Incident Response
FORENSIC & CYBER

DICKER
DATA

Incident Response and Cyber

Dicker Data
Cybersecurity Roadshow

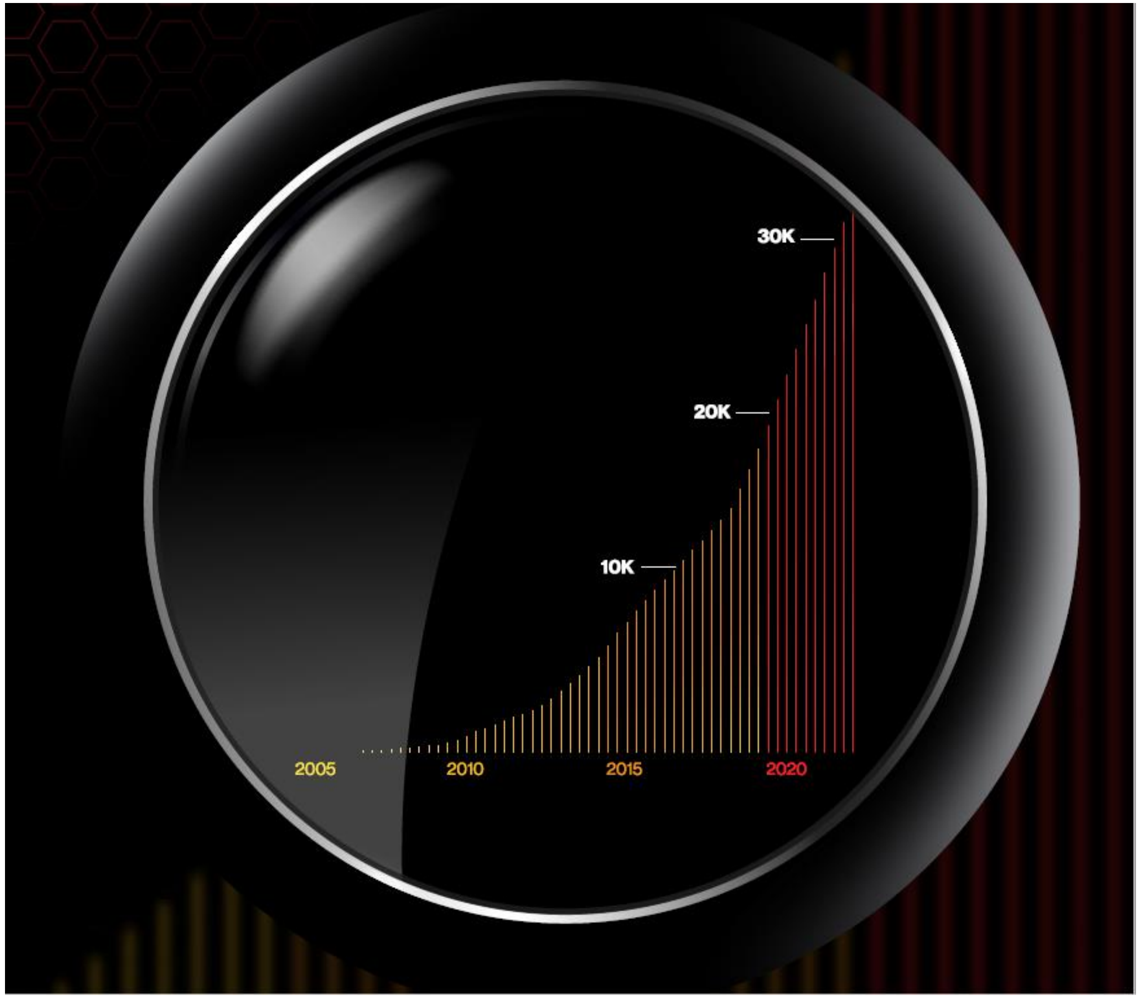
Digital Forensics and Incident Response

Verizon 2023 Data Breach Investigations Report (16th Edition)

- The DBIR was created to provide a place for security practitioners to look for data-driven, **real-world views** on cybercrime.
- This data informs us of the **steps we should take** to protect ourselves.
- The report is used to **increase awareness** of the tactics attackers are likely to use against organisations in your industry.
- It is also used as a tool to encourage executives to **support security initiatives and illustrate to employees** the importance of security and how they can help.

Verizon Data Breach Investigations Report (16th Edition)

- 16,312 security incidents that compromised the integrity, confidentiality or availability of an information asset.
- 5,199 breaches that resulted in the confirmed disclosure of data to an unauthorised party.
- *Total Set*
  - *953,894 incidents*
  - *254,968 breaches*



verizon.com/dbir

What Verizon Found – Key Statistics

- **74%** of all breaches include the <u>human element</u>

  Error, Privilege Misuse, stolen credentials or Social Engineering

- **50%** of all Social Engineering incidents used <u>pretexting</u>

  An invented scenario that tricks someone, that may result in a breach

- **24%** of all breaches involved <u>ransomware</u>

  Maliciously encrypting data and demanding a ransom to return or unlock it

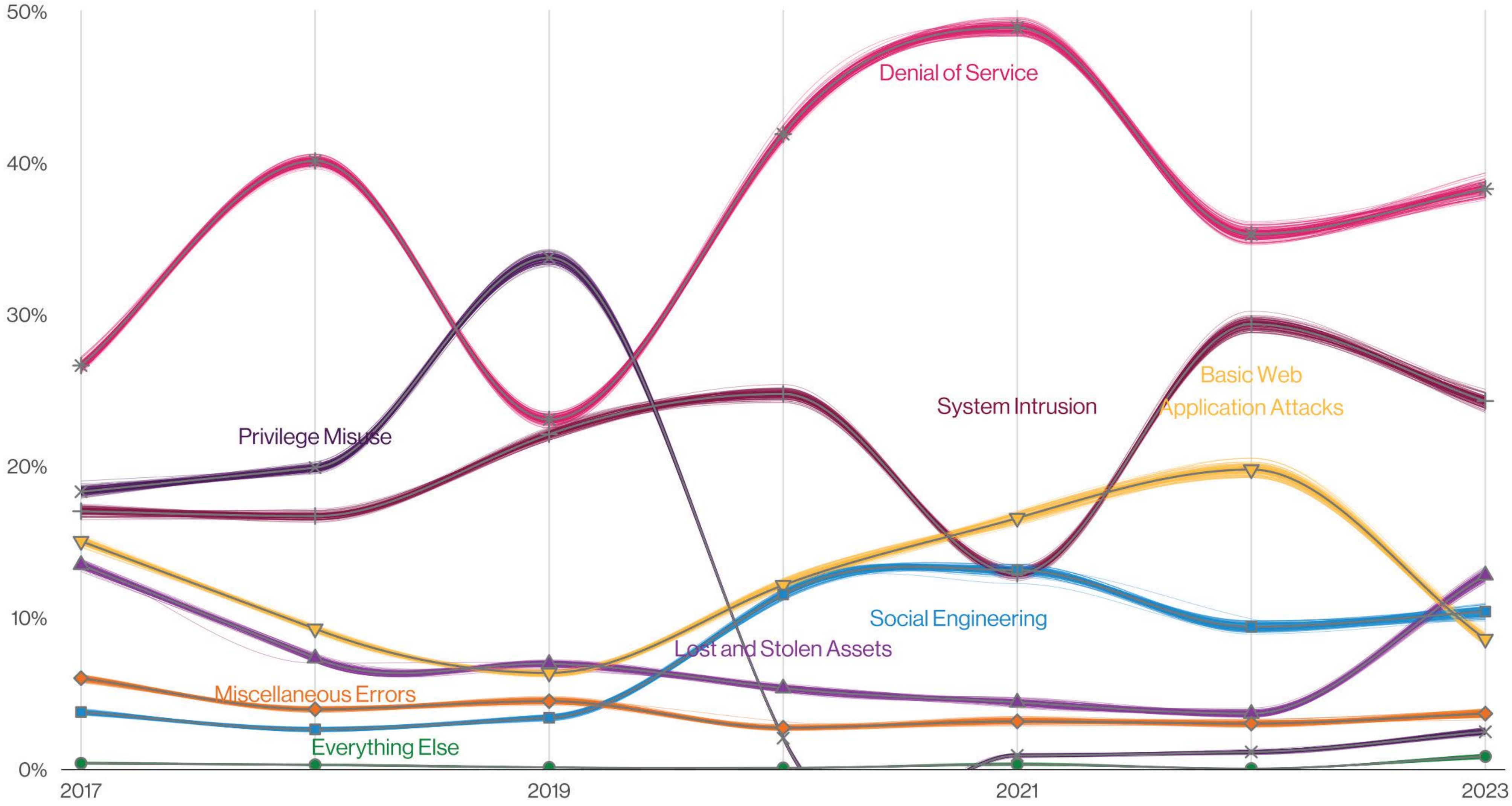
- **19%** involved <u>internal</u> actors

  Intentional and unintentional harm through misuse and simple human errors

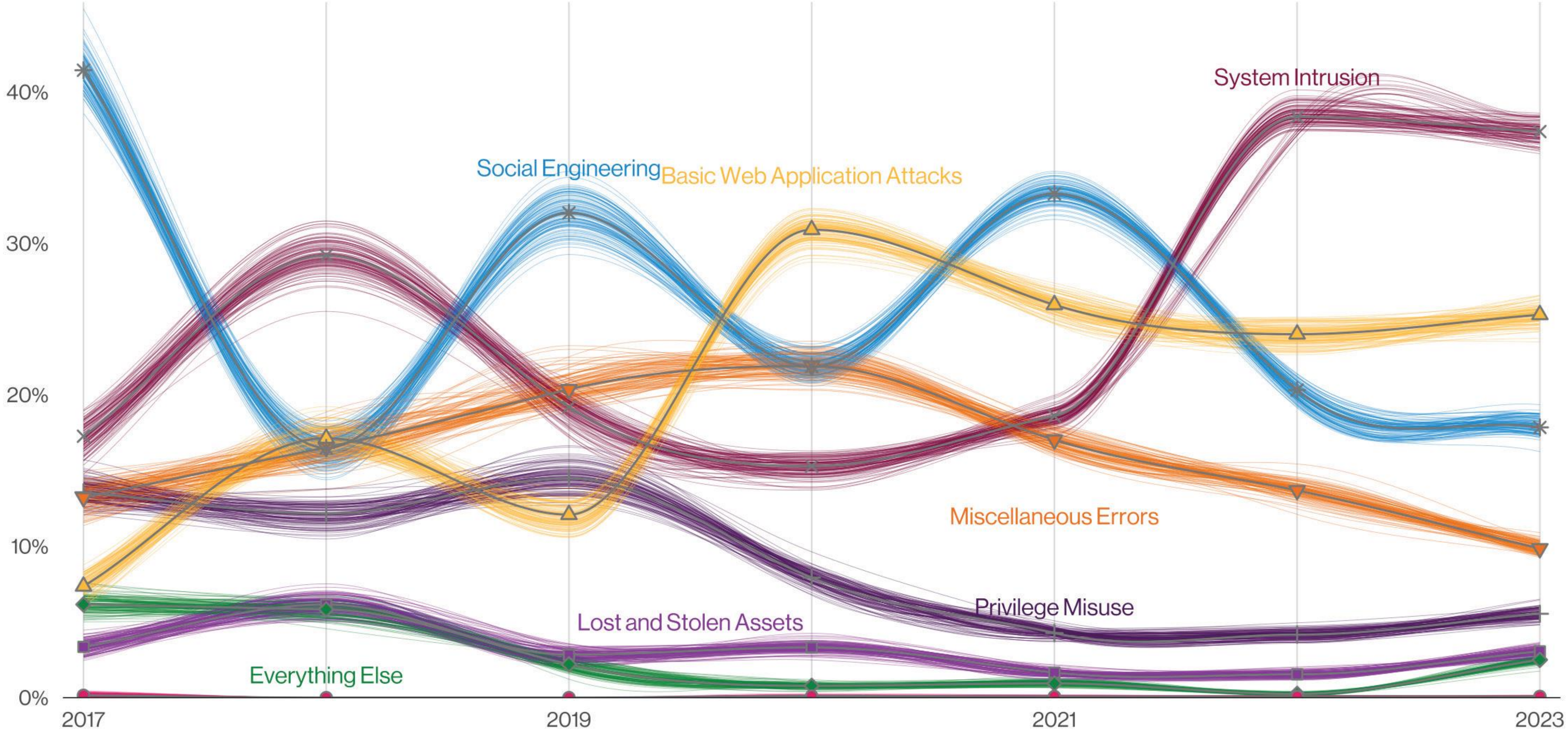
- **95%** of breaches are <u>financially</u> driven

