

# The New Era CISO – Fantasy Unicorn or Superhero?

## A first 120 Days Roadmap

Panagiotis Kalantzis

MScIS, CISSP, CISM, CISO, ISO27001 LA

Cyber Security & Data Privacy Expert



# Agenda

- Modern Threats & Traditional Information Security
- Expectations of a Modern CISO
- Modern CISO Life
- Tools in the Armory of the Modern CISO
- Summary

# Traditional Information Security Function

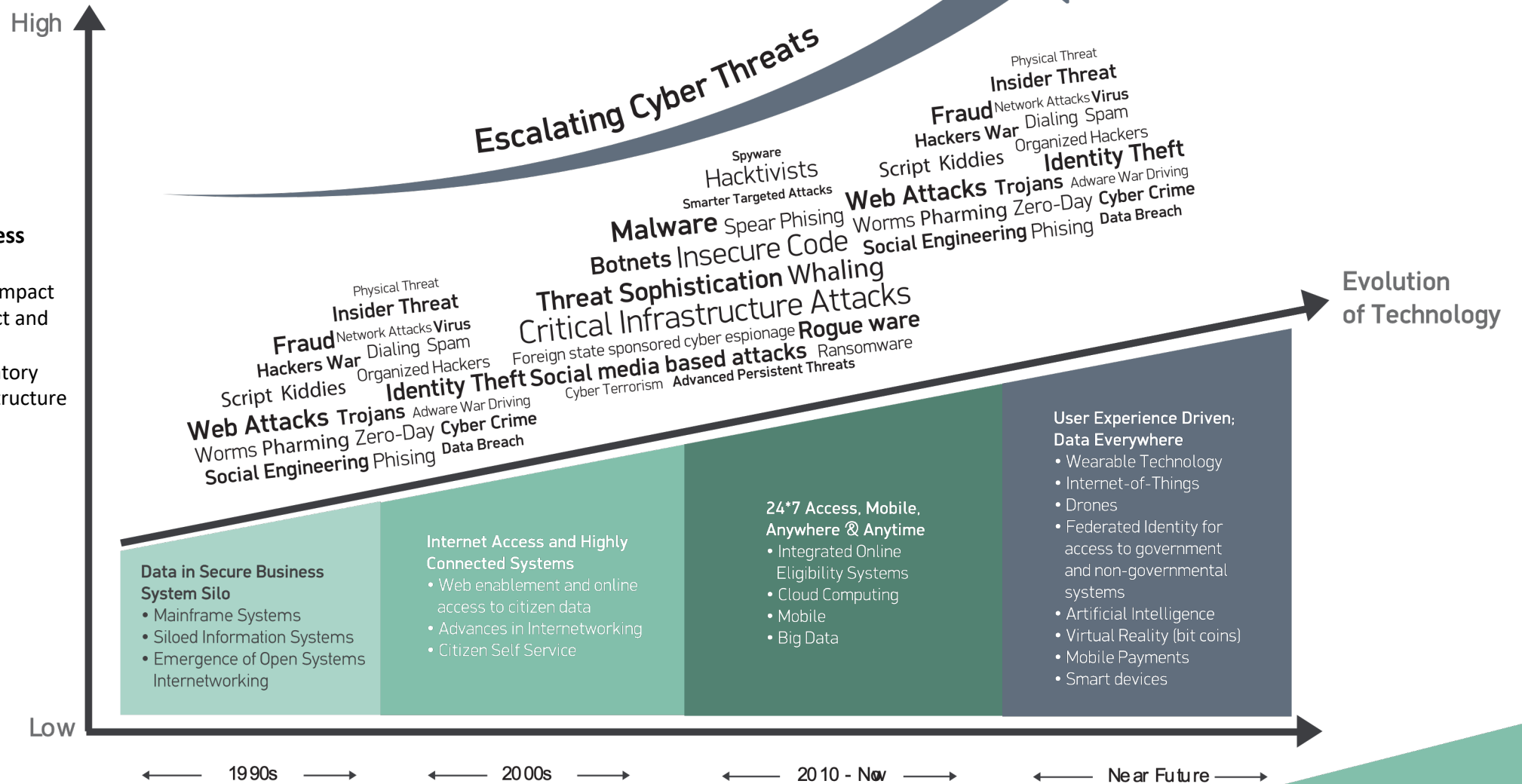


Protect – Shield – Defend - Prevent

