The Truth About AI for Research and Education Institutions

Cyber Summit 2023 – 08 Nov 2023

cira

BACKGROUND

CIRA Cybersecurity Survey 2023

THE STRATEGIC COUNSEL

EXPERIENCE • PASSION • CREATIVITY

TORONTO | OTTAWA | CALGARY
www.thestrategiccounsel.com

cira

A REPORT TO
CIRA

PERCEPTIONS AND ATTITUDES OF CANADIAN ORGANIZATIONS TOWARD CYBERSECURITY

August 2023

BACKGROUND

CIRA Cybersecurity Survey 2023

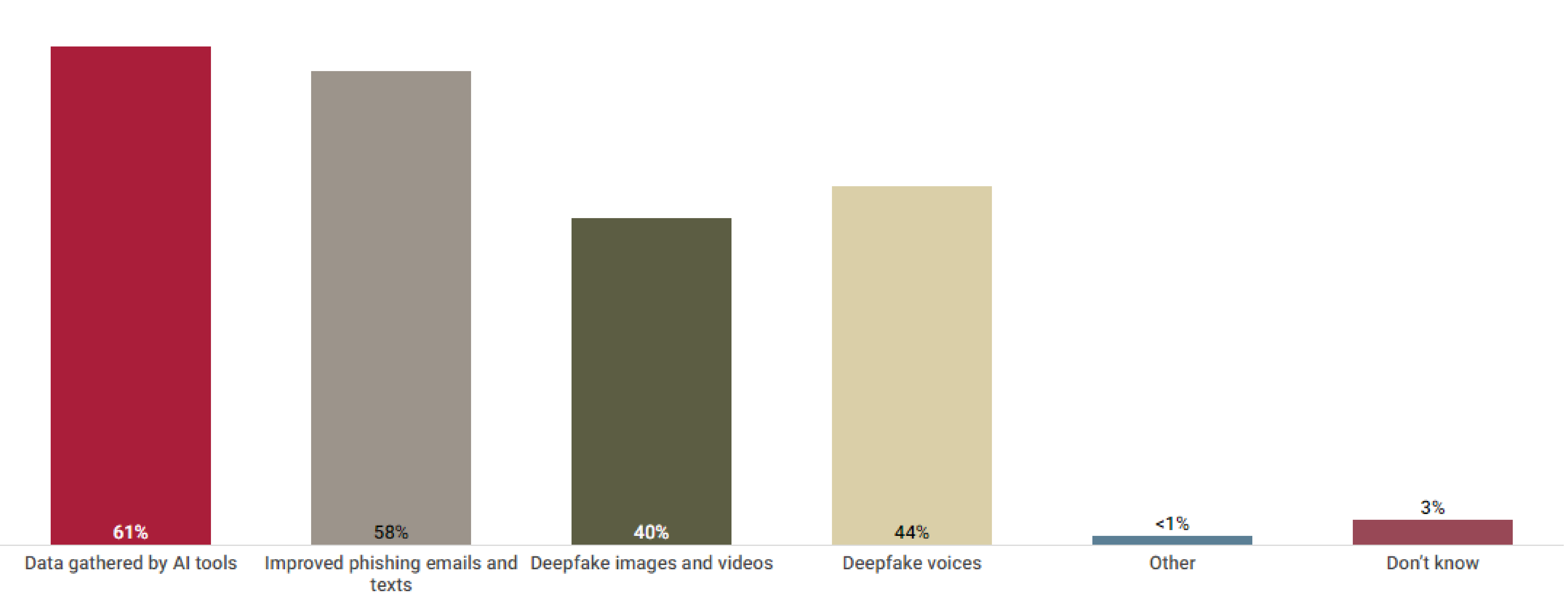
Key Findings

- 68% of organizations worried about cyber threats from generative AI, but **only 32% have an AI policy in place**.

BACKGROUND

CIRA Cybersecurity Survey 2023

Which of the following types of generative AI threats are you most concerned about?



BACKGROUND

CIRA Cybersecurity Survey 2023

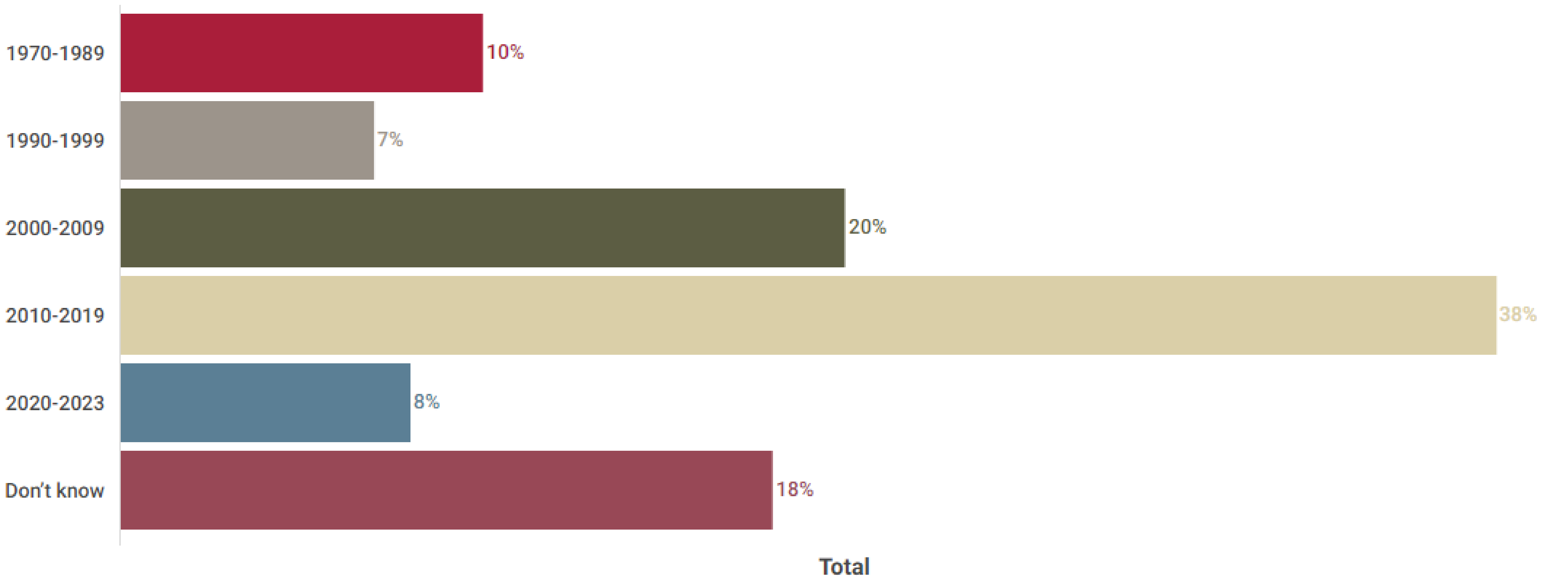
Key Findings

- 68% of organizations worried about cyber threats from generative AI, but **only 32% have an AI policy in place**.
- Among organizations affected by a ransomware attack, **70% indicated that they paid the ransom demands**. Out of those that paid the ransom, nearly one quarter (22 per cent) paid between $50K – $100K.
- **40% experienced a data breach last year** employee and/or customer (an 11 per cent increase from 2022).
- Nearly 30 per cent of organizations experienced a loss of revenue as a result of a cyber attack (up from 17 per cent in 2022), and **24% experienced damage to their reputation**.
- Organizations face cyber risks by relying on outdated technology, with **37% of firms using technology released prior to 2010**.

