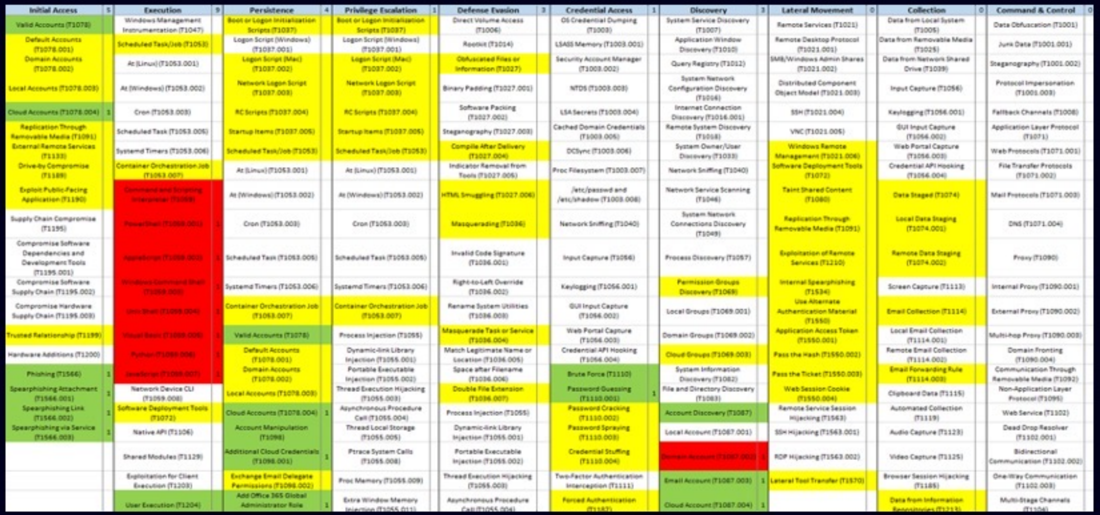
- Recovery Planning
- Improvements
- Communications