  It’s (almost) always about the money

Patterns over time in incidents

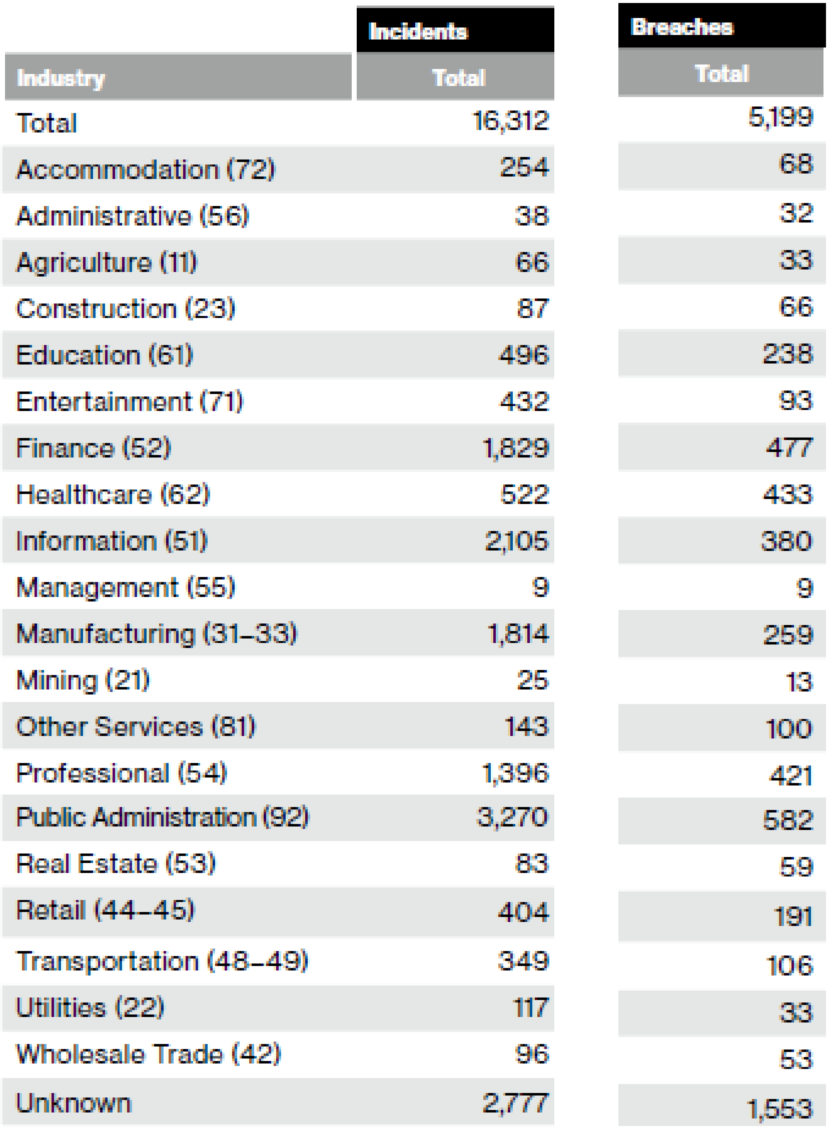


Patterns over time in breaches



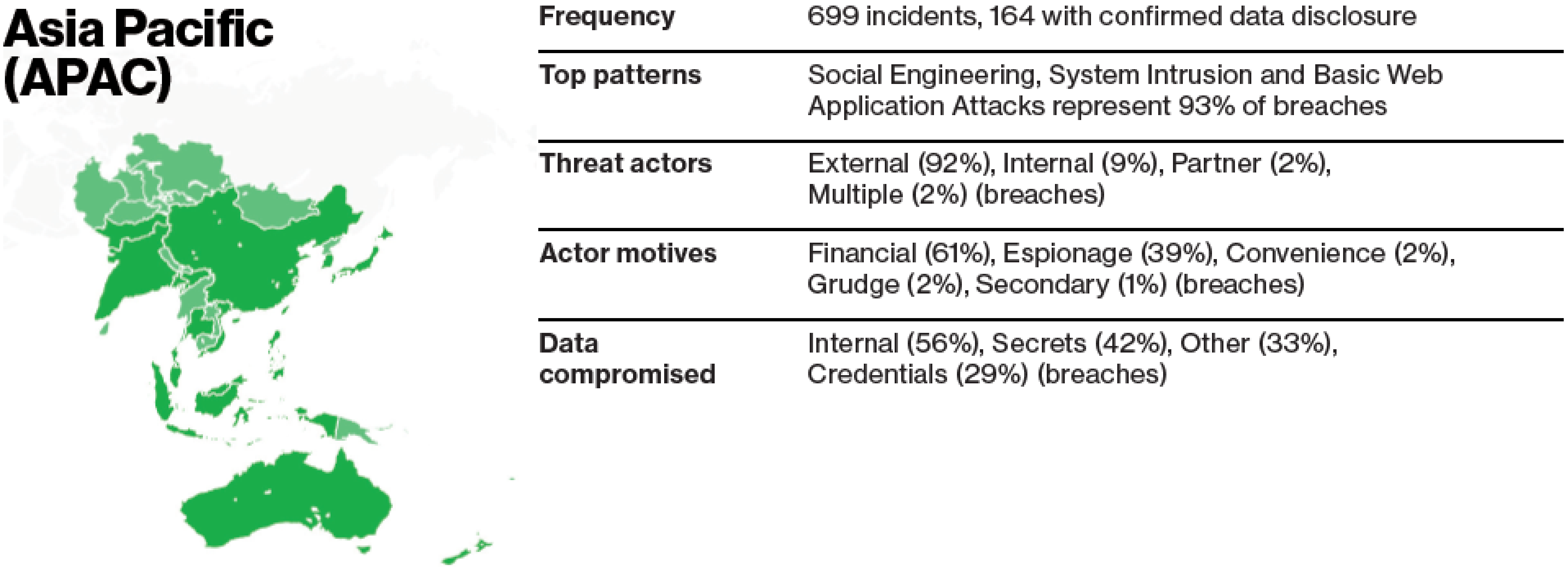
What Verizon Found – By Industry

	Incidents	Breaches
• Education	x 8	x 4
• Finance	x 35	x 9
• Healthcare	x 8	x 7
• Professional	x 26	x 8
• Public Administration	x 36	x 6
• Retail	x 9	x 4



	Incidents	Breaches
Industry	Total	Total
Total	16,312	5,199
Accommodation (72)	254	68
Administrative (56)	38	32
Agriculture (11)	66	33
Construction (23)	87	66
Education (61)	496	238
Entertainment (71)	432	93
Finance (52)	1,829	477
Healthcare (62)	522	433
Information (51)	2,105	380
Management (55)	9	9
Manufacturing (31–33)	1,814	259
Mining (21)	25	13
Other Services (81)	143	100
Professional (54)	1,396	421
Public Administration (92)	3,270	582
Real Estate (53)	83	59
Retail (44–45)	404	191
Transportation (48–49)	349	106
Utilities (22)	117	33
Wholesale Trade (42)	96	53
Unknown	2,777	1,553

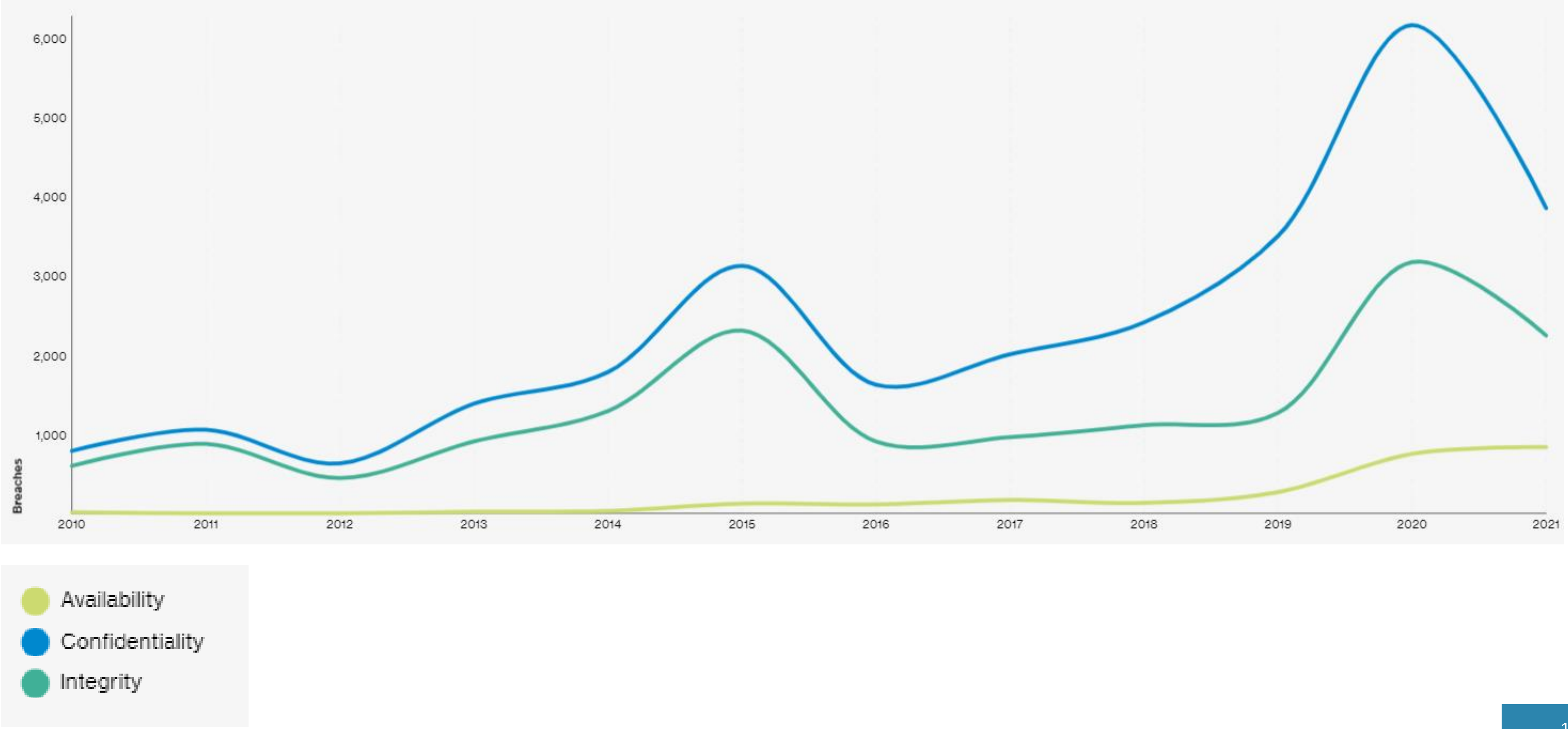
What Verizon Found – Asia Pacific Region



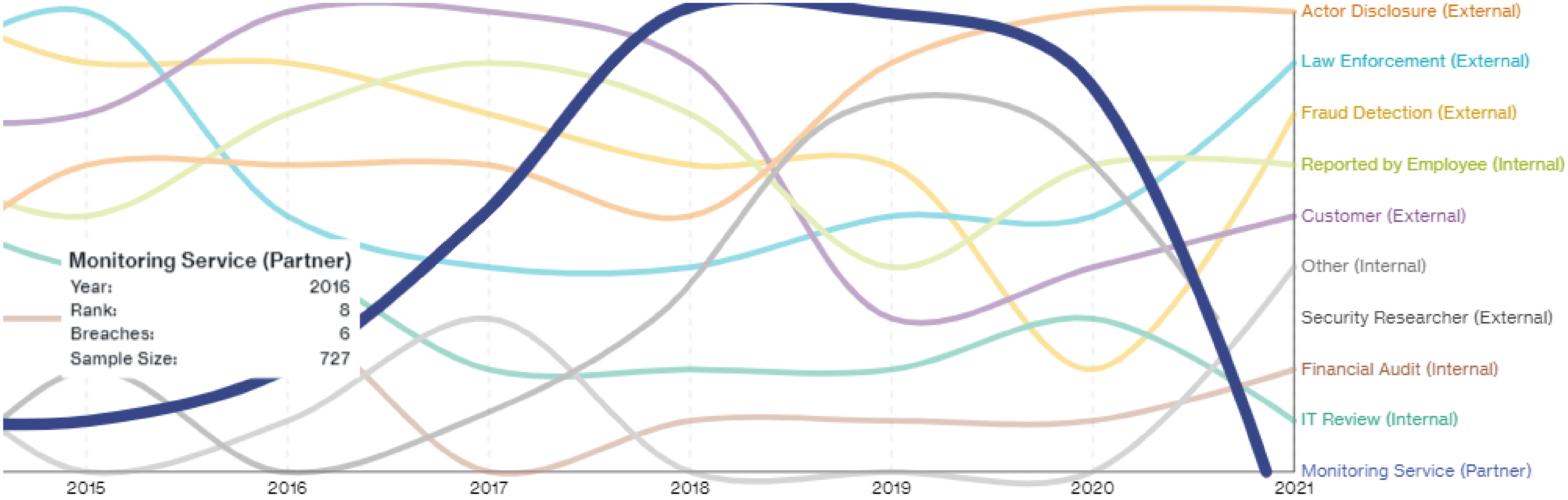
Asia Pacific (APAC)