BACKGROUND

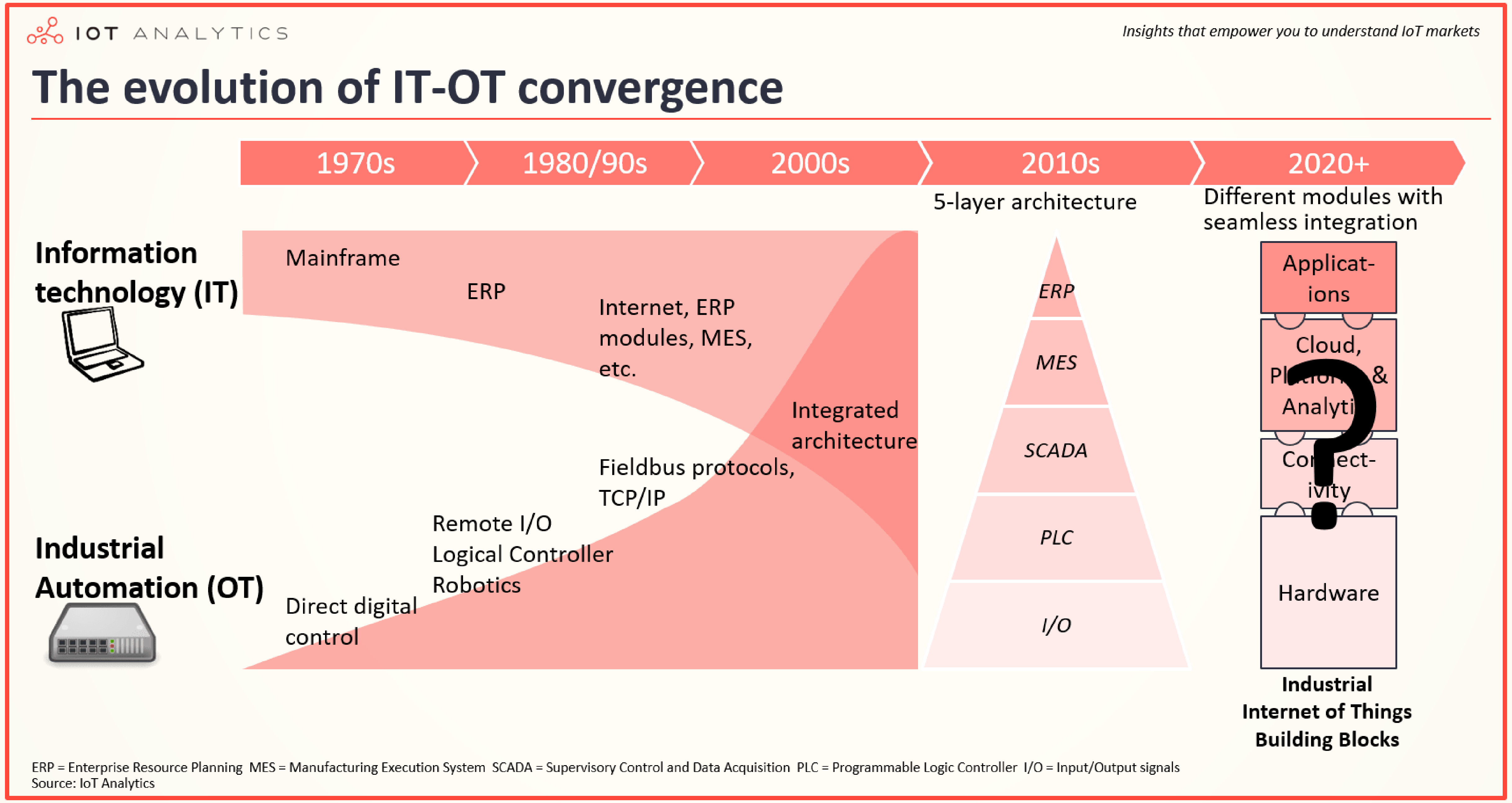
CIRA Cybersecurity Survey 2023

Over one-third are still using technology released prior to 2010.



BACKGROUND

Cyber-Physical Security



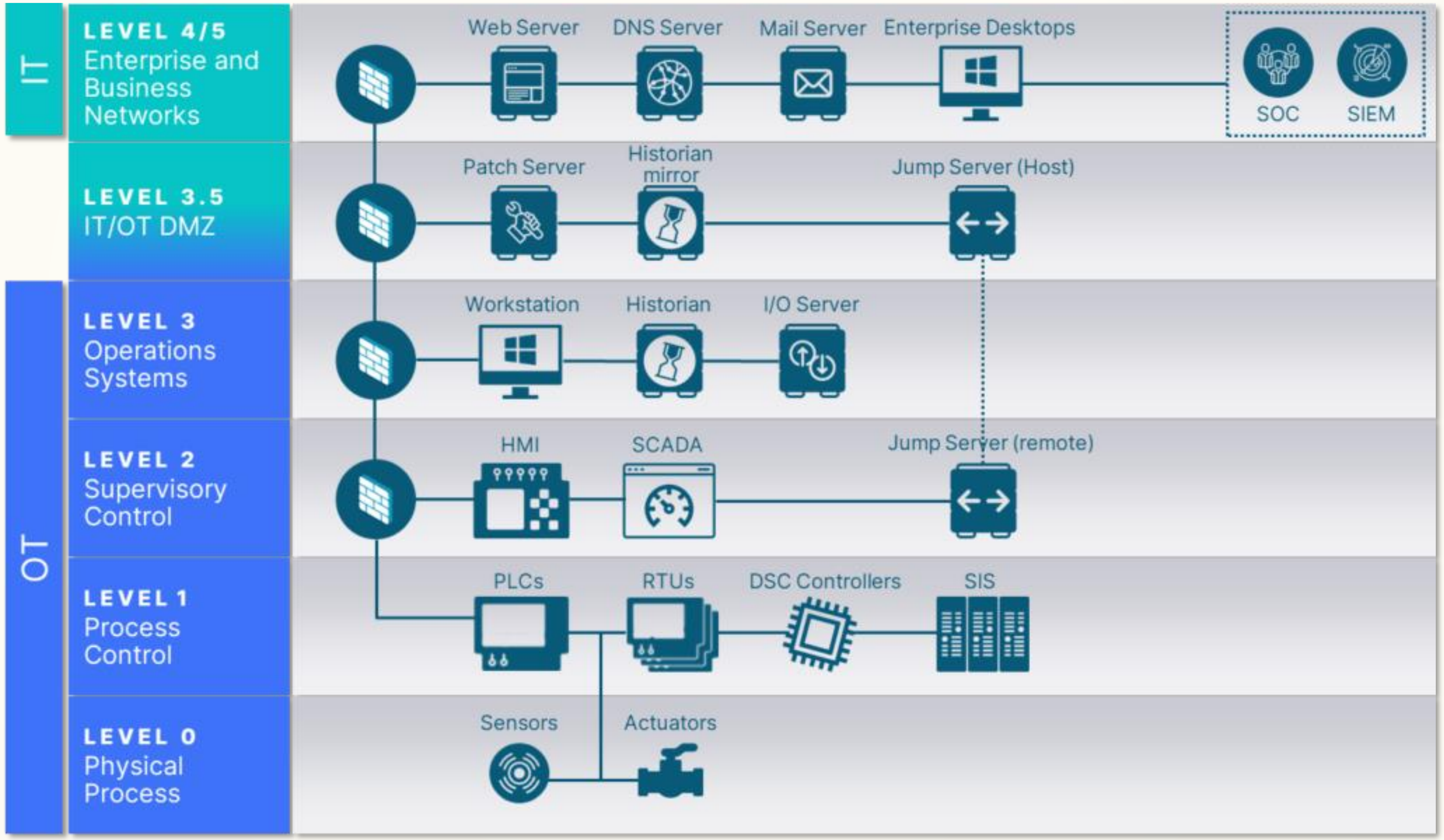
Insights that empower you to understand IoT markets