DELLEMC

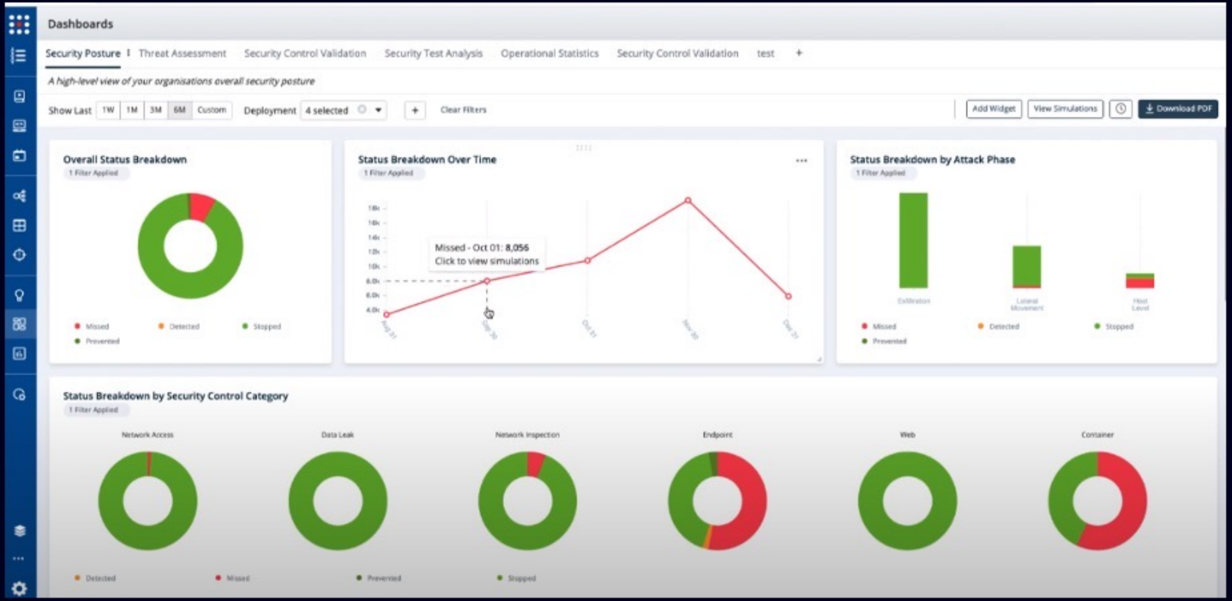
1

BETTER: Measure MITRE ATT&CK Coverage


The frequency of which an attacker uses a specific MITRE ATT&CK technique over time
A specific technique where many other techniques converge or diverge, and eliminating that specific technique would cause disruption to an adversary
The opportunity for a defender to detect or mitigate against each ATT&CK technique based on publicly available analytics and security controls
Prevalence
+
Choke Point
+
Actionability
=
Significant (TOP) Techniques