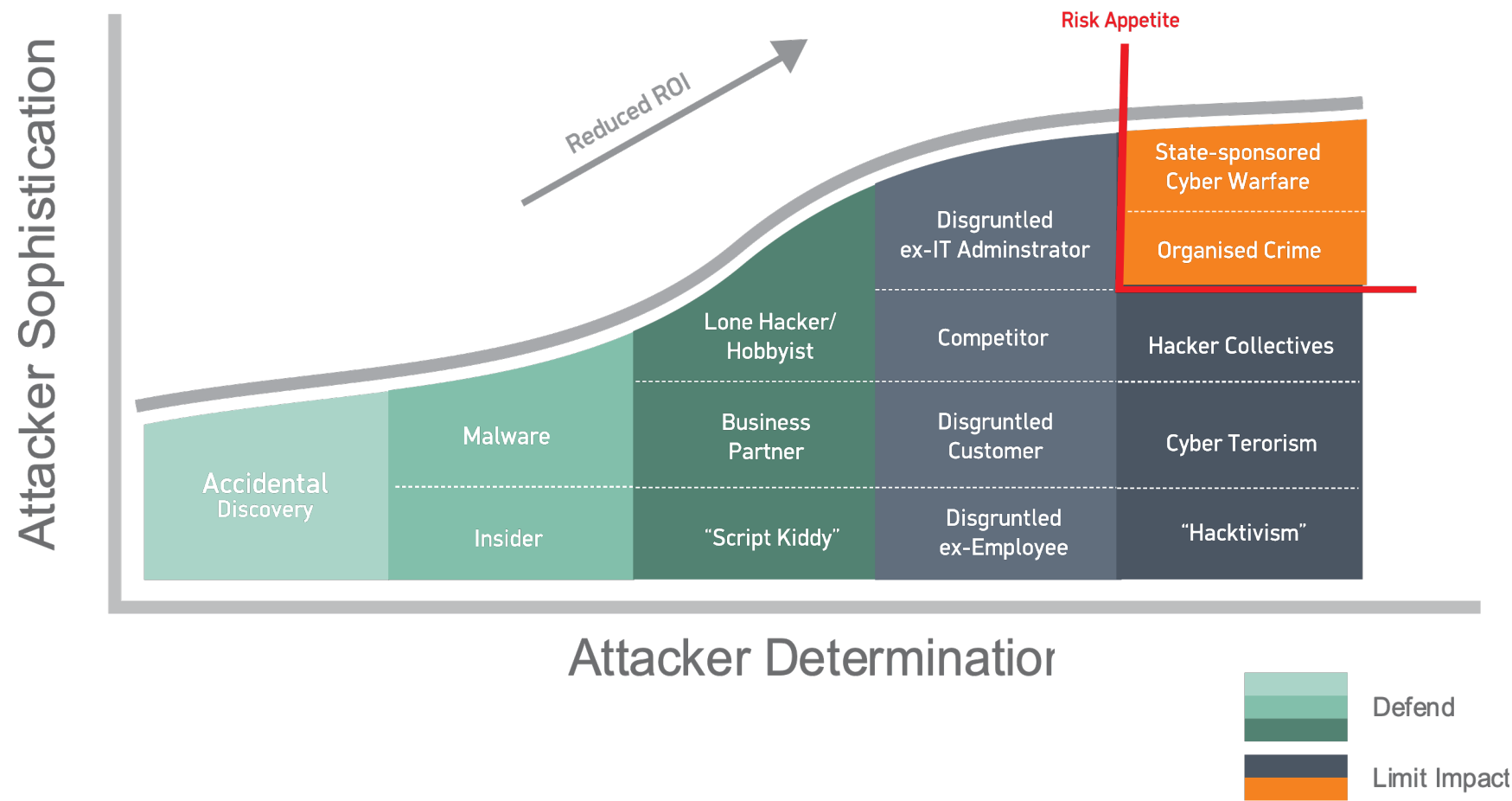
# Technology Landscape Evolution

## Increasing Business Impact

- Citizen Trust Impact
- Cost to protect and remediate
- Legal / Regulatory
- Critical Infrastructure



# Attacker Profile



# Multitude of Requirements





onelogin



Deloitte.



EQUIFAX



dailymotion

verizon



YAHOO!

Verifone



dun & bradstreet  
GROWING RELATIONSHIPS THROUGH DATA



HYATT



UBER

RICOH  
imagine. change.