The evolution of IT-OT convergence

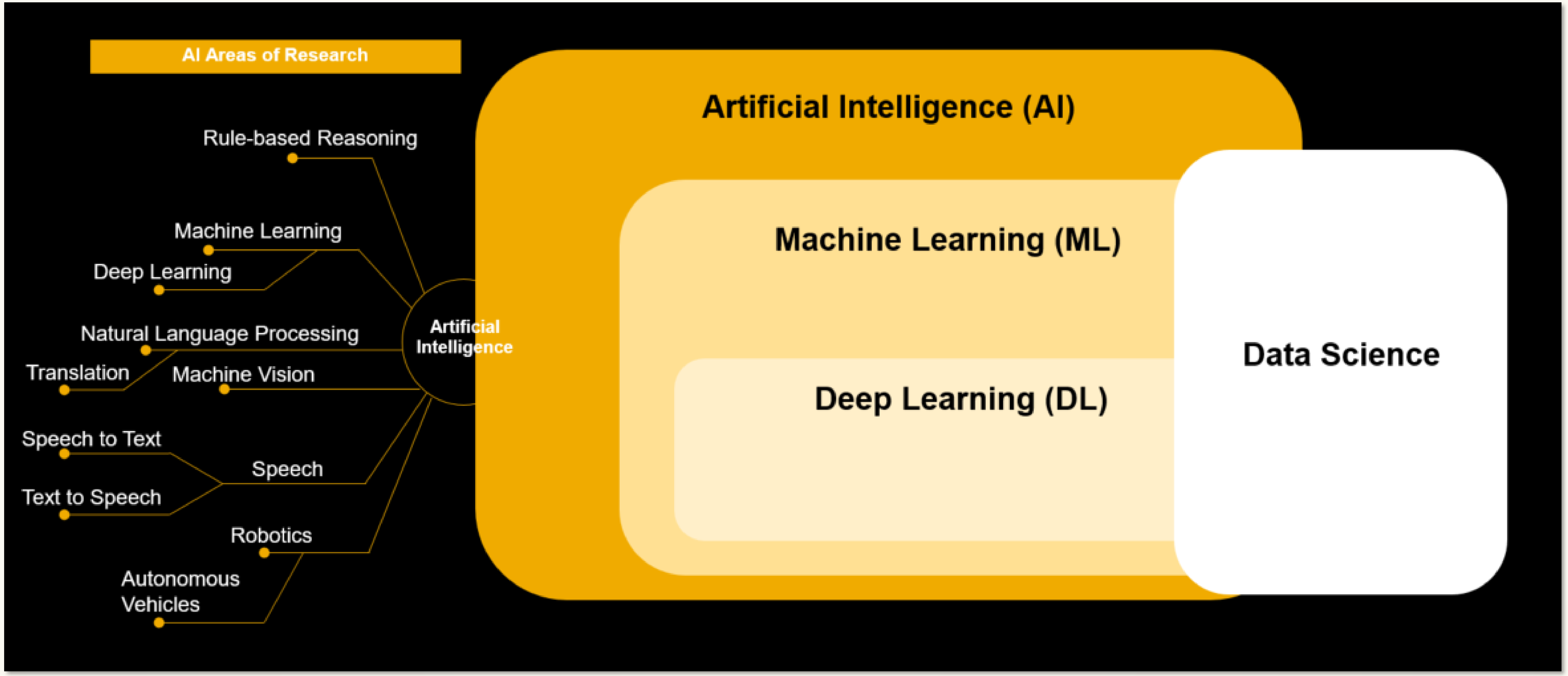
ERP = Enterprise Resource Planning MES = Manufacturing Execution System SCADA = Supervisory Control and Data Acquisition PLC = Programmable Logic Controller I/O = Input/Output signals
Source: IoT Analytics

BACKGROUND

Cyber-Physical Security – Purdue Model



AI vs. ML vs. DL


AI Areas of Research
Rule-based Reasoning
Machine Learning
Deep Learning
Natural Language Processing
Translation
Machine Vision
Speech to Text
Speech
Text to Speech
Robotics
Autonomous Vehicles
Artificial Intelligence
Artificial Intelligence (AI)
Machine Learning (ML)
Deep Learning (DL)
Data Science

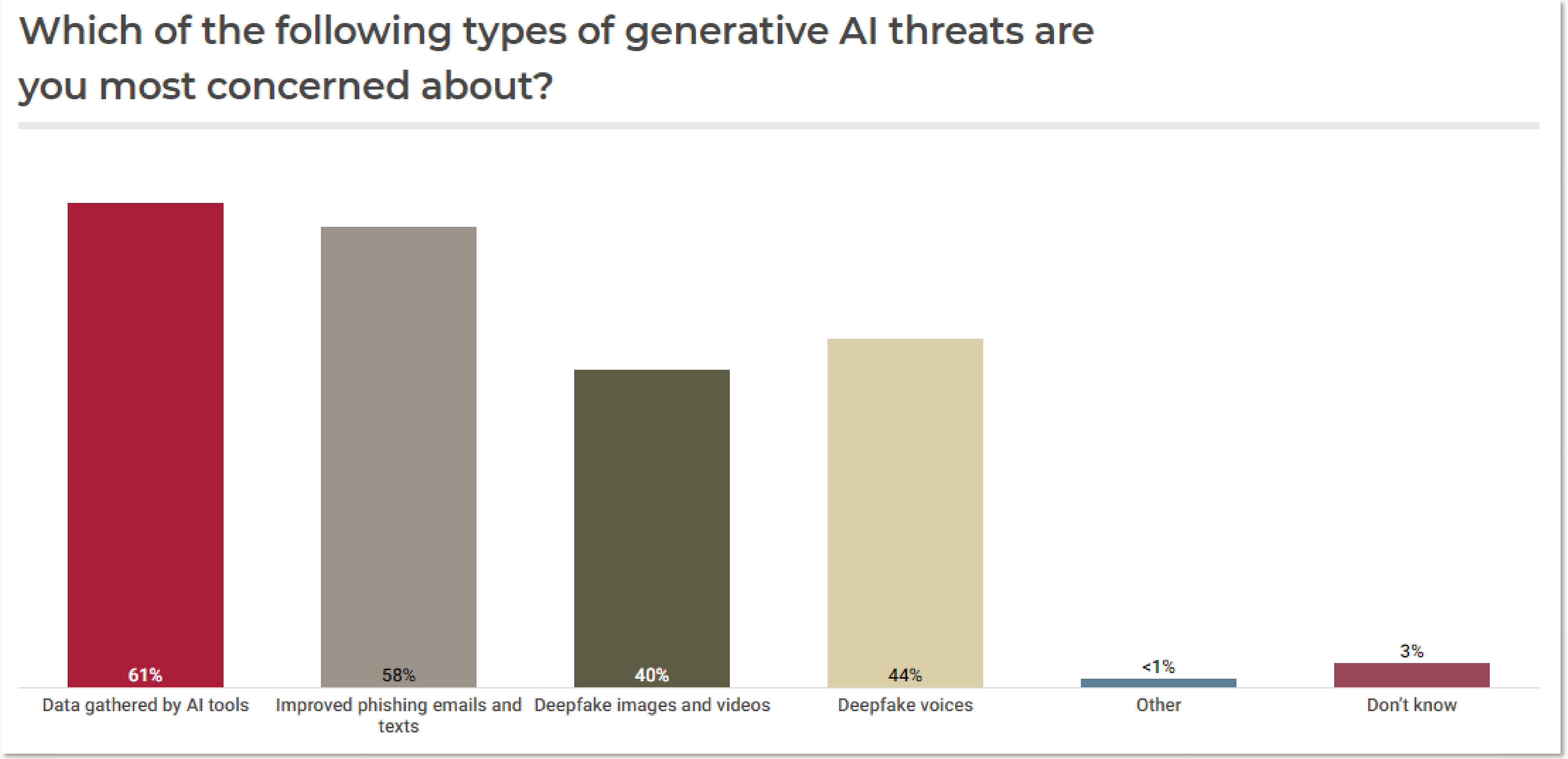
An Already Long History

Existing Benefits

- Handle billions and trillions of events (Big Data)
- Identify patterns and antipatterns / anomalies
- Automate & orchestration response