Initial Access	5	Execution	9	Persistence	4	Privilege Escalation	1	Defense Evasion	3	Credential Access	1	Discovery	3	Lateral Movement	0	Collection	0	Command & Control	0
Valid Accounts (T1078)		Windows Management Instrumentation (T1047)		Boot or Logon Initialization Scripts (T1037)		Boot or Logon Initialization Scripts (T1037)		Direct Volume Access (T1006)		OS Credential Dumping (T1003)		System Service Discovery (T1007)		Remote Services (T1021)		Data from Local System (T1005)		Data Obfuscation (T1001)	
Default Accounts (T1078.001)		Scheduled Task/Job (T1053)		Logon Script (Windows) (T1037.001)		Logon Script (Windows) (T1037.001)		Rootkit (T1014)		LSASS Memory (T1003.001)		Application Window Discovery (T1010)		Remote Desktop Protocol (T1021.001)		Data from Removable Media (T1025)		Junk Data (T1001.001)	
Domain Accounts (T1078.002)		At (Linux) (T1053.001)		Logon Script (Mac) (T1037.002)		Logon Script (Mac) (T1037.002)		Obfuscated Files or Information (T1027)		Security Account Manager (T1003.002)		Query Registry (T1012)		SMB/Windows Admin Shares (T1021.002)		Data from Network Shared Drive (T1039)		Steganography (T1001.002)	
Local Accounts (T1078.003)		At (Windows) (T1053.002)		Network Logon Script (T1037.003)		Network Logon Script (T1037.003)		Binary Padding (T1027.001)		NTDS (T1003.003)		System Network Configuration Discovery (T1016)		Distributed Component Object Model (T1021.003)		Input Capture (T1056)		Protocol Impersonation (T1001.003)	
Cloud Accounts (T1078.004)	1	Cron (T1053.003)		RC Scripts (T1037.004)		RC Scripts (T1037.004)		Software Packing (T1027.002)		LSA Secrets (T1003.004)		Internet Connection Discovery (T1016.001)		SSH (T1021.004)		Keylogging (T1056.001)		Fallback Channels (T1008)	
Replication Through Removable Media (T1091)		Scheduled Task (T1053.005)		Startup Items (T1037.005)		Startup Items (T1037.005)		Steganography (T1027.003)		Cached Domain Credentials (T1003.005)		Remote System Discovery (T1018)		VNC (T1021.005)		GUI Input Capture (T1056.002)		Application Layer Protocol (T1071)	
External Remote Services (T1133)		Systemd Timers (T1053.006)		Scheduled Task/Job (T1053)		Scheduled Task/Job (T1053)		Compile After Delivery (T1027.004)		DCSync (T1003.006)		System Owner/User Discovery (T1033)		Windows Remote Management (T1021.006)		Web Portal Capture (T1056.003)		Web Protocols (T1071.001)	
Drive-by Compromise (T1189)		Container Orchestration Job (T1053.007)		At (Linux) (T1053.001)		At (Linux) (T1053.001)		Indicator Removal from Tools (T1027.005)		Proc Filesystem (T1003.007)		Network Sniffing (T1040)		Software Deployment Tools (T1072)		Credential API Hooking (T1056.004)		File Transfer Protocols (T1071.002)	
Exploit Public-Facing Application (T1190)		Command and Scripting Interpreter (T1059)		At (Windows) (T1053.002)		At (Windows) (T1053.002)		HTML Smuggling (T1027.006)		/etc/passwd and /etc/shadow (T1003.008)		Network Service Scanning (T1046)		Taint Shared Content (T1080)		Data Staged (T1074)		Mail Protocols (T1071.003)	
Supply Chain Compromise (T1195)		PowerShell (T1059.001)	1	Cron (T1053.003)		Cron (T1053.003)		Masquerading (T1036)		Network Sniffing (T1040)		System Network Connections Discovery (T1049)		Replication Through Removable Media (T1091)		Local Data Staging (T1074.001)		DNS (T1071.004)	
Compromise Software Dependencies and Development Tools (T1195.001)		AppleScript (T1059.002)	1	Scheduled Task (T1053.005)		Scheduled Task (T1053.005)		Invalid Code Signature (T1036.001)		Input Capture (T1056)		Process Discovery (T1057)		Exploitation of Remote Services (T1210)		Remote Data Staging (T1074.002)		Proxy (T1090)	
Compromise Software Supply Chain (T1195.002)		Windows Command Shell (T1059.003)	1	Systemd Timers (T1053.006)		Systemd Timers (T1053.006)		Right-to-Left Override (T1036.002)		Keylogging (T1056.001)		Permission Groups Discovery (T1069)		Internal Spearphishing (T1534)		Screen Capture (T1113)		Internal Proxy (T1090.001)	
Compromise Hardware Supply Chain (T1195.003)		Unix Shell (T1059.004)	1	Container Orchestration Job (T1053.007)		Container Orchestration Job (T1053.007)		Rename System Utilities (T1036.003)		GUI Input Capture (T1056.002)		Local Groups (T1069.001)		Use Alternate Authentication Material (T1550)		Email Collection (T1114)		External Proxy (T1090.002)	
Trusted Relationship (T1199)		Visual Basic (T1059.005)	1	Valid Accounts (T1078)		Process Injection (T1055)		Masquerade Task or Service (T1036.004)		Web Portal Capture (T1056.003)		Domain Groups (T1069.002)		Application Access Token (T1550.001)		Local Email Collection (T1114.001)		Multi-hop Proxy (T1090.003)	
Hardware Additions (T1200)		Python (T1059.006)	1	Default Accounts (T1078.001)		Dynamic-link Library Injection (T1055.001)		Match Legitimate Name or Location (T1036.005)		Credential API Hooking (T1056.004)		Cloud Groups (T1069.003)		Pass the Hash (T1550.002)		Remote Email Collection (T1114.002)		Domain Fronting (T1090.004)	
Phishing (T1566)	1	JavaScript (T1059.007)	1	Domain Accounts (T1078.002)		Portable Executable Injection (T1055.002)		Space after Filename (T1036.006)		Brute Force (T1110)		System Information Discovery (T1082)		Pass the Ticket (T1550.003)		Email Forwarding Rule (T1114.003)		Communication Through Removable Media (T1092)	
Spearphishing Attachment (T1566.001)	1	Network Device CLI (T1059.008)		Local Accounts (T1078.003)		Thread Execution Hijacking (T1055.003)		Double File Extension (T1036.007)		Password Guessing (T1110.001)	1	File and Directory Discovery (T1083)		Web Session Cookie (T1550.004)		Clipboard Data (T1115)		Non-Application Layer Protocol (T1095)	
Spearphishing Link (T1566.002)	1	Software Deployment Tools (T1072)		Cloud Accounts (T1078.004)	1	Asynchronous Procedure Call (T1055.004)		Process Injection (T1055)		Password Cracking (T1110.002)		Account Discovery (T1087)		Remote Service Session Hijacking (T1563)		Automated Collection (T1119)		Web Service (T1102)	
Spearphishing via Service (T1566.003)	1	Native API (T1106)		Account Manipulation (T1098)		Thread Local Storage (T1055.005)		Dynamic-link Library Injection (T1055.001)		Password Spraying (T1110.003)		Local Account (T1087.001)		SSH Hijacking (T1563.001)		Audio Capture (T1123)		Dead Drop Resolver (T1102.001)	
		Shared Modules (T1129)		Additional Cloud Credentials (T1098.001)	1	Ptrace System Calls (T1055.008)		Portable Executable Injection (T1055.002)		Credential Stuffing (T1110.004)		Domain Account (T1087.002)	1	RDP Hijacking (T1563.002)		Video Capture (T1125)		Bidirectional Communication (T1102.002)	
		Exploitation for Client Execution (T1203)		Exchange Email Delegate Permissions (T1098.002)		Proc Memory (T1055.009)		Thread Execution Hijacking (T1055.003)		Two-Factor Authentication Interception (T1111)		Email Account (T1087.003)	1	Lateral Tool Transfer (T1570)		Browser Session Hijacking (T1185)		One-Way Communication (T1102.003)	
		User Execution (T1204)		Add Office 365 Global Administrator Role	1	Extra Window Memory Injection (T1055.011)		Asynchronous Procedure Call (T1055.004)		Forced Authentication (T1187)		Cloud Account (T1087.004)	1			Data from Information Repositories (T1213)		Multi-Stage Channels (T1104)	