# Traditional Information Security Function

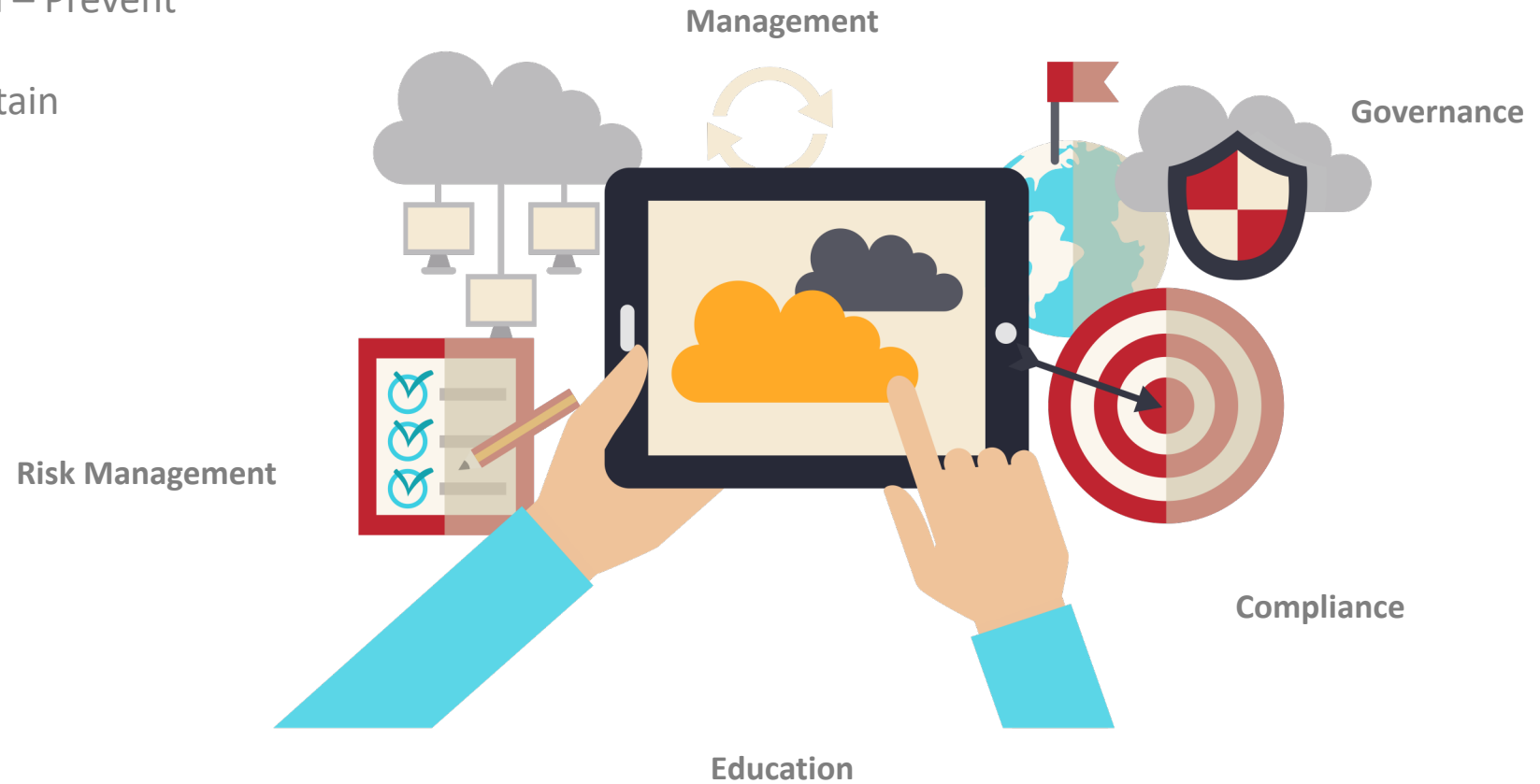


Protect – Shield – Defend - Prevent

- ✓ Is Necessary
- ✓ Is Not Sufficient
- ✓ **Fails too Frequently**

# Towards a Modern Information Security Function

1. Protect – Shield – Defend – Prevent
2. Monitor – Detect – Hunt
3. Respond – Recover – Sustain



A photograph of four business professionals in a modern boardroom. A man in a blue suit stands on the left, looking towards a woman in a white shirt and dark skirt who is standing in the center. To her right, another woman in a dark blazer and white shirt is smiling and looking towards a man in a blue suit on the far right. They are standing around a long white conference table with several green upholstered chairs. A large screen is visible in the background.