AI & CYBERSECURITY

CIRA Cybersecurity Survey 2023



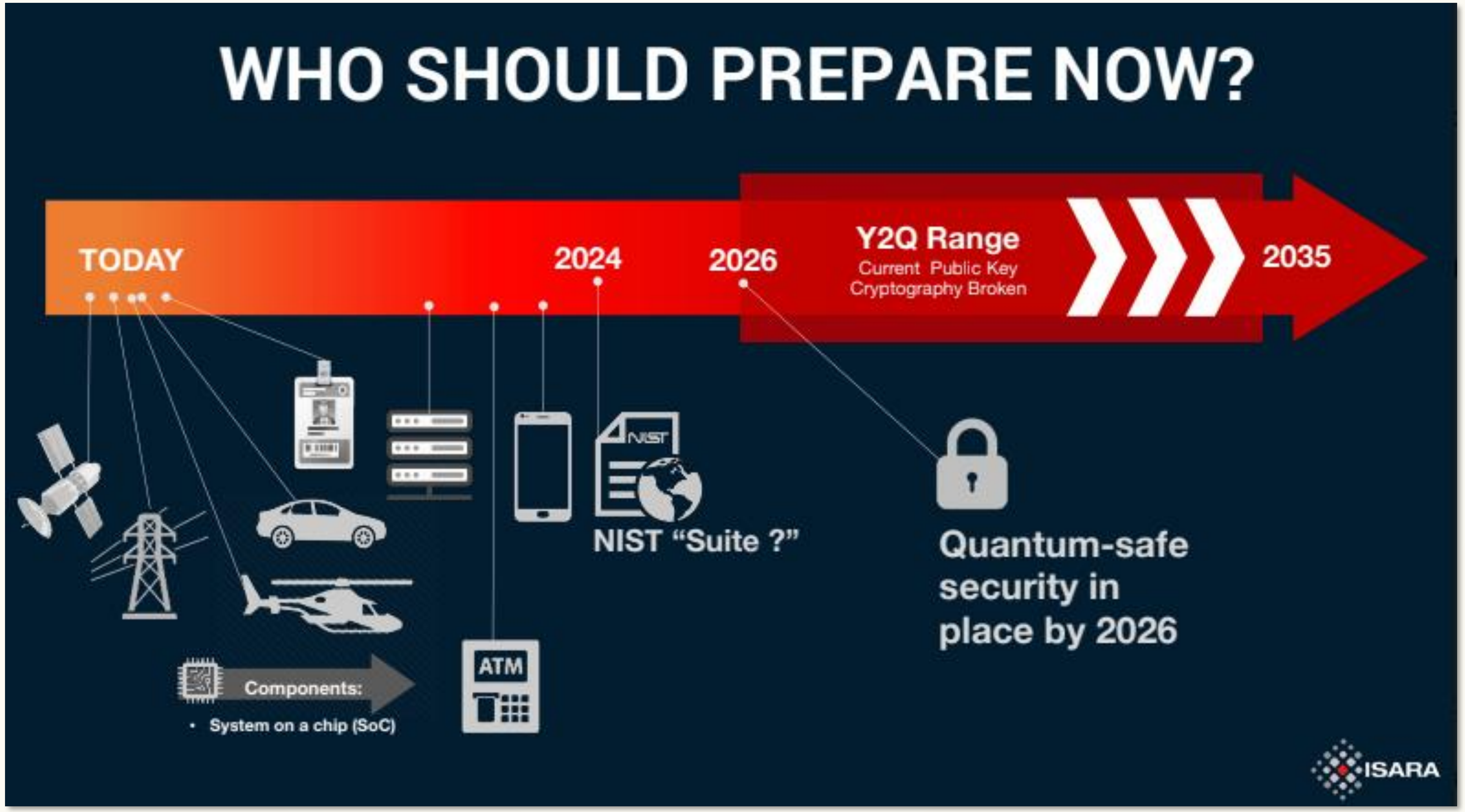
HACKING WITH CHATGPT

UNDERSTANDING CRYPTOGRAPHY

ENISA Reports on Crypto Assets and Post-Quantum Cryptography

$\hat{z} = |0\rangle$
$|\psi\rangle$
θ
ϕ
$\hat{x}$
$\hat{y}$

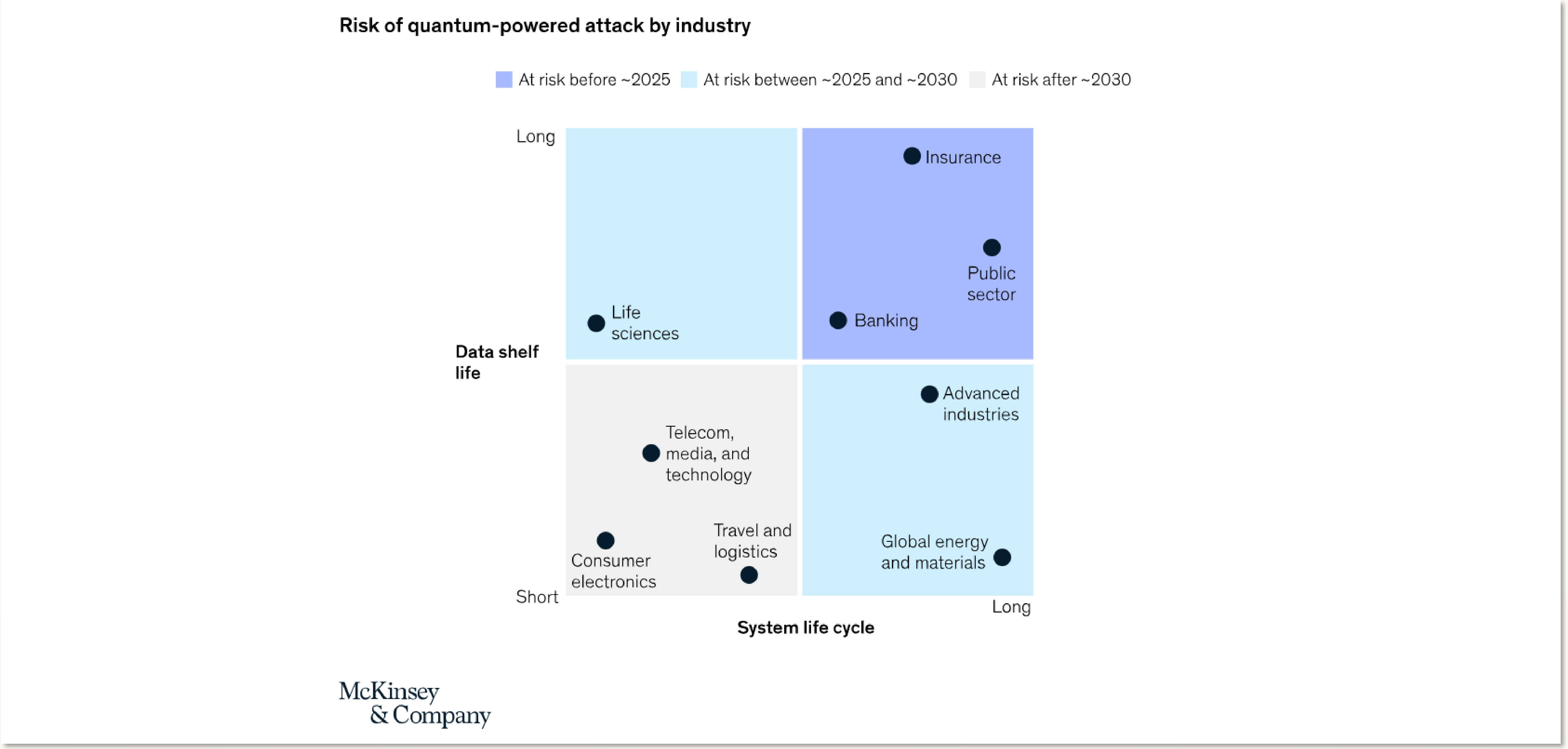
Y2Q



WHO SHOULD PREPARE NOW?

Quantum-safe security in place by 2026