Dashboards

Security Posture | Threat Assessment | Security Control Validation | Security Test Analysis | Operational Statistics | Security Control Validation | test | +

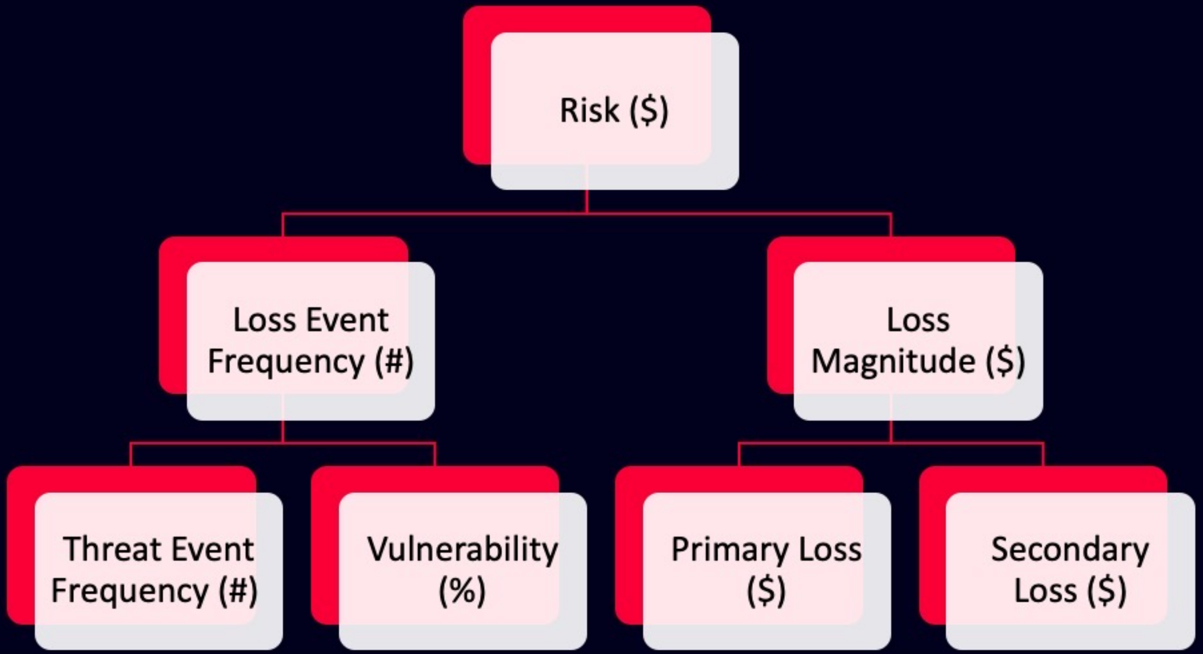
A high-level view of your organisations overall security posture

Show Last: 1W 1M 3M [✓ 6M] Custom — Deployment: 4 selected — Clear Filters

Missed - Oct 01: 8,056
Click to view simulations

BEST:

Leverage FAIR Risk Analysis
Leverage Risk Quantification Services


Risk ($)

Loss Event Frequency (#)