Frequency	699 incidents, 164 with confirmed data disclosure
Top patterns	Social Engineering, System Intrusion and Basic Web Application Attacks represent 93% of breaches
Threat actors	External (92%), Internal (9%), Partner (2%), Multiple (2%) (breaches)
Actor motives	Financial (61%), Espionage (39%), Convenience (2%), Grudge (2%), Secondary (1%) (breaches)
Data compromised	Internal (56%), Secrets (42%), Other (33%), Credentials (29%) (breaches)

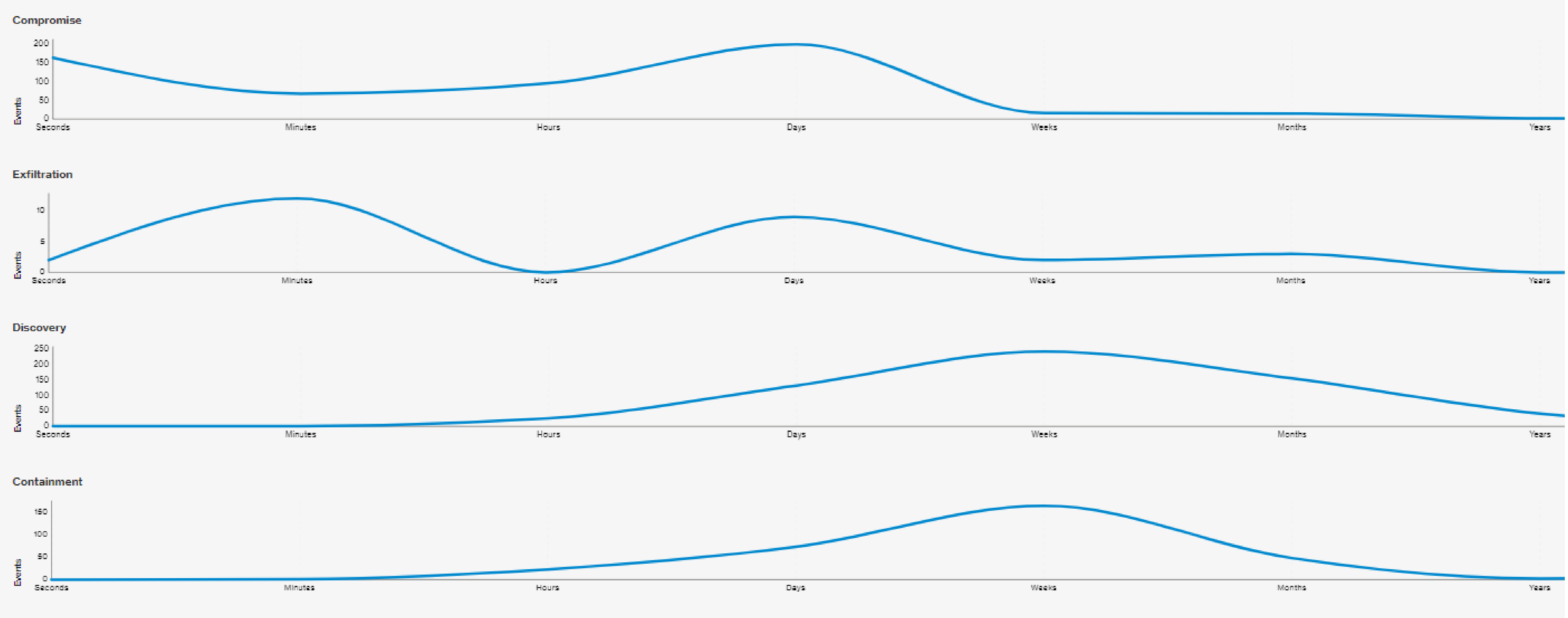
What Verizon Found - Breach Trends (15th Edition)



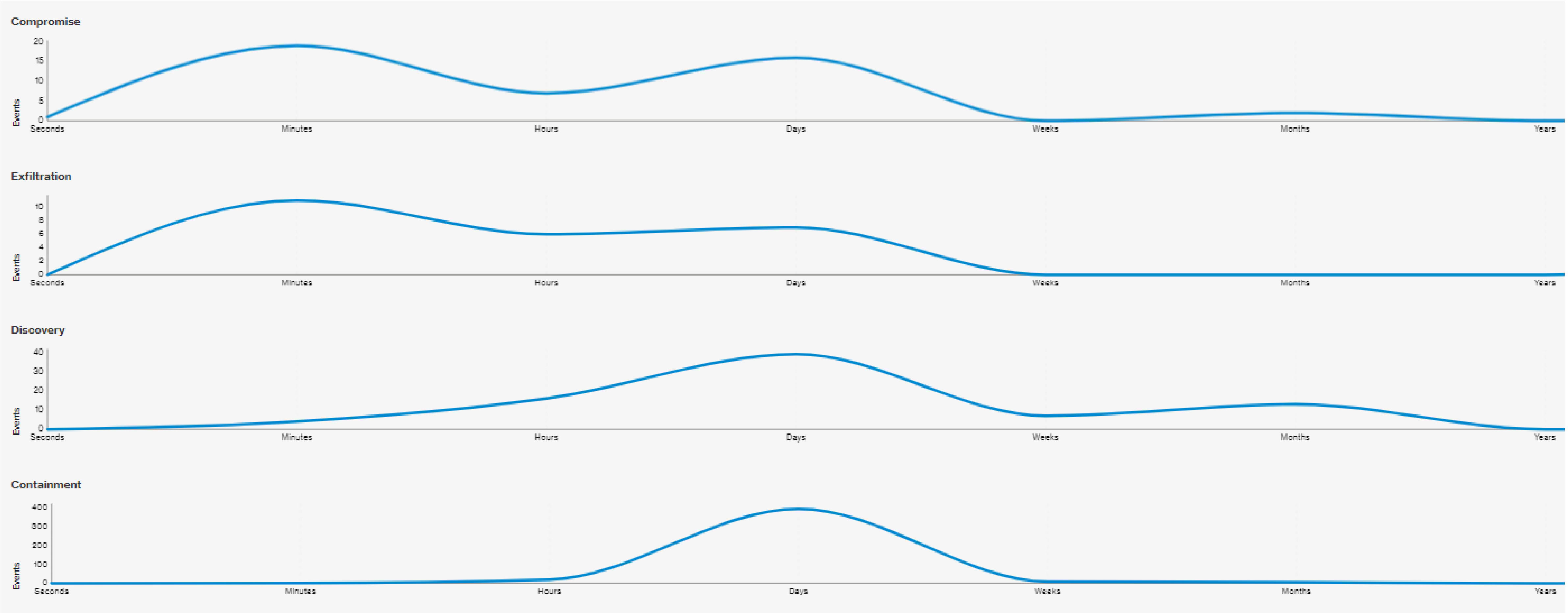
Discovery Methods Used Over Time (15th Edition)



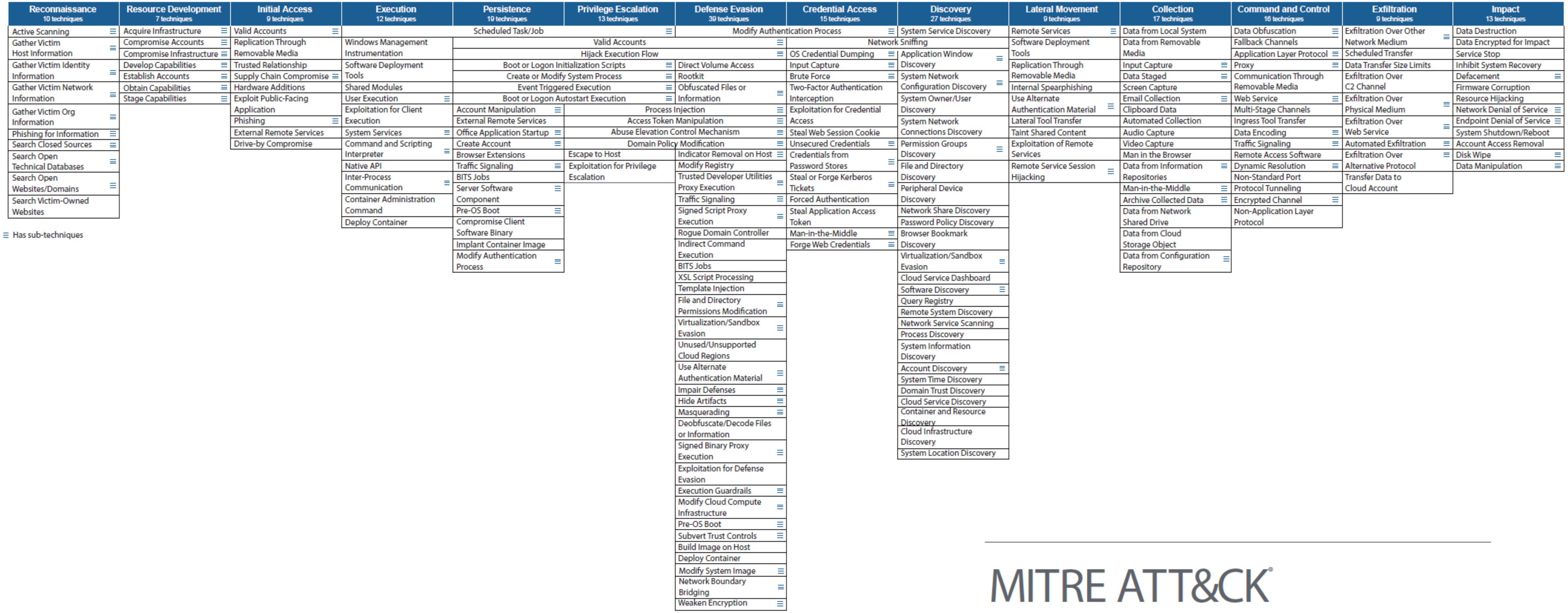
Response Time For Breach Events – 2010 (15th Edition)



Response Time For Breach Events – 2021 (15th Edition)