Y2Q Timeline



Risk of quantum-powered attack by industry

LAWS, REGULATIONS, AND FRAMEWORKS

The Difference

CMMC + CPCSC

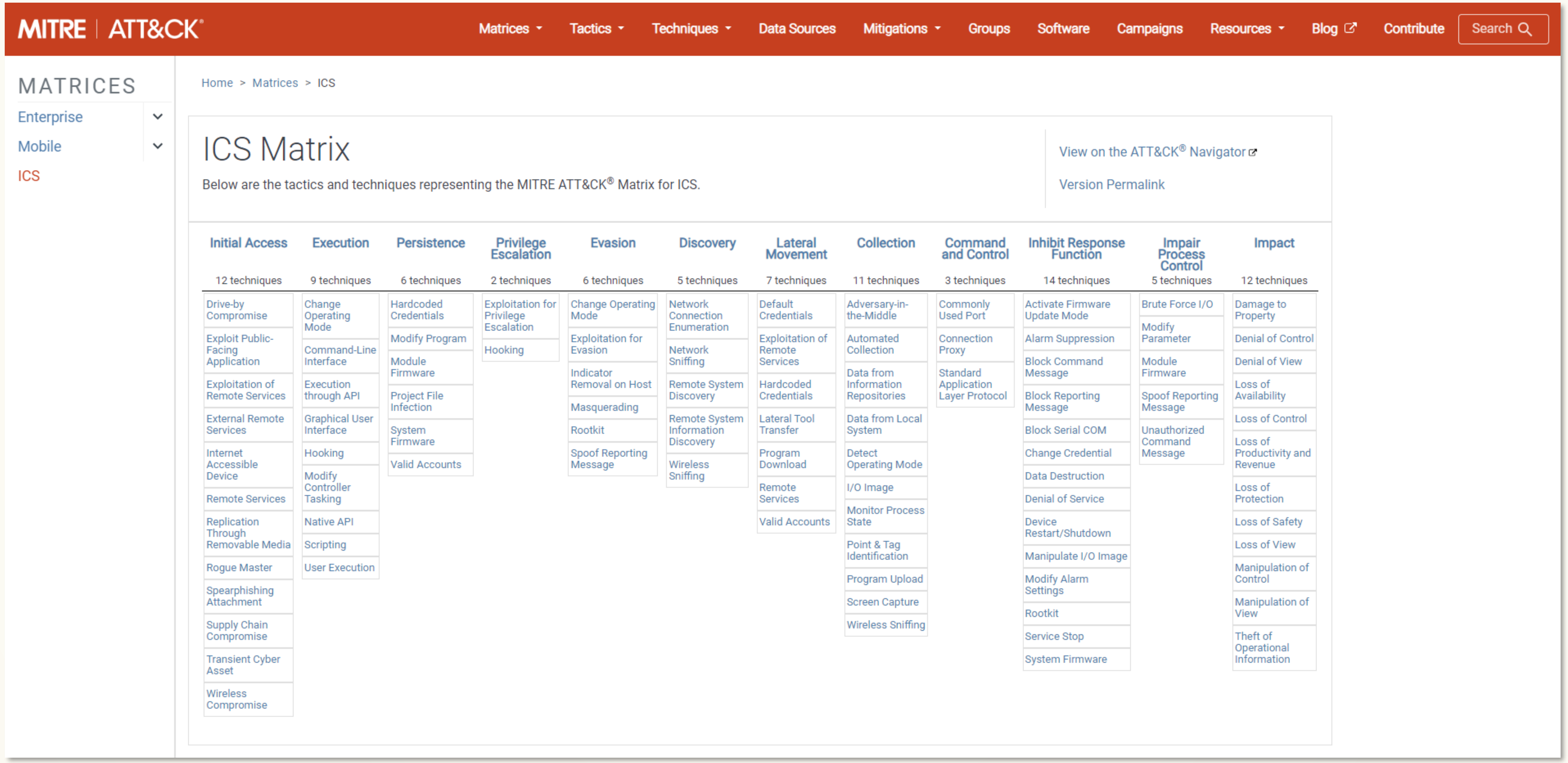
CMMC (Cyber Security Maturity Model Certification)

- US DoD framework aligned with NIST, etc.
- CMMC 2.0 now out
  - (5 levels -> 3 levels)

CPCSC (Canadian Program for Cyber Security Certification)