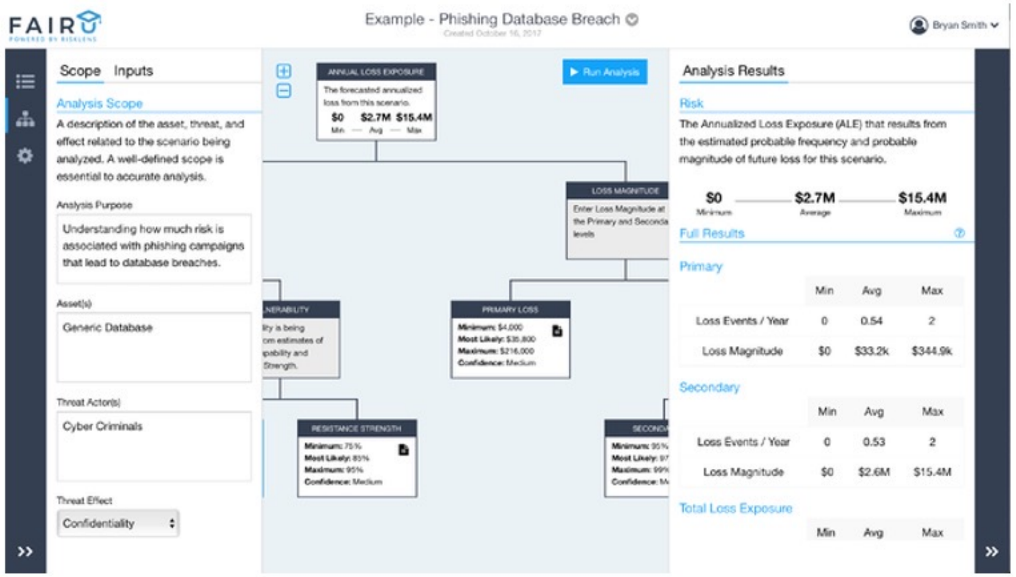
Loss Magnitude ($)

Threat Event Frequency (#)

Vulnerability (%)

Primary Loss ($)

Secondary Loss ($)



Example - Phishing Database Breach

Created October 16, 2017

Analysis Scope

A description of the asset, threat, and effect related to the scenario being analyzed. A well-defined scope is essential to accurate analysis.

Analysis Purpose: Understanding how much risk is associated with phishing campaigns that lead to database breaches.

Asset(s): Generic Database

Threat Actor(s): Cyber Criminals

Threat Effect: Confidentiality

ANNUAL LOSS EXPOSURE: The forecasted annualized loss from this scenario. $0 Min — $2.7M Avg — $15.4M Max

LOSS MAGNITUDE: Enter Loss Magnitude at the Primary and Seconda levels

…NERABILITY: …ity is being …om estimates of …pability and Strength.

PRIMARY LOSS: **Minimum:** $4,000 **Most Likely:** $35,800 **Maximum:** $216,000 **Confidence:** Medium

RESISTANCE STRENGTH: **Minimum:** 75% **Most Likely:** 85% **Maximum:** 95% **Confidence:** Medium

SECONDA…: **Minimum:** 95% **Most Likely:** 97 **Maximum:** 99% **Confidence:** M…

Analysis Results

Risk

The Annualized Loss Exposure (ALE) that results from the estimated probable frequency and probable magnitude of future loss for this scenario.