MITRE ATT&CK®



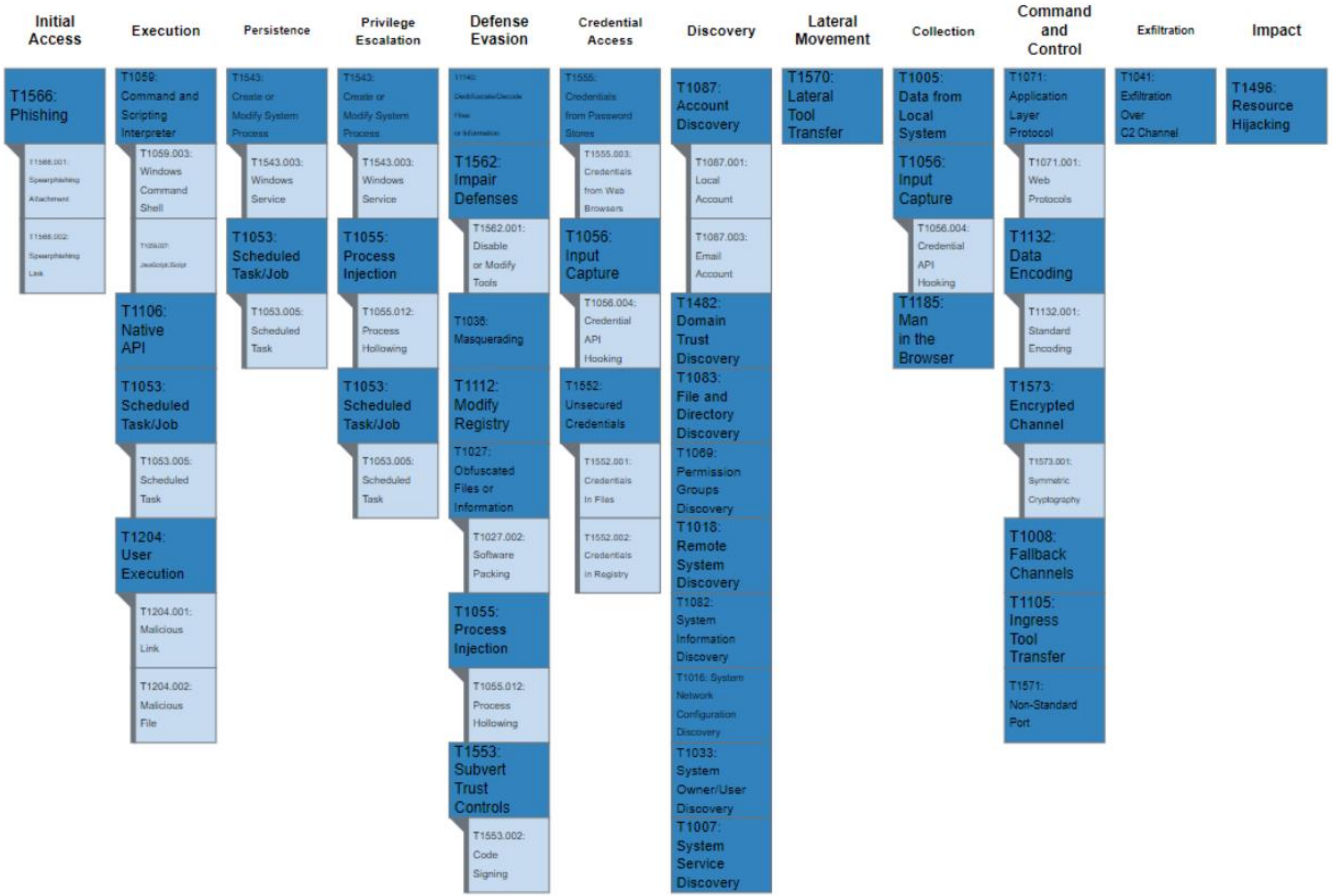
Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning	Acquire Infrastructure	Valid Accounts	Scheduled Task/Job			Modify Authentication Process		System Service Discovery	Remote Services	Data from Local System	Data Obfuscation	Exfiltration Over Other Network Medium	Data Destruction
Gather Victim Host Information	Compromise Accounts	Replication Through Removable Media	Windows Management Instrumentation	Valid Accounts			Network Sniffing		Software Deployment Tools	Data from Removable Media	Fallback Channels		Data Encrypted for Impact
	Compromise Infrastructure			Hijack Execution Flow			OS Credential Dumping	Application Window Discovery			Application Layer Protocol	Scheduled Transfer	Service Stop
Gather Victim Identity Information	Develop Capabilities	Trusted Relationship	Software Deployment Tools	Boot or Logon Initialization Scripts		Direct Volume Access	Input Capture		Replication Through Removable Media	Input Capture	Proxy	Data Transfer Size Limits	Inhibit System Recovery
	Establish Accounts	Supply Chain Compromise		Create or Modify System Process		Rootkit	Brute Force	System Network Configuration Discovery		Data Staged	Communication Through Removable Media	Exfiltration Over C2 Channel	Defacement
Gather Victim Network Information	Obtain Capabilities	Hardware Additions	Shared Modules	Event Triggered Execution		Obfuscated Files or Information	Two-Factor Authentication Interception		Internal Spearphishing	Screen Capture			Firmware Corruption
	Stage Capabilities	Exploit Public-Facing Application	User Execution	Boot or Logon Autostart Execution				System Owner/User Discovery	Use Alternate Authentication Material	Email Collection	Web Service	Exfiltration Over Physical Medium	Resource Hijacking
Gather Victim Org Information			Exploitation for Client Execution	Account Manipulation	Process Injection		Exploitation for Credential Access			Clipboard Data	Multi-Stage Channels		Network Denial of Service
		Phishing		External Remote Services	Access Token Manipulation			System Network Connections Discovery	Lateral Tool Transfer	Automated Collection	Ingress Tool Transfer	Exfiltration Over Web Service	Endpoint Denial of Service
Phishing for Information		External Remote Services	System Services	Office Application Startup	Abuse Elevation Control Mechanism		Steal Web Session Cookie		Taint Shared Content	Audio Capture	Data Encoding		System Shutdown/Reboot
Search Closed Sources		Drive-by Compromise	Command and Scripting Interpreter	Create Account	Domain Policy Modification		Unsecured Credentials	Permission Groups Discovery	Exploitation of Remote Services	Video Capture	Traffic Signaling	Automated Exfiltration	Account Access Removal
Search Open Technical Databases				Browser Extensions	Escape to Host	Indicator Removal on Host	Credentials from Password Stores			Man in the Browser	Remote Access Software	Exfiltration Over Alternative Protocol	Disk Wipe
			Native API	Traffic Signaling	Exploitation for Privilege Escalation	Modify Registry		File and Directory Discovery	Remote Service Session Hijacking	Data from Information Repositories	Dynamic Resolution		Data Manipulation
Search Open Websites/Domains			Inter-Process Communication	BITS Jobs		Trusted Developer Utilities Proxy Execution	Steal or Forge Kerberos Tickets				Non-Standard Port	Transfer Data to Cloud Account	
				Server Software Component				Peripheral Device Discovery		Man-in-the-Middle	Protocol Tunneling		
Search Victim-Owned Websites			Container Administration Command			Traffic Signaling	Forced Authentication			Archive Collected Data	Encrypted Channel		
				Pre-OS Boot		Signed Script Proxy Execution	Steal Application Access Token	Network Share Discovery		Data from Network Shared Drive	Non-Application Layer Protocol		
			Deploy Container	Compromise Client Software Binary				Password Policy Discovery					
						Rogue Domain Controller	Man-in-the-Middle	Browser Bookmark Discovery		Data from Cloud Storage Object			
				Implant Container Image		Indirect Command Execution	Forge Web Credentials						
				Modify Authentication Process				Virtualization/Sandbox Evasion		Data from Configuration Repository			
						BITS Jobs		Cloud Service Dashboard					
						XSL Script Processing		Software Discovery					
						Template Injection		Query Registry					
						File and Directory Permissions Modification		Remote System Discovery					
						Virtualization/Sandbox Evasion		Network Service Scanning					
						Unused/Unsupported Cloud Regions		Process Discovery					
						Use Alternate Authentication Material		System Information Discovery					
						Impair Defenses		Account Discovery					
						Hide Artifacts		System Time Discovery					
						Masquerading		Domain Trust Discovery					
						Deobfuscate/Decode Files or Information		Cloud Service Discovery					
						Signed Binary Proxy Execution		Container and Resource Discovery					
						Exploitation for Defense Evasion		Cloud Infrastructure Discovery					
						Execution Guardrails		System Location Discovery					
						Modify Cloud Compute Infrastructure							
						Pre-OS Boot							
						Subvert Trust Controls							
						Build Image on Host							
						Deploy Container							
						Modify System Image							
						Network Boundary Bridging							
						Weaken Encryption							

≡ Has sub-techniques

MITRE ATT&CK®
Enterprise Framework

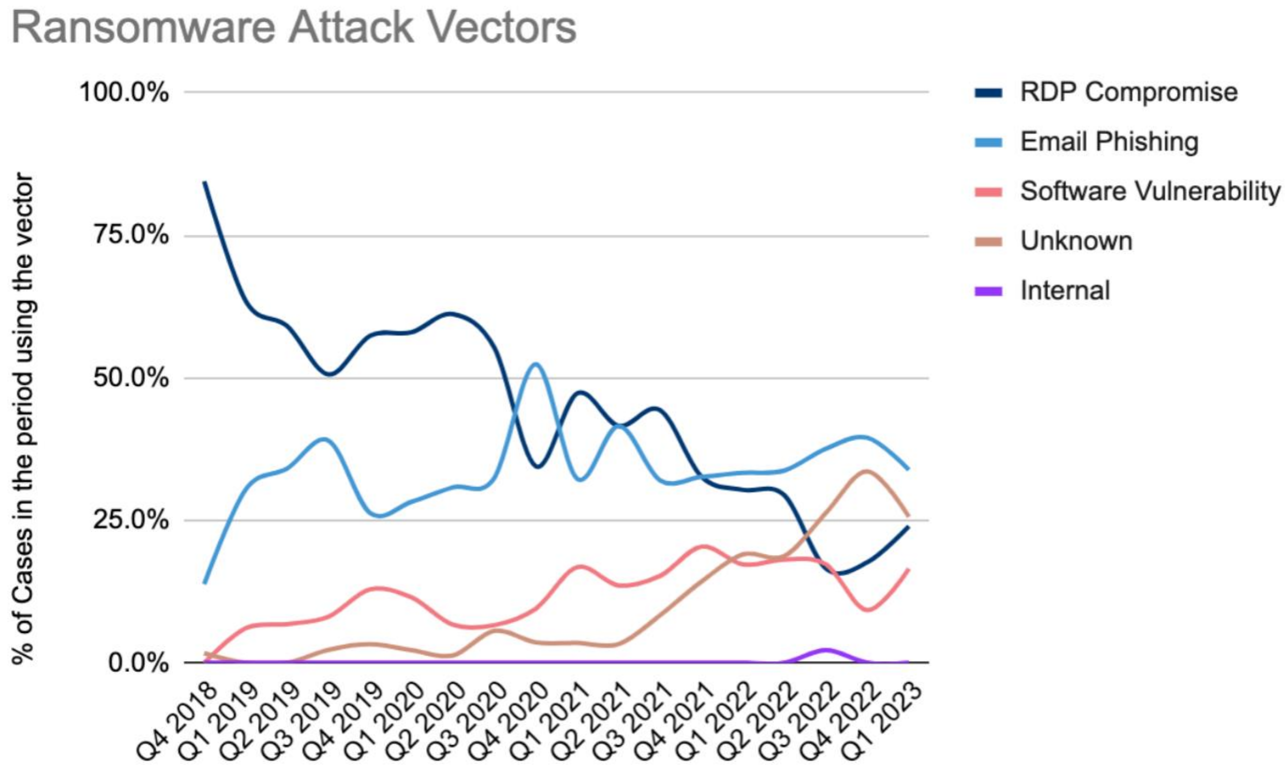
attack.mitre.org

MITRE ATT&CK® - Trickbot



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
T1566: Phishing	T1059: Command and Scripting Interpreter	T1543: Create or Modify System Process	T1543: Create or Modify System Process	T1140: Deobfuscate/Decode Files or Information	T1555: Credentials from Password Stores	T1087: Account Discovery	T1570: Lateral Tool Transfer	T1005: Data from Local System	T1071: Application Layer Protocol	T1041: Exfiltration Over C2 Channel	T1496: Resource Hijacking
T1566.001: Spearphishing Attachment	T1059.003: Windows Command Shell	T1543.003: Windows Service	T1543.003: Windows Service	T1562: Impair Defenses	T1555.003: Credentials from Web Browsers	T1087.001: Local Account		T1056: Input Capture	T1071.001: Web Protocols		
T1566.002: Spearphishing Link	T1059.007: JavaScript/JScript	T1053: Scheduled Task/Job	T1055: Process Injection	T1562.001: Disable or Modify Tools	T1056: Input Capture	T1087.003: Email Account		T1056.004: Credential API Hooking	T1132: Data Encoding		
	T1106: Native API	T1053.005: Scheduled Task	T1055.012: Process Hollowing	T1036: Masquerading	T1056.004: Credential API Hooking	T1482: Domain Trust Discovery		T1185: Man in the Browser	T1132.001: Standard Encoding		
	T1053: Scheduled Task/Job		T1053: Scheduled Task/Job	T1112: Modify Registry	T1552: Unsecured Credentials	T1083: File and Directory Discovery			T1573: Encrypted Channel		
	T1053.005: Scheduled Task		T1053.005: Scheduled Task	T1027: Obfuscated Files or Information	T1552.001: Credentials In Files	T1069: Permission Groups Discovery			T1573.001: Symmetric Cryptography		
	T1204: User Execution			T1027.002: Software Packing	T1552.002: Credentials in Registry	T1018: Remote System Discovery			T1008: Fallback Channels		
	T1204.001: Malicious Link			T1055: Process Injection		T1082: System Information Discovery			T1105: Ingress Tool Transfer		
	T1204.002: Malicious File			T1055.012: Process Hollowing		T1016: System Network Configuration Discovery			T1571: Non-Standard Port		
				T1553: Subvert Trust Controls		T1033: System Owner/User Discovery					
				T1553.002: Code Signing		T1007: System Service Discovery					