- Aligned with CMMC
- Mandatory for defence contracts as early as winter 2024

MITRE ATT&CK



Home > Matrices > ICS

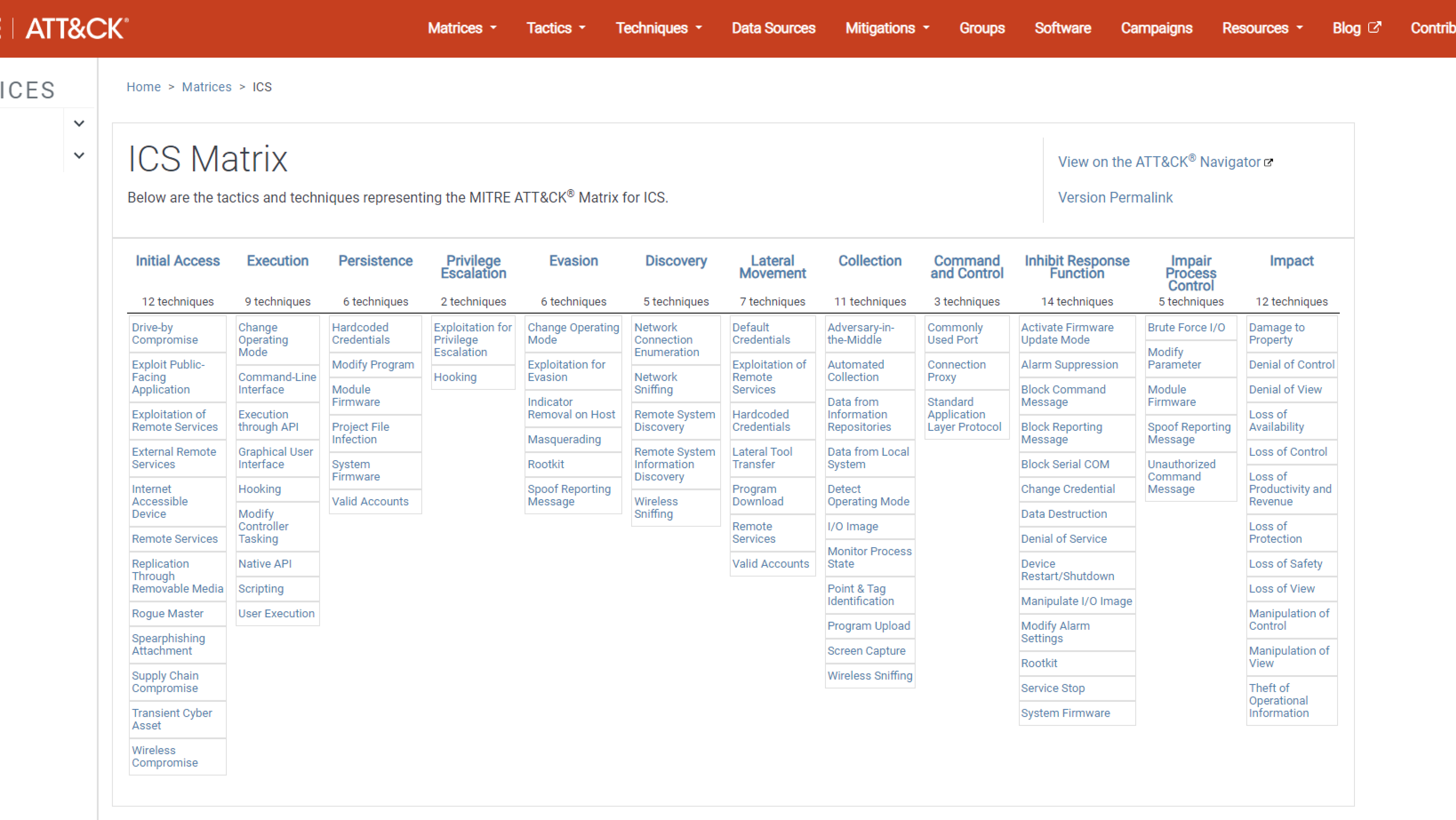
ICS Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for ICS.

View on the ATT&CK® Navigator

Version Permalink

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Scripting						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	User Execution						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise							Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		



Home > Matrices > ICS

ICS Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for ICS.

View on the ATT&CK® Navigator

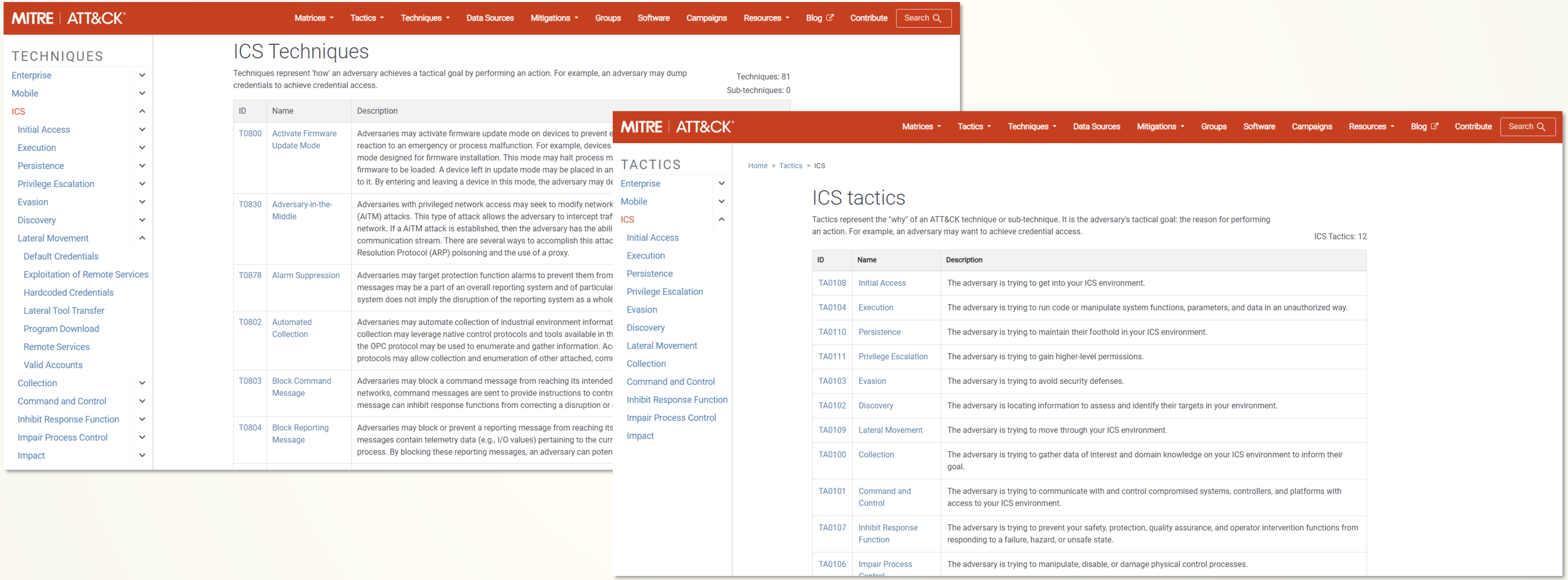
Version Permalink

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Scripting						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	User Execution						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise							Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

FACING CYBER ATTACKS

TTPs

W W W . C I R A . C A



ICS Techniques

Techniques represent 'how' an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access.

Techniques: 81
Sub-techniques: 0

ID	Name	Description
T0800	Activate Firmware Update Mode	Adversaries may activate firmware update mode on devices to prevent e reaction to an emergency or process malfunction. For example, devices mode designed for firmware installation. This mode may halt process m firmware to be loaded. A device left in update mode may be placed in an to it. By entering and leaving a device in this mode, the adversary may de
T0830	Adversary-in-the-Middle	Adversaries with privileged network access may seek to modify network (AiTM) attacks. This type of attack allows the adversary to intercept traf network. If a AiTM attack is established, then the adversary has the abili communication stream. There are several ways to accomplish this attac Resolution Protocol (ARP) poisoning and the use of a proxy.
T0878	Alarm Suppression	Adversaries may target protection function alarms to prevent them from messages may be a part of an overall reporting system and of particular system does not imply the disruption of the reporting system as a whole
T0802	Automated Collection	Adversaries may automate collection of industrial environment informat collection may leverage native control protocols and tools available in th the OPC protocol may be used to enumerate and gather information. Ac protocols may allow collection and enumeration of other attached, comr
T0803	Block Command Message	Adversaries may block a command message from reaching its intended networks, command messages are sent to provide instructions to contr message can inhibit response functions from correcting a disruption or
T0804	Block Reporting Message	Adversaries may block or prevent a reporting message from reaching its messages contain telemetry data (e.g., I/O values) pertaining to the curr process. By blocking these reporting messages, an adversary can poten

ICS tactics

Tactics represent the "why" of an ATT&CK technique or sub-technique. It is the adversary's tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access.