$0 Minimum — $2.7M Average — $15.4M Maximum

Full Results

Primary

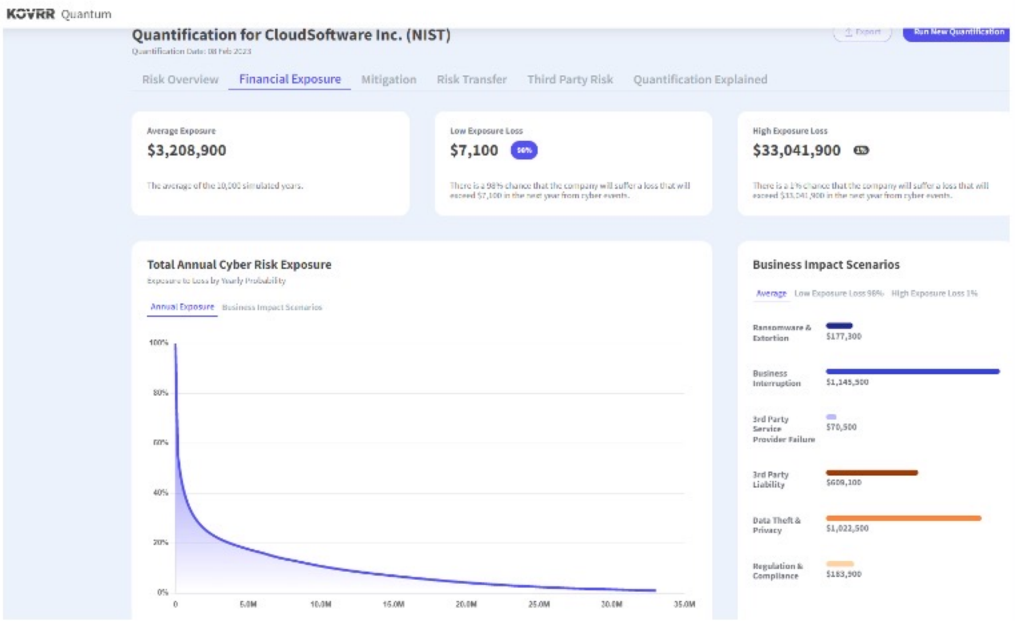
	Min	Avg	Max
Loss Events / Year	0	0.54	2
Loss Magnitude	$0	$33.2k	$344.9k

Secondary

	Min	Avg	Max
Loss Events / Year	0	0.53	2
Loss Magnitude	$0	$2.6M	$15.4M

Total Loss Exposure

Min	Avg	Max



Quantification for CloudSoftware Inc. (NIST)

Quantification Date: 08 Feb 2023

Average Exposure: **$3,208,900** — The average of the 10,000 simulated years.

Low Exposure Loss: **$7,100** 98% — There is a 98% chance that the company will suffer a loss that will exceed $7,100 in the next year from cyber events.

High Exposure Loss: **$33,041,900** 1% — There is a 1% chance that the company will suffer a loss that will exceed $33,041,900 in the next year from cyber events.

Total Annual Cyber Risk Exposure

Exposure to Loss by Yearly Probability

Business Impact Scenarios

Ransomware & Extortion	$177,300
Business Interruption	$1,145,900
3rd Party Service Provider Failure	$70,500
3rd Party Liability	$609,100
Data Theft & Privacy	$1,022,500
Regulation & Compliance	$183,900