Ransomware – Vectors and Groups



Rank	Ransomware Type	Market Share %
1	BlackCat	12.6%
2	Black Basta	11.8%
2	Royal	11.8%
3	Hive	7.1%
4	Lockbit 3.0	6.3%
5	Phobos	4.7%
5	BianLian	4.7%
6	Play Ransomware	3.9%

https://www.coveware.com/ransomware-quarterly-reports

Digital Forensics

nuix

reveal | brainspace

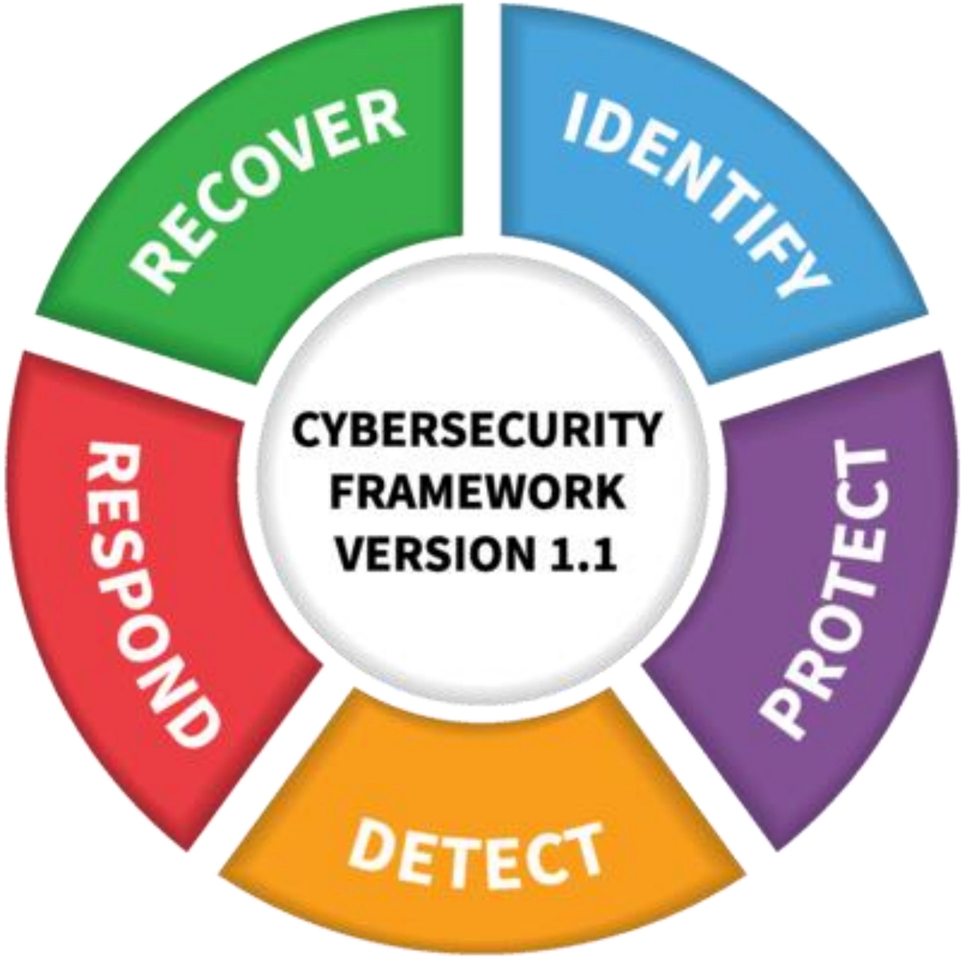
Relativity®

Cellebrite

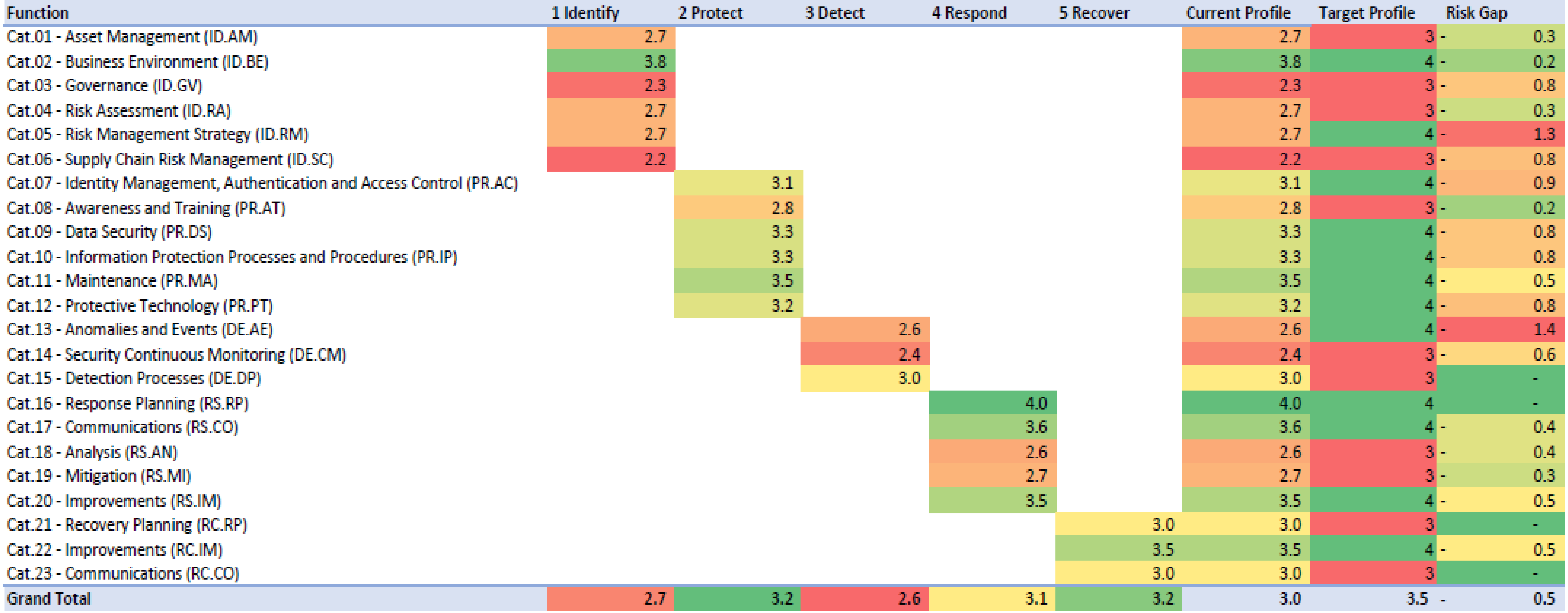
Canopy

Cyber Governance

NIST Cyber Security Framework

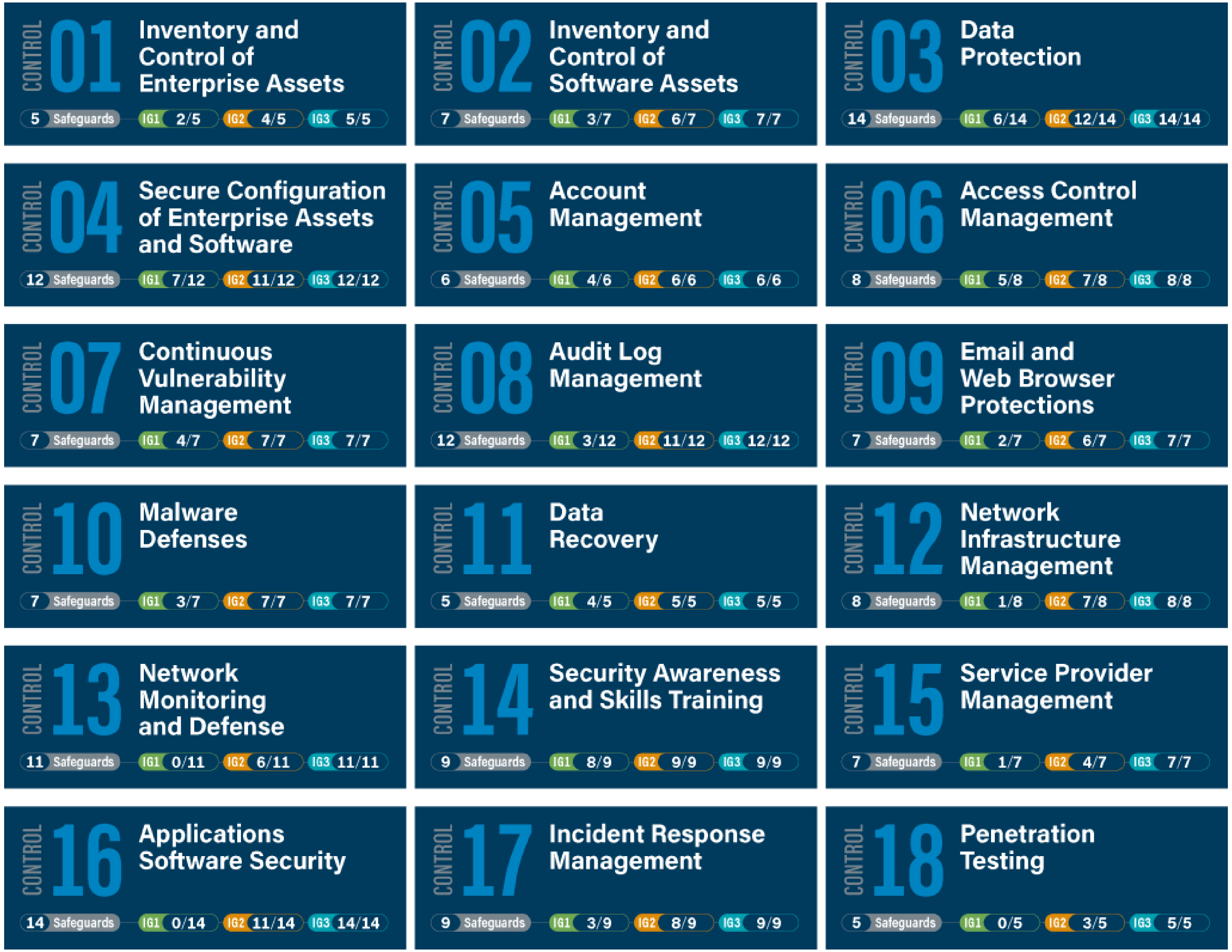


Completed Framework Example



Function	1 Identify	2 Protect	3 Detect	4 Respond	5 Recover	Current Profile	Target Profile	Risk Gap
Cat.01 - Asset Management (ID.AM)	2.7					2.7	3	- 0.3
Cat.02 - Business Environment (ID.BE)	3.8					3.8	4	- 0.2
Cat.03 - Governance (ID.GV)	2.3					2.3	3	- 0.8
Cat.04 - Risk Assessment (ID.RA)	2.7					2.7	3	- 0.3
Cat.05 - Risk Management Strategy (ID.RM)	2.7					2.7	4	- 1.3
Cat.06 - Supply Chain Risk Management (ID.SC)	2.2					2.2	3	- 0.8
Cat.07 - Identity Management, Authentication and Access Control (PR.AC)		3.1				3.1	4	- 0.9
Cat.08 - Awareness and Training (PR.AT)		2.8				2.8	3	- 0.2
Cat.09 - Data Security (PR.DS)		3.3				3.3	4	- 0.8
Cat.10 - Information Protection Processes and Procedures (PR.IP)		3.3				3.3	4	- 0.8
Cat.11 - Maintenance (PR.MA)		3.5				3.5	4	- 0.5
Cat.12 - Protective Technology (PR.PT)		3.2				3.2	4	- 0.8
Cat.13 - Anomalies and Events (DE.AE)			2.6			2.6	4	- 1.4
Cat.14 - Security Continuous Monitoring (DE.CM)			2.4			2.4	3	- 0.6
Cat.15 - Detection Processes (DE.DP)			3.0			3.0	3	-
Cat.16 - Response Planning (RS.RP)				4.0		4.0	4	-
Cat.17 - Communications (RS.CO)				3.6		3.6	4	- 0.4
Cat.18 - Analysis (RS.AN)				2.6		2.6	3	- 0.4
Cat.19 - Mitigation (RS.MI)				2.7		2.7	3	- 0.3
Cat.20 - Improvements (RS.IM)				3.5		3.5	4	- 0.5
Cat.21 - Recovery Planning (RC.RP)					3.0	3.0	3	-
Cat.22 - Improvements (RC.IM)					3.5	3.5	4	- 0.5
Cat.23 - Communications (RC.CO)					3.0	3.0	3	-
Grand Total	2.7	3.2	2.6	3.1	3.2	3.0	3.5	- 0.5

CIS Controls



CONTROL 01 Inventory and Control of Enterprise Assets
5 Safeguards IG1 2/5 IG2 4/5 IG3 5/5

CONTROL 02 Inventory and Control of Software Assets
7 Safeguards IG1 3/7 IG2 6/7 IG3 7/7

CONTROL 03 Data Protection
14 Safeguards IG1 6/14 IG2 12/14 IG3 14/14

CONTROL 04 Secure Configuration of Enterprise Assets and Software
12 Safeguards IG1 7/12 IG2 11/12 IG3 12/12