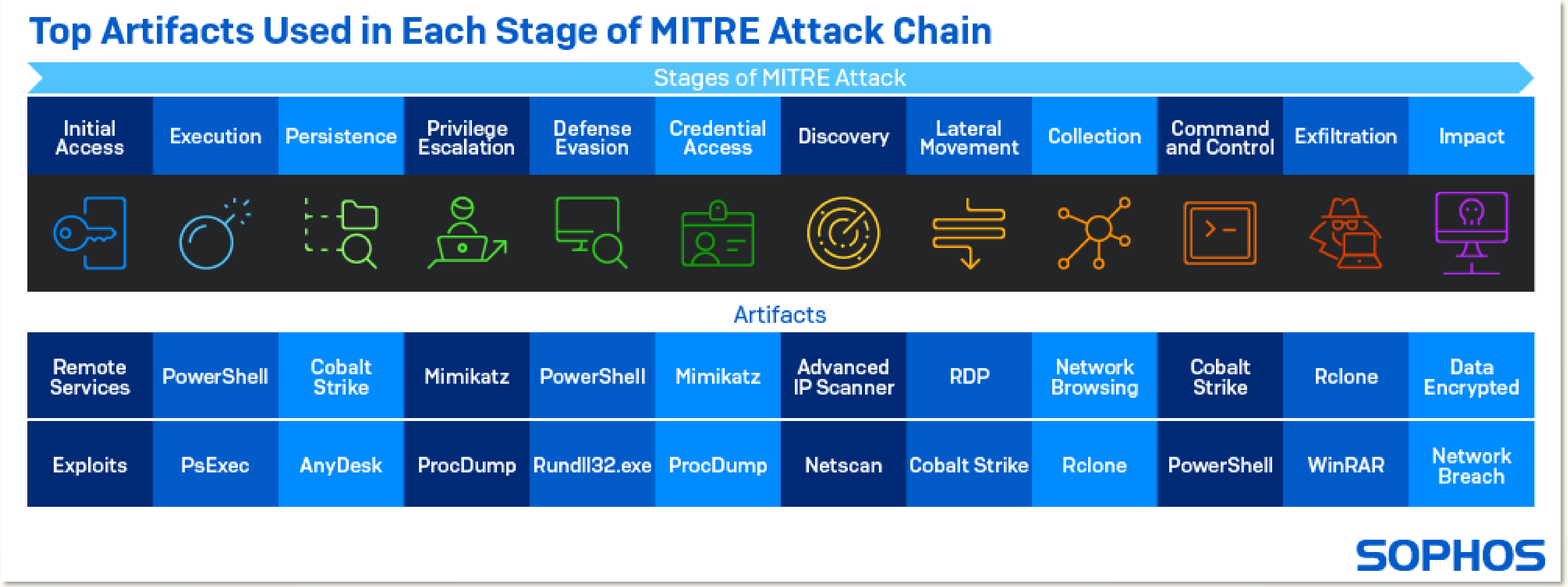
ICS Tactics: 12

ID	Name	Description
TA0108	Initial Access	The adversary is trying to get into your ICS environment.
TA0104	Execution	The adversary is trying to run code or manipulate system functions, parameters, and data in an unauthorized way.
TA0110	Persistence	The adversary is trying to maintain their foothold in your ICS environment.
TA0111	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0103	Evasion	The adversary is trying to avoid security defenses.
TA0102	Discovery	The adversary is locating information to assess and identify their targets in your environment.
TA0109	Lateral Movement	The adversary is trying to move through your ICS environment.
TA0100	Collection	The adversary is trying to gather data of interest and domain knowledge on your ICS environment to inform their goal.
TA0101	Command and Control	The adversary is trying to communicate with and control compromised systems, controllers, and platforms with access to your ICS environment.
TA0107	Inhibit Response Function	The adversary is trying to prevent your safety, protection, quality assurance, and operator intervention functions from responding to a failure, hazard, or unsafe state.
TA0106	Impair Process Control	The adversary is trying to manipulate, disable, or damage physical control processes.

cira

FACING CYBER ATTACKS

What to Look For



Top Artifacts Used in Each Stage of MITRE Attack Chain

Stages of MITRE Attack

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Remote Services	PowerShell	Cobalt Strike	Mimikatz	PowerShell	Mimikatz	Advanced IP Scanner	RDP	Network Browsing	Cobalt Strike	Rclone	Data Encrypted
Exploits	PsExec	AnyDesk	ProcDump	Rundll32.exe	ProcDump	Netscan	Cobalt Strike	Rclone	PowerShell	WinRAR	Network Breach