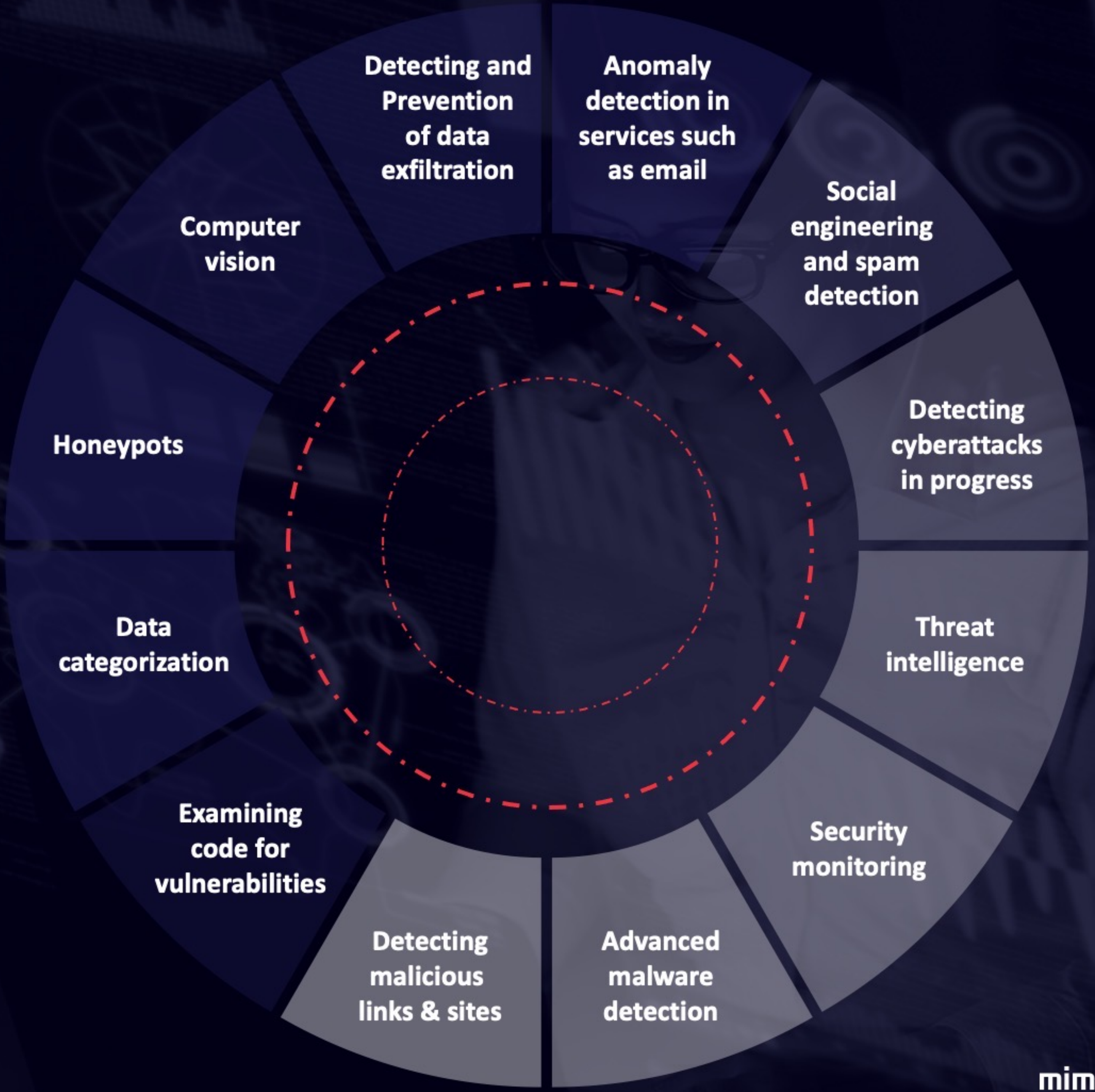
Cyber Security Burnout

mimecast

FORCE MULTIPLIER

- CYBER SKILLS SHORTAGE
- MACHINE SPEED
- SOC DATA FLOW
- EXPANDING ATTACK SURFACE

Where AI/ML is used in Cyber



Detecting and Prevention of data exfiltration

Anomaly detection in services such as email

Social engineering and spam detection

Detecting cyberattacks in progress

Threat intelligence

Security monitoring

Advanced malware detection

Detecting malicious links & sites

Examining code for vulnerabilities

Data categorization

Honeypots

Computer vision

AI and ML augments
(but doesn’t replace)

PEOPLE

TOOLSETS

INTELLIGENCE

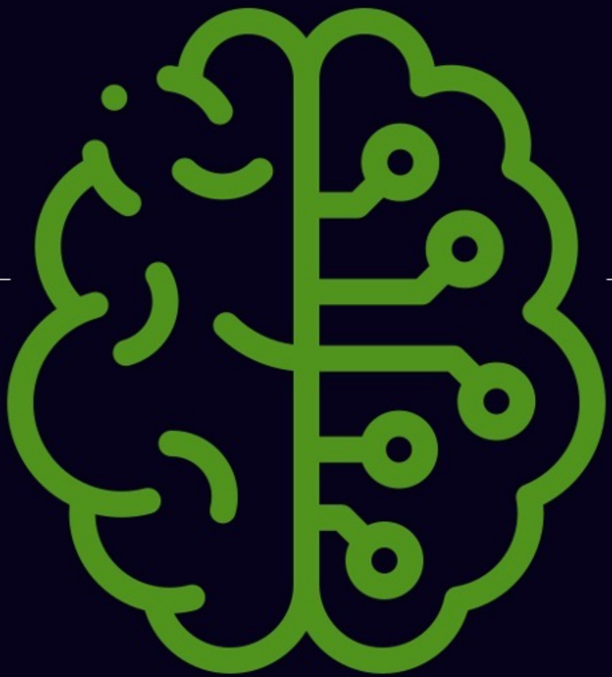
Use **AI**

To Address:

- Cyber Skills Shortage with automation
- Machine Speed vs human speed problems (with caution)
- SOC Data Flow with automation
- Expanding Attack Surface with automation