CONTROL 05 Account Management
6 Safeguards IG1 4/6 IG2 6/6 IG3 6/6

CONTROL 06 Access Control Management
8 Safeguards IG1 5/8 IG2 7/8 IG3 8/8

CONTROL 07 Continuous Vulnerability Management
7 Safeguards IG1 4/7 IG2 7/7 IG3 7/7

CONTROL 08 Audit Log Management
12 Safeguards IG1 3/12 IG2 11/12 IG3 12/12

CONTROL 09 Email and Web Browser Protections
7 Safeguards IG1 2/7 IG2 6/7 IG3 7/7

CONTROL 10 Malware Defenses
7 Safeguards IG1 3/7 IG2 7/7 IG3 7/7

CONTROL 11 Data Recovery
5 Safeguards IG1 4/5 IG2 5/5 IG3 5/5

CONTROL 12 Network Infrastructure Management
8 Safeguards IG1 1/8 IG2 7/8 IG3 8/8

CONTROL 13 Network Monitoring and Defense
11 Safeguards IG1 0/11 IG2 6/11 IG3 11/11

CONTROL 14 Security Awareness and Skills Training
9 Safeguards IG1 8/9 IG2 9/9 IG3 9/9

CONTROL 15 Service Provider Management
7 Safeguards IG1 1/7 IG2 4/7 IG3 7/7

CONTROL 16 Applications Software Security
14 Safeguards IG1 0/14 IG2 11/14 IG3 14/14

CONTROL 17 Incident Response Management
9 Safeguards IG1 3/9 IG2 8/9 IG3 9/9

CONTROL 18 Penetration Testing
5 Safeguards IG1 0/5 IG2 3/5 IG3 5/5

CIS Controls

IG1 is the definition of basic cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

56
Cyber defense Safeguards

IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

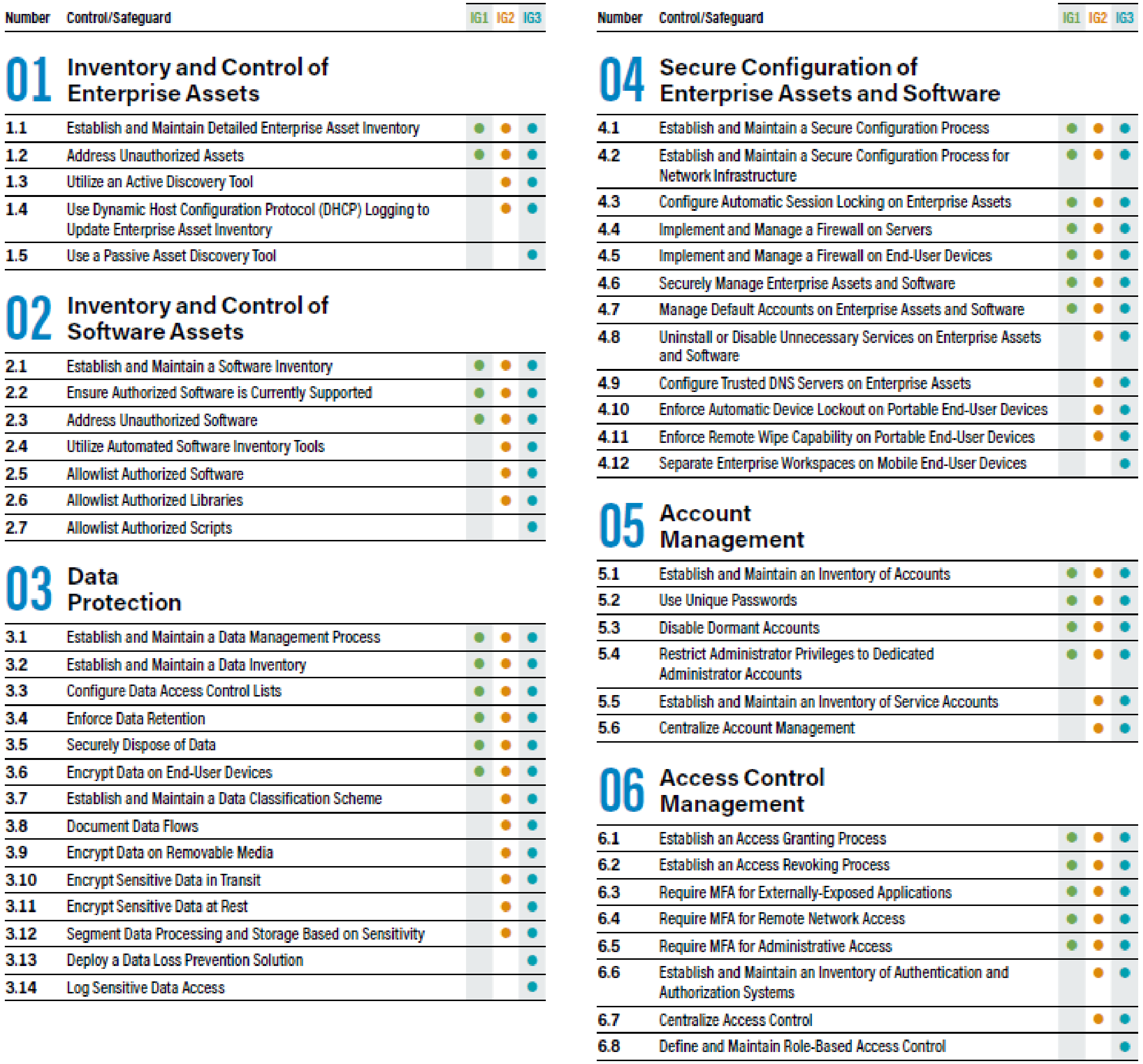
74
Additional cyber defense Safeguards

IG3 assists enterprises with IT security experts secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

23
Additional cyber defense Safeguards

Total Safeguards **153**

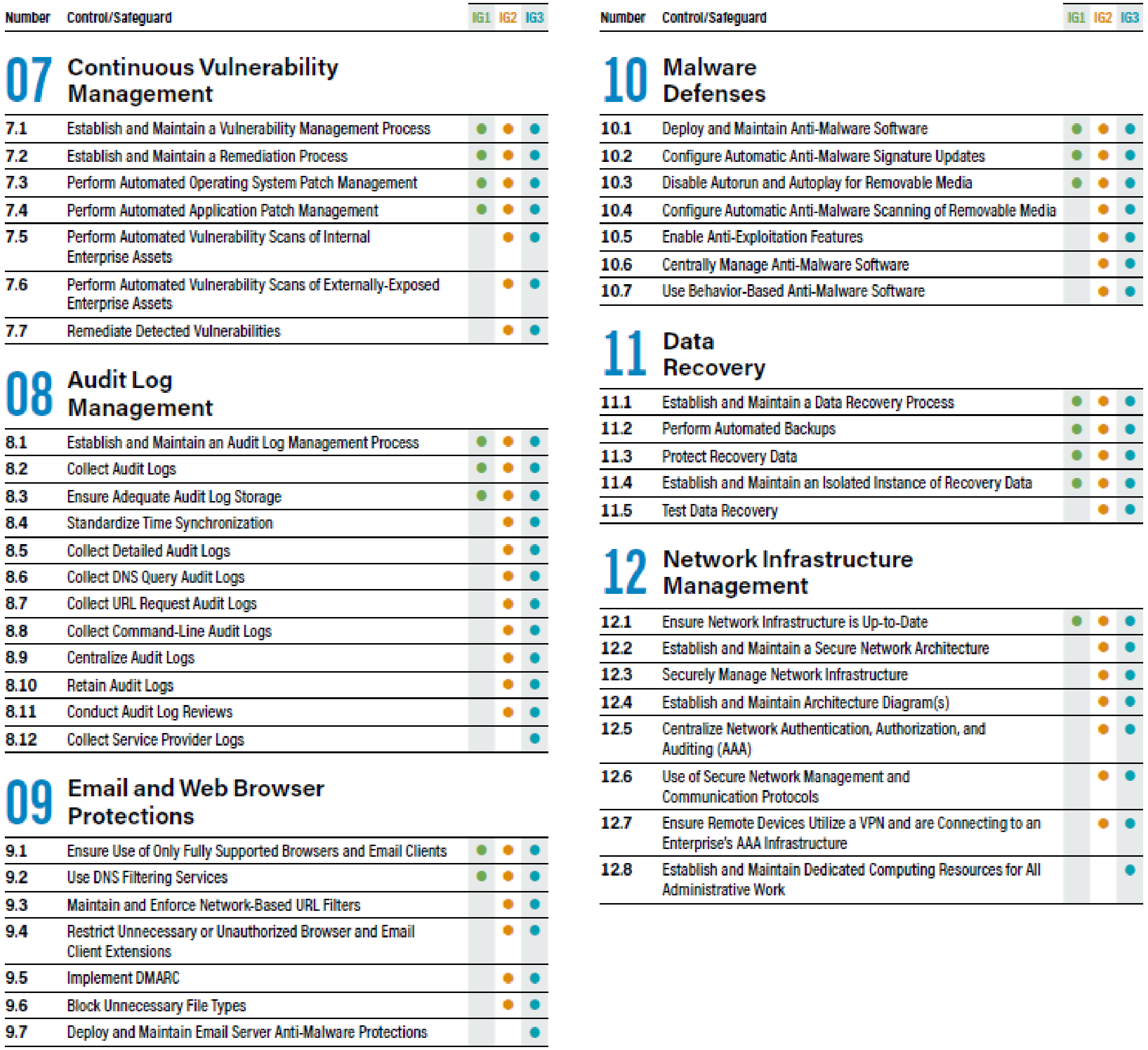
CIS Controls



Number	Control/Safeguard	IG1	IG2	IG3
01	**Inventory and Control of Enterprise Assets**			
1.1	Establish and Maintain Detailed Enterprise Asset Inventory	●	●	●
1.2	Address Unauthorized Assets	●	●	●
1.3	Utilize an Active Discovery Tool		●	●
1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory		●	●
1.5	Use a Passive Asset Discovery Tool			●
02	**Inventory and Control of Software Assets**			
2.1	Establish and Maintain a Software Inventory	●	●	●
2.2	Ensure Authorized Software is Currently Supported	●	●	●
2.3	Address Unauthorized Software	●	●	●
2.4	Utilize Automated Software Inventory Tools		●	●
2.5	Allowlist Authorized Software		●	●
2.6	Allowlist Authorized Libraries		●	●
2.7	Allowlist Authorized Scripts			●
03	**Data Protection**			
3.1	Establish and Maintain a Data Management Process	●	●	●
3.2	Establish and Maintain a Data Inventory	●	●	●
3.3	Configure Data Access Control Lists	●	●	●
3.4	Enforce Data Retention	●	●	●
3.5	Securely Dispose of Data	●	●	●
3.6	Encrypt Data on End-User Devices	●	●	●
3.7	Establish and Maintain a Data Classification Scheme		●	●
3.8	Document Data Flows		●	●
3.9	Encrypt Data on Removable Media		●	●
3.10	Encrypt Sensitive Data in Transit		●	●
3.11	Encrypt Sensitive Data at Rest		●	●
3.12	Segment Data Processing and Storage Based on Sensitivity		●	●
3.13	Deploy a Data Loss Prevention Solution			●
3.14	Log Sensitive Data Access			●

Number	Control/Safeguard	IG1	IG2	IG3
04	**Secure Configuration of Enterprise Assets and Software**			
4.1	Establish and Maintain a Secure Configuration Process	●	●	●
4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	●	●	●
4.3	Configure Automatic Session Locking on Enterprise Assets	●	●	●
4.4	Implement and Manage a Firewall on Servers	●	●	●
4.5	Implement and Manage a Firewall on End-User Devices	●	●	●
4.6	Securely Manage Enterprise Assets and Software	●	●	●
4.7	Manage Default Accounts on Enterprise Assets and Software	●	●	●
4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software		●	●
4.9	Configure Trusted DNS Servers on Enterprise Assets		●	●
4.10	Enforce Automatic Device Lockout on Portable End-User Devices		●	●
4.11	Enforce Remote Wipe Capability on Portable End-User Devices		●	●
4.12	Separate Enterprise Workspaces on Mobile End-User Devices			●
05	**Account Management**			
5.1	Establish and Maintain an Inventory of Accounts	●	●	●
5.2	Use Unique Passwords	●	●	●
5.3	Disable Dormant Accounts	●	●	●
5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	●	●	●
5.5	Establish and Maintain an Inventory of Service Accounts		●	●
5.6	Centralize Account Management		●	●
06	**Access Control Management**			
6.1	Establish an Access Granting Process	●	●	●
6.2	Establish an Access Revoking Process	●	●	●
6.3	Require MFA for Externally-Exposed Applications	●	●	●
6.4	Require MFA for Remote Network Access	●	●	●
6.5	Require MFA for Administrative Access	●	●	●
6.6	Establish and Maintain an Inventory of Authentication and Authorization Systems		●	●
6.7	Centralize Access Control		●	●
6.8	Define and Maintain Role-Based Access Control			●