Artifacts

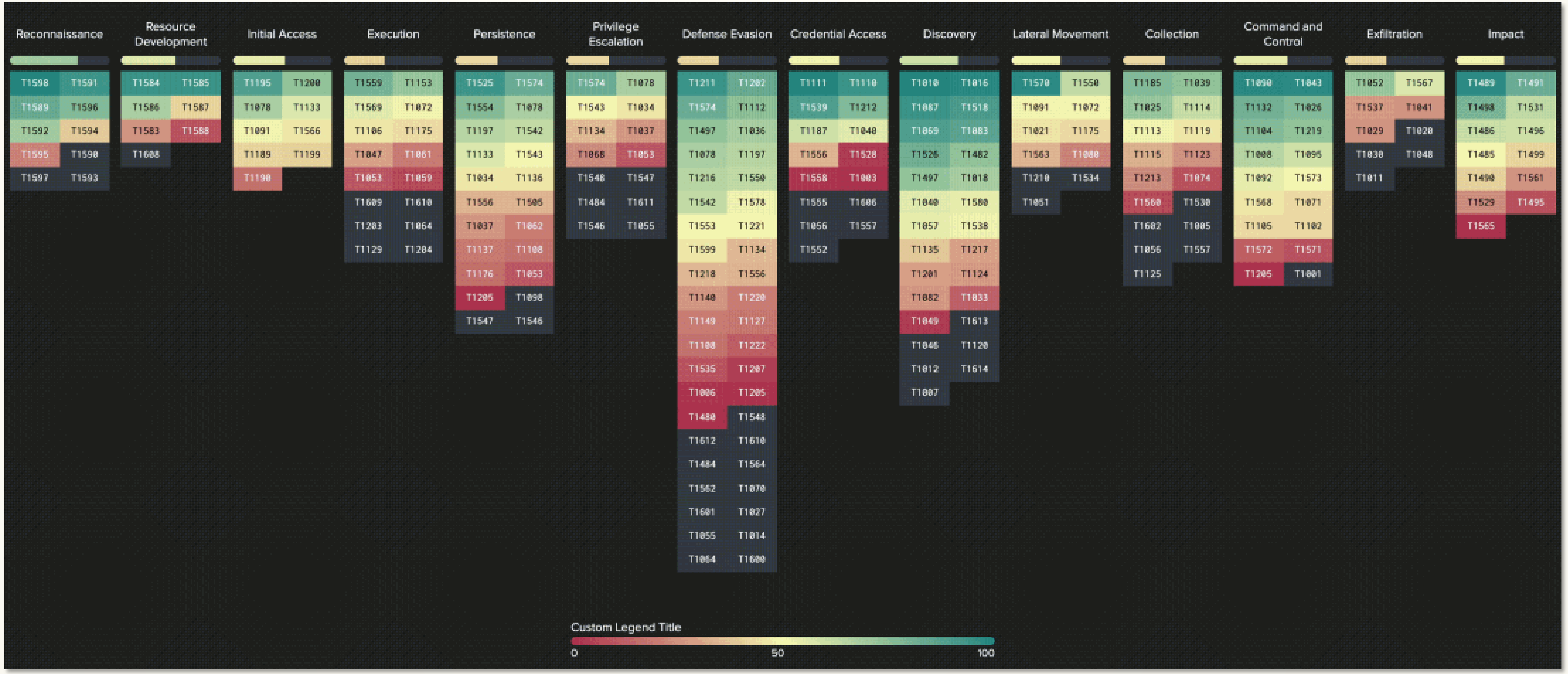
SOPHOS

W W W . C I R A . C A

cira

FACING CYBER ATTACKS

MITRE ATT&CK Heatmap



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
T1598 T1591	T1584 T1585	T1195 T1200	T1559 T1153	T1525 T1574	T1574 T1078	T1211 T1202
T1589 T1596	T1586 T1587	T1078 T1133	T1569 T1072	T1554 T1078	T1543 T1034	T1574 T1112
T1592 T1594	T1583 T1588	T1091 T1566	T1106 T1175	T1197 T1542	T1134 T1037	T1497 T1036
T1595 T1590	T1608	T1189 T1199	T1047 T1061	T1133 T1543	T1068 T1053	T1078 T1197
T1597 T1593		T1190	T1053 T1059	T1034 T1136	T1548 T1547	T1216 T1550
			T1609 T1610	T1556 T1505	T1484 T1611	T1542 T1578
			T1203 T1064	T1037 T1062	T1546 T1055	T1553 T1221
			T1129 T1204	T1137 T1108		T1599 T1134
				T1176 T1053		T1218 T1556
				T1205 T1098		T1140 T1220
				T1547 T1546		T1149 T1127
						T1108 T1222
						T1535 T1207
						T1006 T1205
						T1480 T1548
						T1612 T1610
						T1484 T1564
						T1562 T1070
						T1601 T1027
						T1055 T1014
						T1064 T1600

Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
T1111 T1110	T1010 T1016	T1570 T1550	T1185 T1039	T1090 T1043	T1052 T1567	T1489 T1491
T1539 T1212	T1087 T1518	T1091 T1072	T1025 T1114	T1132 T1026	T1537 T1041	T1498 T1531
T1187 T1040	T1069 T1083	T1021 T1175	T1113 T1119	T1104 T1219	T1029 T1020	T1486 T1496
T1556 T1528	T1526 T1482	T1563 T1080	T1115 T1123	T1008 T1095	T1030 T1048	T1485 T1499
T1558 T1003	T1497 T1018	T1210 T1534	T1213 T1074	T1092 T1573	T1011	T1490 T1561
T1555 T1606	T1040 T1580	T1051	T1560 T1530	T1568 T1071		T1529 T1495
T1056 T1557	T1057 T1538		T1602 T1005	T1105 T1102		T1565
T1552	T1135 T1217		T1056 T1557	T1572 T1571		
	T1201 T1124		T1125	T1205 T1001		
	T1082 T1033					
	T1049 T1613					
	T1046 T1120					
	T1012 T1614					
	T1007					

CONCLUSION

Don’t Panic – Do Act Now

Key Takeaways

- Non-technical impacts (IP, regulatory, and confidentiality) are equally major AI concerns.
- The impact of AI and quantum computing on cybersecurity (beyond Y2Q) gets hard to predict.
- This is the worst AI will ever be…

Q&A

THANK YOU FROM CIRA

Jamie Hari

Director of Product, Cyber/DNS

𝕏 @jamie_hari

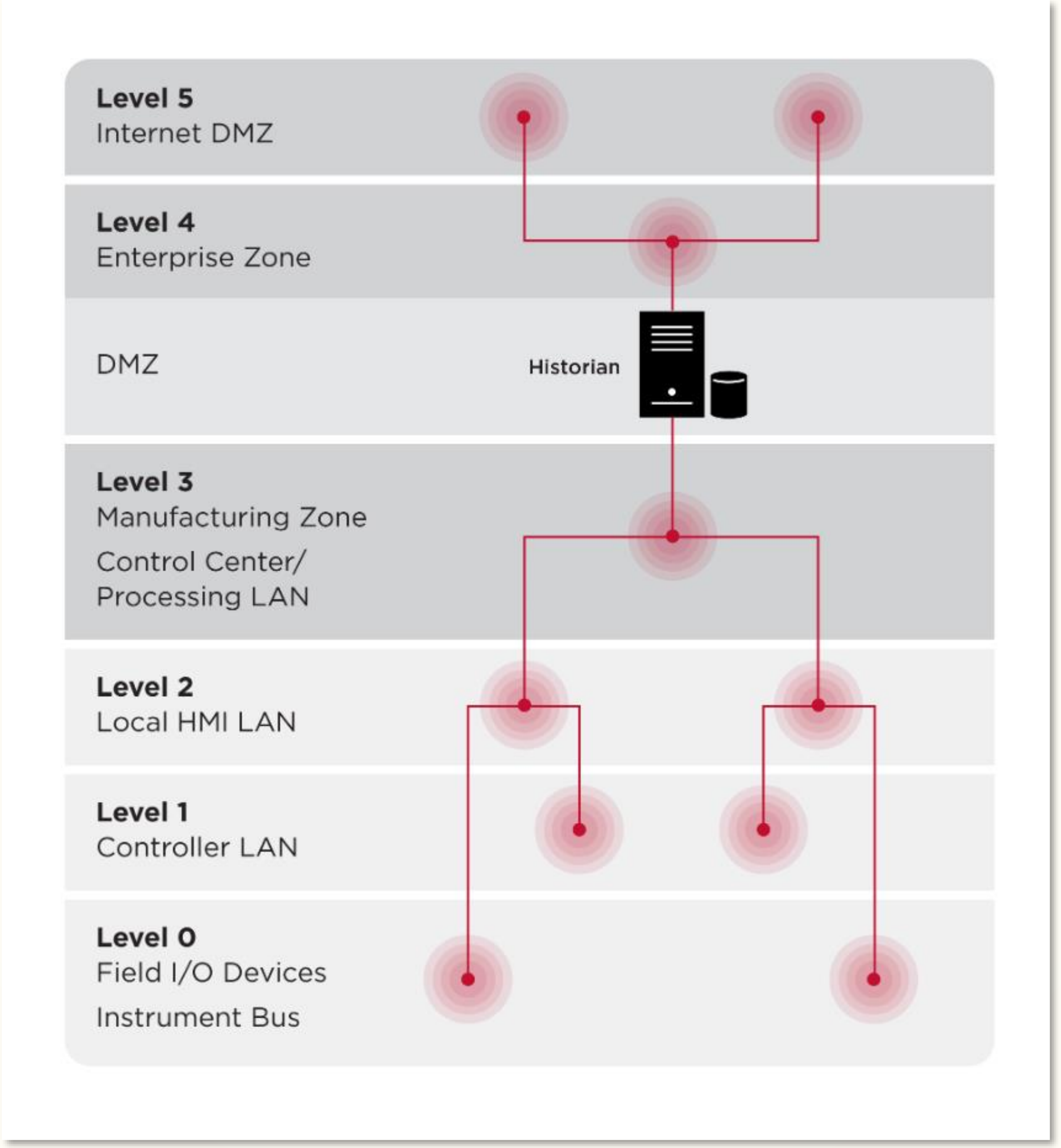
in linkedin.com/in/jamiehari

🌐 www.cira.ca

✉ info@cira.ca

CYBER-PHYSICAL SECURITY

Pivot Points


Level 5
Internet DMZ
Level 4
Enterprise Zone
DMZ
Historian
Level 3
Manufacturing Zone
Control Center/
Processing LAN
Level 2
Local HMI LAN
Level 1
Controller LAN
Level 0
Field I/O Devices
Instrument Bus