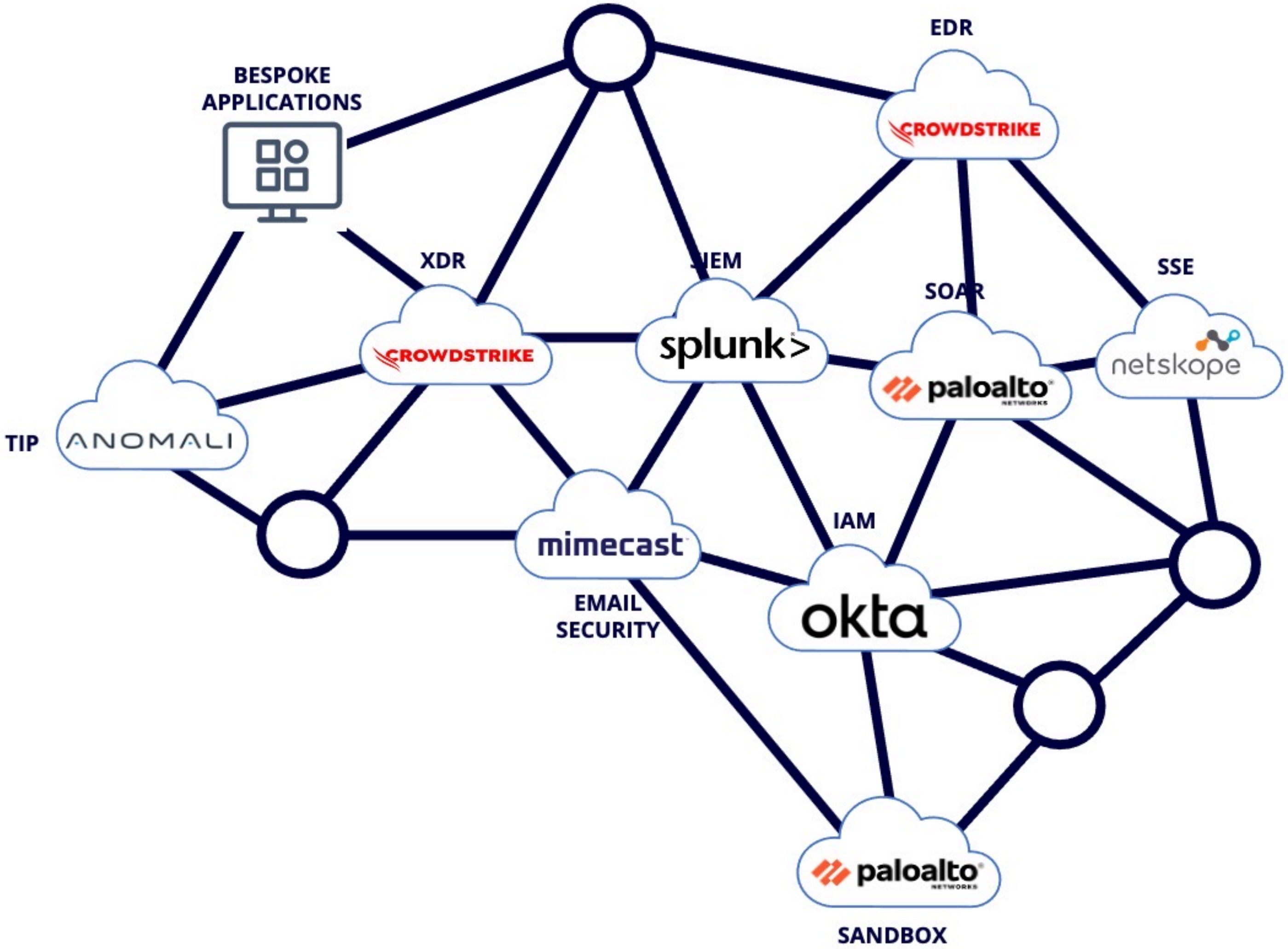
As part of defense in depth

Augment with other controls



To take more proactive and predictive approaches to cyber intelligence and defense

Enhance your security landscape



WORK PROTECTED.™

mimecast®