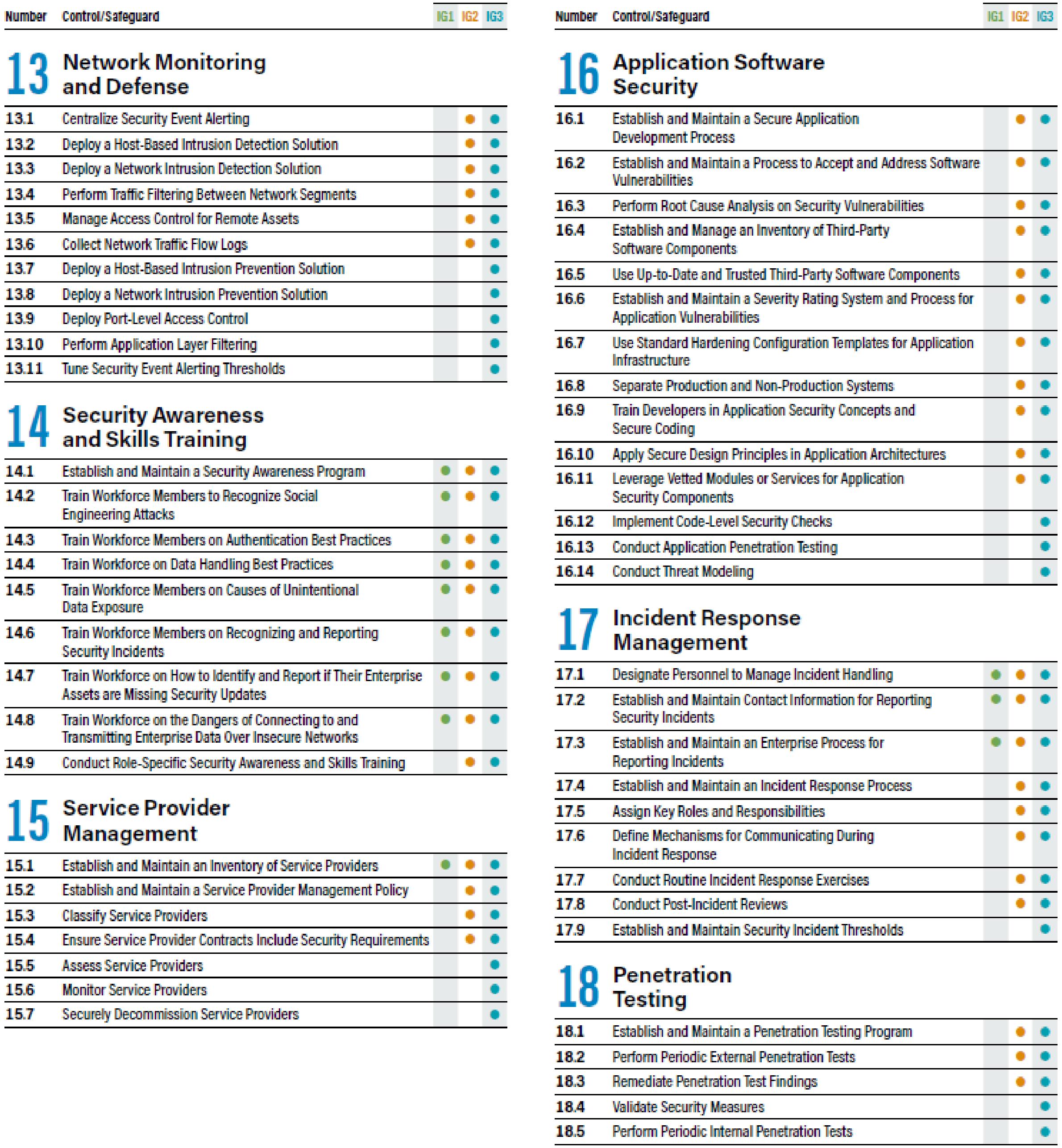
CIS Controls



Number	Control/Safeguard	IG1	IG2	IG3
07	**Continuous Vulnerability Management**			
7.1	Establish and Maintain a Vulnerability Management Process	●	●	●
7.2	Establish and Maintain a Remediation Process	●	●	●
7.3	Perform Automated Operating System Patch Management	●	●	●
7.4	Perform Automated Application Patch Management	●	●	●
7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets		●	●
7.6	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets		●	●
7.7	Remediate Detected Vulnerabilities		●	●
08	**Audit Log Management**			
8.1	Establish and Maintain an Audit Log Management Process	●	●	●
8.2	Collect Audit Logs	●	●	●
8.3	Ensure Adequate Audit Log Storage	●	●	●
8.4	Standardize Time Synchronization		●	●
8.5	Collect Detailed Audit Logs		●	●
8.6	Collect DNS Query Audit Logs		●	●
8.7	Collect URL Request Audit Logs		●	●
8.8	Collect Command-Line Audit Logs		●	●
8.9	Centralize Audit Logs		●	●
8.10	Retain Audit Logs		●	●
8.11	Conduct Audit Log Reviews		●	●
8.12	Collect Service Provider Logs			●
09	**Email and Web Browser Protections**			
9.1	Ensure Use of Only Fully Supported Browsers and Email Clients	●	●	●
9.2	Use DNS Filtering Services	●	●	●
9.3	Maintain and Enforce Network-Based URL Filters		●	●
9.4	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions		●	●
9.5	Implement DMARC		●	●
9.6	Block Unnecessary File Types		●	●
9.7	Deploy and Maintain Email Server Anti-Malware Protections			●

Number	Control/Safeguard	IG1	IG2	IG3
10	**Malware Defenses**			
10.1	Deploy and Maintain Anti-Malware Software	●	●	●
10.2	Configure Automatic Anti-Malware Signature Updates	●	●	●
10.3	Disable Autorun and Autoplay for Removable Media	●	●	●
10.4	Configure Automatic Anti-Malware Scanning of Removable Media		●	●
10.5	Enable Anti-Exploitation Features		●	●
10.6	Centrally Manage Anti-Malware Software		●	●
10.7	Use Behavior-Based Anti-Malware Software		●	●
11	**Data Recovery**			
11.1	Establish and Maintain a Data Recovery Process	●	●	●
11.2	Perform Automated Backups	●	●	●
11.3	Protect Recovery Data	●	●	●
11.4	Establish and Maintain an Isolated Instance of Recovery Data	●	●	●
11.5	Test Data Recovery		●	●
12	**Network Infrastructure Management**			
12.1	Ensure Network Infrastructure is Up-to-Date	●	●	●
12.2	Establish and Maintain a Secure Network Architecture		●	●
12.3	Securely Manage Network Infrastructure		●	●
12.4	Establish and Maintain Architecture Diagram(s)		●	●
12.5	Centralize Network Authentication, Authorization, and Auditing (AAA)		●	●
12.6	Use of Secure Network Management and Communication Protocols		●	●
12.7	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure		●	●
12.8	Establish and Maintain Dedicated Computing Resources for All Administrative Work			●

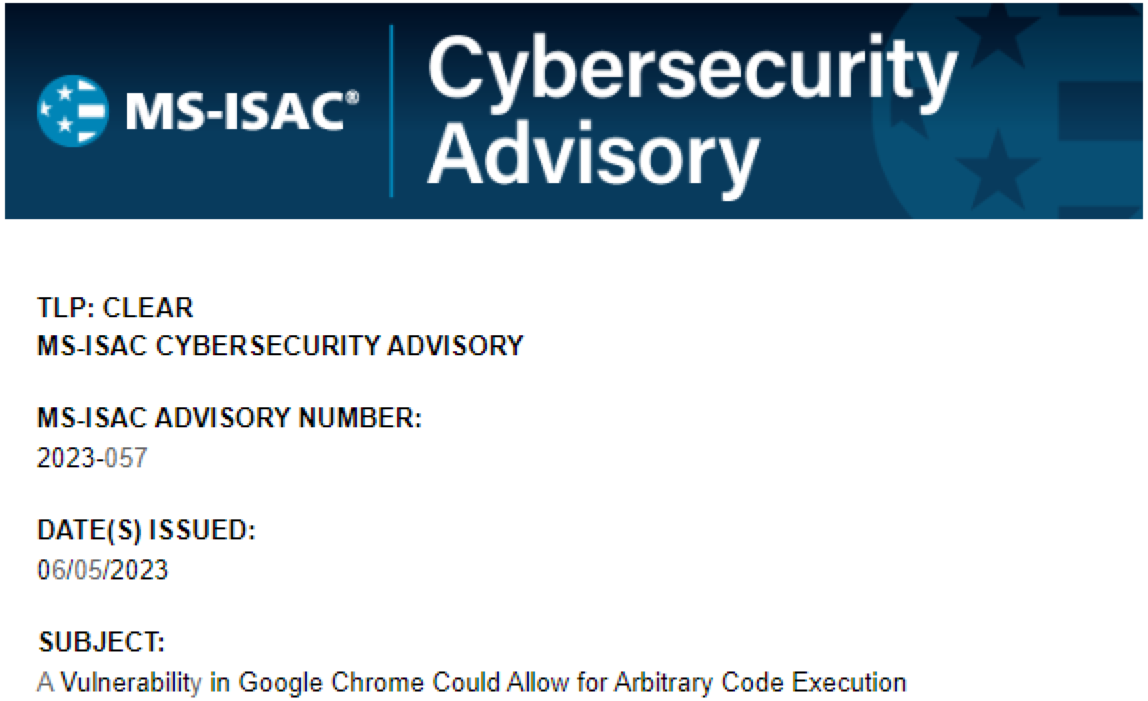
CIS Controls



Number	Control/Safeguard	IG1	IG2	IG3
13	**Network Monitoring and Defense**			
13.1	Centralize Security Event Alerting		●	●
13.2	Deploy a Host-Based Intrusion Detection Solution		●	●
13.3	Deploy a Network Intrusion Detection Solution		●	●
13.4	Perform Traffic Filtering Between Network Segments		●	●
13.5	Manage Access Control for Remote Assets		●	●
13.6	Collect Network Traffic Flow Logs		●	●
13.7	Deploy a Host-Based Intrusion Prevention Solution			●
13.8	Deploy a Network Intrusion Prevention Solution			●
13.9	Deploy Port-Level Access Control			●
13.10	Perform Application Layer Filtering			●
13.11	Tune Security Event Alerting Thresholds			●
14	**Security Awareness and Skills Training**			
14.1	Establish and Maintain a Security Awareness Program	●	●	●
14.2	Train Workforce Members to Recognize Social Engineering Attacks	●	●	●
14.3	Train Workforce Members on Authentication Best Practices	●	●	●
14.4	Train Workforce on Data Handling Best Practices	●	●	●
14.5	Train Workforce Members on Causes of Unintentional Data Exposure	●	●	●
14.6	Train Workforce Members on Recognizing and Reporting Security Incidents	●	●	●
14.7	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	●	●	●
14.8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	●	●	●
14.9	Conduct Role-Specific Security Awareness and Skills Training		●	●
15	**Service Provider Management**			
15.1	Establish and Maintain an Inventory of Service Providers	●	●	●
15.2	Establish and Maintain a Service Provider Management Policy		●	●
15.3	Classify Service Providers		●	●
15.4	Ensure Service Provider Contracts Include Security Requirements		●	●
15.5	Assess Service Providers			●
15.6	Monitor Service Providers			●
15.7	Securely Decommission Service Providers			●

Number	Control/Safeguard	IG1	IG2	IG3
16	**Application Software Security**			
16.1	Establish and Maintain a Secure Application Development Process		●	●
16.2	Establish and Maintain a Process to Accept and Address Software Vulnerabilities		●	●
16.3	Perform Root Cause Analysis on Security Vulnerabilities		●	●
16.4	Establish and Manage an Inventory of Third-Party Software Components		●	●
16.5	Use Up-to-Date and Trusted Third-Party Software Components		●	●
16.6	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities		●	●
16.7	Use Standard Hardening Configuration Templates for Application Infrastructure		●	●
16.8	Separate Production and Non-Production Systems		●	●
16.9	Train Developers in Application Security Concepts and Secure Coding		●	●
16.10	Apply Secure Design Principles in Application Architectures		●	●
16.11	Leverage Vetted Modules or Services for Application Security Components		●	●
16.12	Implement Code-Level Security Checks			●
16.13	Conduct Application Penetration Testing			●
16.14	Conduct Threat Modeling			●
17	**Incident Response Management**			
17.1	Designate Personnel to Manage Incident Handling	●	●	●
17.2	Establish and Maintain Contact Information for Reporting Security Incidents	●	●	●
17.3	Establish and Maintain an Enterprise Process for Reporting Incidents	●	●	●
17.4	Establish and Maintain an Incident Response Process		●	●
17.5	Assign Key Roles and Responsibilities		●	●
17.6	Define Mechanisms for Communicating During Incident Response		●	●
17.7	Conduct Routine Incident Response Exercises		●	●
17.8	Conduct Post-Incident Reviews		●	●
17.9	Establish and Maintain Security Incident Thresholds			●
18	**Penetration Testing**			
18.1	Establish and Maintain a Penetration Testing Program		●	●
18.2	Perform Periodic External Penetration Tests		●	●
18.3	Remediate Penetration Test Findings		●	●
18.4	Validate Security Measures			●
18.5	Perform Periodic Internal Penetration Tests			●