# Information Security in the Boardroom

# Modern CISO Life NOT Simple



# Modern CISO Expectations

<b>Strategic security</b>	<b>Technical security</b>
Security framework	Hardware hardening
Policy development	Incident response
Awareness campaigns (ISTAP)	Firewalls
Security procedures	Anti-virus software
Regulatory compliance	Intrusion detection and prevention
IS management systems	Vulnerability scans
Risk analysis	Penetration testing
Best practices	Data-loss prevention tools
Data privacy (GDPR)	Access control
Crisis management	System security
Organisational view	Network security
Security regardless of technology	System monitoring
Government models (Cyber Essentials)	IT disaster recovery

**Network Security**

- Network Firewall**
  - Infoblox, Cisco, Barracuda, Dell, SonicWall, Juniper
  - Microsoft Packet Engine, Untangle, StormShield, McAfee, Fortinet
  - Sangfor, Hillstone, Cato, Huawei, BlueCat
  - paloalto, WatchGuard, Check Point, Sophos
- Network Monitoring/Forensics**
  - Blue Coat, Sec, Cisco, Ixia, Dyonix
  - NetScout, Solarwinds, Gigamon, ProtectWise, Lumeta
  - Spiceworks, PacketSight, Corvil, Juniper, Utmahome
  - ForeScout, Broadband Networks, RSA, Riverbed
- Intrusion Prevention Systems**
  - IBM, Cisco, Corero, Sophos, Check Point
  - Microsoft Packet Engine, Paloalto, Fortinet, DeepNines
  - Extreme, McAfee, Huawei, FireEye
  - Juniper, NSFOCUS, Rware, AirLight
- Unified Threat Management**
  - Fortinet, Juniper, Paloalto, FireEye
  - Dell, Hillstone, Cisco, Check Point
  - Endian, Gateprotect, StormShield, Sophos
  - Huawei, Clavister, Barracuda, WatchGuard

**Endpoint Security**

**Endpoint Prevention**

**Endpoint Detection & Response**

**Endpoint Security Vendors:**

- Endpoint Prevention:** McAfee, CYCLANCE, deepinstinct, avast!, KASPERSKY, F-Secure, P Safe, Microsoft, sparkognition, ThreatTrack, AhnLab, CROWDSTRIKE, MINERVA, WEBROOT, FORTINET, Barkly, ivanti, eset, invincea, STORMSHIELD, paloalto, SAFERVPN, SentinelOne, Malwarebytes, FIXME STICK.
- Endpoint Detection & Response:** OPSWAT, ziften, SentinelOne, cyberession, CYPHORT, Zonefox, morphick, CounterTack, Fluency, TANIUM, redcanary, Hexas, Bromium, certego, TOPSECT, HEXADITE, QinetiQ, GUIDANCE, OUTLIER, CARBON BLACK, CYBERBIT, FireEye, MAUCONET, Cynet, CORE SECURITY, invincea, NEMEMIA, DTEX, RSA, LIGHTCYBER, Fidelity, CROWDSTRIKE, SECOD, DIGITAL GUARDIAN, nexthink, ENDGAME.

The diagram illustrates the relationship between three main security domains: Application Security, WAF & Application Security, and Vulnerability Assessment. Each domain is represented by a colored box with a corresponding icon. Below each domain, a list of security vendors is provided, each with its logo and name.

- Application Security** (Blue box with a shield icon):
  - AIO Networks
  - PENTA security
  - QUALYS
  - namogoo
  - ALERT LOGIC Security Compliance Cloud
  - StealthSecurity
  - Trustwave
- WAF & Application Security** (Green box with a shield icon):
  - waratek
  - PREVOTY
  - SUCURI
  - NSFOCUS
  - ZENEDGE
  - onapsis
  - SHIELD
  - Akamai
  - denyall
  - ARXAN
  - FIREBLADE
  - netsparkr
  - CERTES
  - SOHA
  - ergon
  - CITRIX
- Vulnerability Assessment** (Red box with a shield icon):
  - DBAPP Security
  - FORTINET
  - SEWORKS
  - Barracuda
  - radware
  - positive technologies
  - IMPERVA

Below these domains, a row of additional vendors is listed, each with its logo and name:

- bugcrowd
- WhiteHat SECURITY
- RAPID7
- Trustwave
- CHECKMARX
- McAfee
- FLEXERA
- BLACKDUCK
- nccgroup
- onapsis
- Hewlett Packard Enterprise
- RandomStorm
- CORE SECURITY
- VERACODE
- hackerone
- snyk
- SRCCLR
- IBM
- BeyondTrust
- Synack
- Cigital
- Outpost24
- QUALYS

Managed Security Service Provider

at&t SOLUTIONARY verizon Trustwave OPTIV ALERT LOGIC Symantec

CSC Fortinet Clone Systems Netwatch nuspire Meridian CenturyLink

IBM SecureWorks Microsoft ENTERPRISE PACKARD ENTERPRISE DATASHIELD BT ORANGE WIPRO eSentire