Applying Controls from Advisories



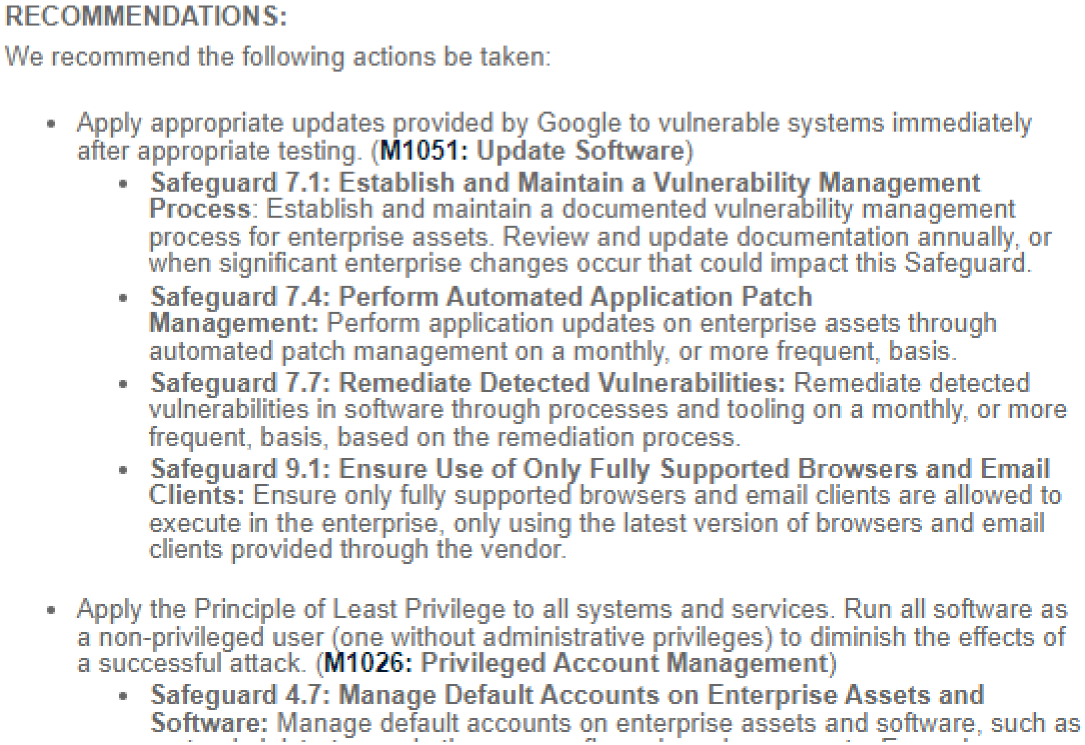
MS-ISAC® Cybersecurity Advisory

TLP: CLEAR
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2023-057

DATE(S) ISSUED:
06/05/2023

SUBJECT:
A Vulnerability in Google Chrome Could Allow for Arbitrary Code Execution



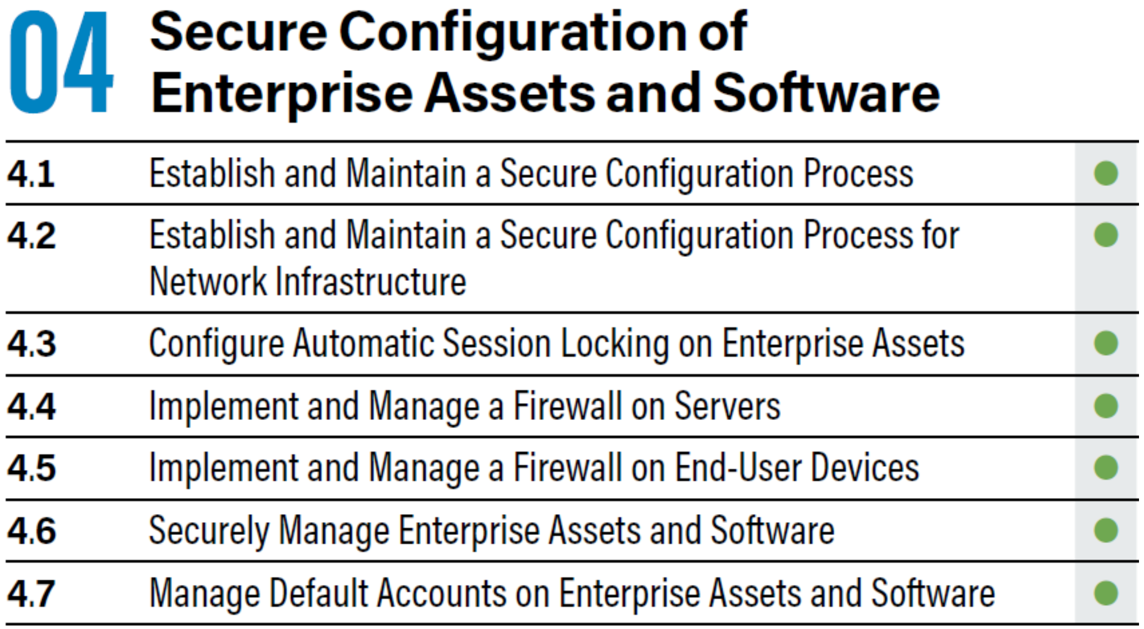
RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate updates provided by Google to vulnerable systems immediately after appropriate testing. (**M1051: Update Software**)
  - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
  - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
  - **Safeguard 7.7: Remediate Detected Vulnerabilities:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
  - **Safeguard 9.1: Ensure Use of Only Fully Supported Browsers and Email Clients:** Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.

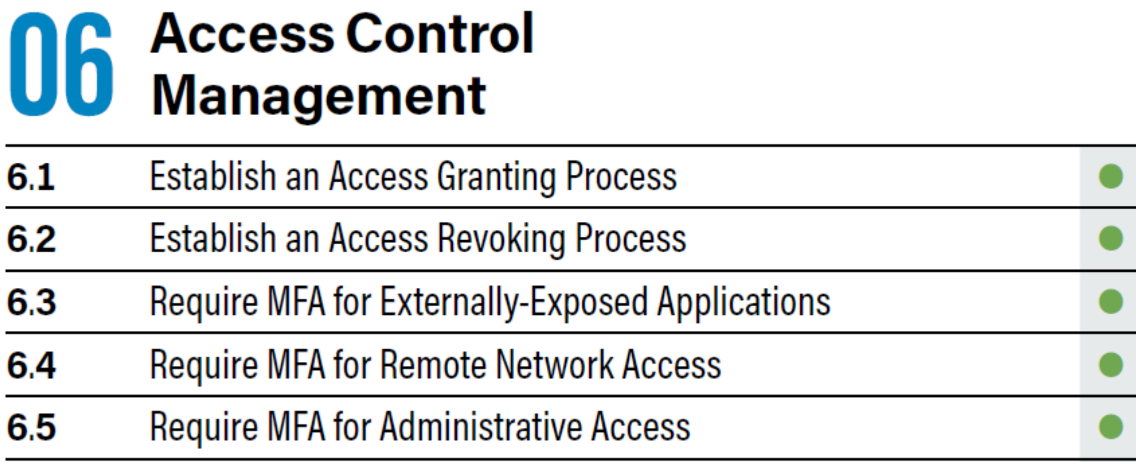
- Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. (**M1026: Privileged Account Management**)
  - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as

Applying Controls from the lessons learned



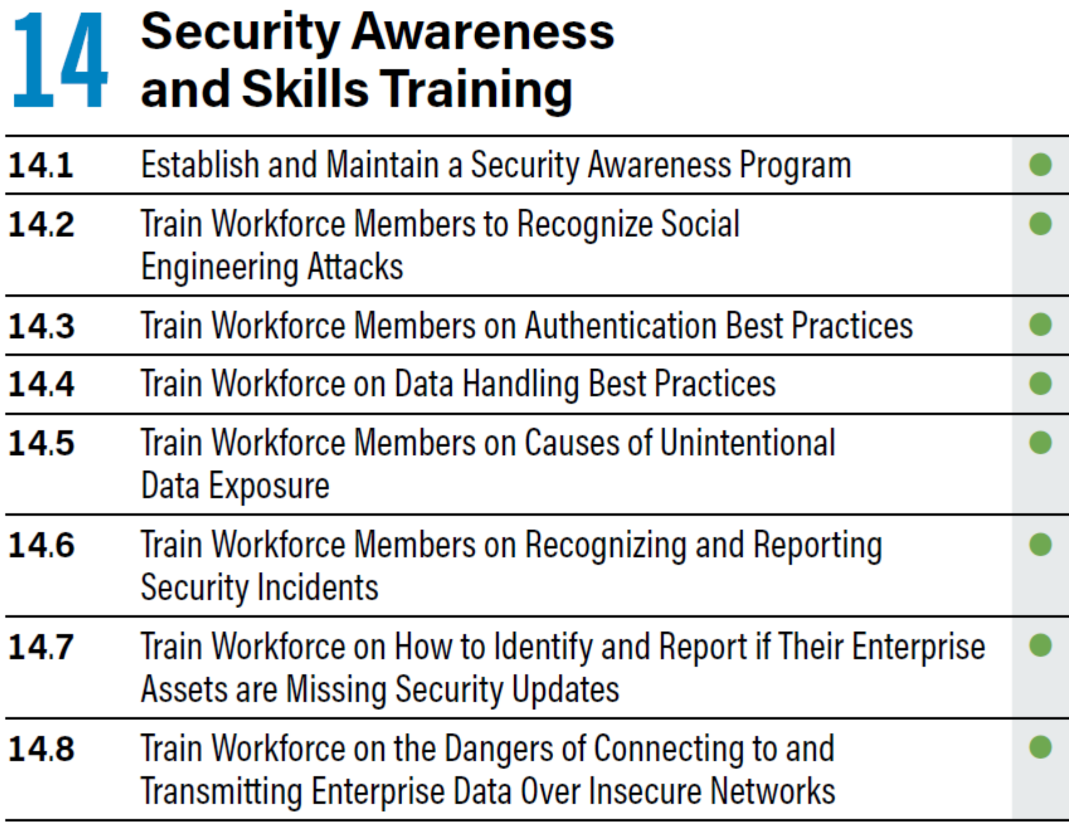
04 Secure Configuration of Enterprise Assets and Software

4.1	Establish and Maintain a Secure Configuration Process	●
4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	●
4.3	Configure Automatic Session Locking on Enterprise Assets	●
4.4	Implement and Manage a Firewall on Servers	●
4.5	Implement and Manage a Firewall on End-User Devices	●
4.6	Securely Manage Enterprise Assets and Software	●
4.7	Manage Default Accounts on Enterprise Assets and Software	●



06 Access Control Management

6.1	Establish an Access Granting Process	●
6.2	Establish an Access Revoking Process	●
6.3	Require MFA for Externally-Exposed Applications	●
6.4	Require MFA for Remote Network Access	●
6.5	Require MFA for Administrative Access	●



14 Security Awareness and Skills Training

14.1	Establish and Maintain a Security Awareness Program	●
14.2	Train Workforce Members to Recognize Social Engineering Attacks	●
14.3	Train Workforce Members on Authentication Best Practices	●
14.4	Train Workforce on Data Handling Best Practices	●
14.5	Train Workforce Members on Causes of Unintentional Data Exposure	●
14.6	Train Workforce Members on Recognizing and Reporting Security Incidents	●
14.7	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	●
14.8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	●

What services are clients engaging in?

- Cyber framework
- Cyber controls
- Incident response plans and playbooks
- Incident response control room
- Tabletop simulations
- Responding to incidents including forensics
- Incident response retainer

Thank you

Campbell McKenzie

0800 WITNESS or 021 779 310

campbell@incidentresponse.co.nz

incidentresponse.co.nz

whistleblowers.co.nz

Incident Response
FORENSIC & CYBER