SAC SYSTEMS

**Risk & Compliance**

PICUS SECURITY cytegit GRX R-sam  
 RiskVISION RISKSENSE REDSEAL  
 MetricStream PREVALENT BITSIGHT  
 ATTACK61 FICO bringa tufin  
 cenna UpGuard PALADION  
 iMint SecurityScorecard FIRE M Q  
 VERODIN netwrix TEMPLAR  
 corax algosec CRONUS  
 SafeBreach RSA Archer CYENCE  
 riskrecon MEDIAPRO  
 NISPSEC NormShield Cobalt

The collage features logos for several cybersecurity vendors:

- SIEM Category:** IBM, LogRhythm, sumlogic, RSA, TIBCO, tenable network security, EventTracker, RedLock, splunk, logentries, CORRELIO, CORRELOG, SKYBOX, Logscale, panaseer, Huntsman, NetIQ, Hewlett Packard Enterprise, Trustwave, solarwinds, BLACKSTRATUS, logz.io, FORTINET, NETNASTERY, ALERT LOGIC, Fluency, and logpoint.
- Security Incident Response Category:** Phantom, radar, eLASS, DEMISTO, UPLEVEL, ayehu, serviceNow, HEXADITE, Resilient, cyberscan, Norton encode, CuckooLABS, GUIDANCE, Doss, Hexas, and Infoblox.

OPSWAT SPIRION VERA NUTO THINAIR StorageCraft  
 NETWORKS Actifile ENSIO wickr IONIC SECURITY WIRELOCK  
 globalvelocitor virtru CYPHRE PKWARE COVERTIX  
 SOMANSA VORMETRIC CIPHERCLOUD REVERSING LABS  
 BLUE TALON CENTRI SECLORE DIGITAL GUARDIAN  
 THREATQUOTIENT THREAT CONNECT  
 SURFWATCH CYBERINT  
 CAVISINT WHEEL LABS NOK NOK LABS

Mobile Security

Lookout MobileIron Skycore AppSecure wandera  
 nuro bitglass silent circle airwatch tigerconnect  
 PSAFE BLUE COAST SYSTEMS MOCANA TRUSTLOOK TESKALABS  
 appthority Snocoo! Wave Auth iVolution BETTER  
 OFFILOCKS CyberSense apt Mobility Airtight wickr  
 NowSecure COMMUNITAKE KOOLSPAN prodeco salsit  
 pindrop OPENLEAK ZIMPERIUM TeleSign

Cloud Security

ACLE SAVVINT CloudPassage Stratego illumio

**Industrial / IoT Security**

<b>MOCANA</b>	<b>cryptosoft</b> networks secured	<b>Bastille</b>
<b>utimaco</b>	<b>Rubicon</b>	<b>ICON LABS</b>
<b>IMUBIT</b>	<b>riscure</b>	<b>ZingBox</b>
<b>endian</b>	<b>IOActive</b>	<b>Cloudw@re</b>
<b>Infinion</b>	<b>SECURE AUTHORITY</b>	<b>ArtinQ</b>
<b>CYPHRE</b>	<b>PEP</b> PROTECT, ENFORCE, PREVENT	<b>CYBERBIT</b> INDUSTRIAL SOLUTIONS
<b>TEMPERED</b>	<b>CLARITY</b>	<b>WE8ROOT</b> Security for Everything
<b>ARGUS</b> CYBER SECURITY	<b>Indegy</b>	<b>Karamba Security</b>
<b>SECURITYTHINGS</b>	<b>ARM</b>	<b>BAYSHORE</b>

PALADIN SKYBOX CYBER TRIAGE SEMPLIFY RAPID7  
 CYBERBIT Swimlane Raytheon CYBERRESPONSE  
 SYNCURITY THREAT CONNECT SECDO DARK/LIGHT nuix

**Fraud Prevention / Transaction Security**

FICO UNIKEN feedzai Iovation ethoca  
 BIOCATCH IdenTrust DataSecurity EARLY WARNING FORTER  
 SIGNIFYD ThreatMetrix Guardian Analytics AU1 TITX  
 CARDINAL COMMERCIAL sift science DataSecurity socure riskified  
 Brighterion IdentityMind MAXMIND Acculynk Kount

A collage of various threat intelligence logos and company names, including iSIGHT PARTNERS, ThreatMetrix, RISKIQ, INTEL471, DOMAINTOOLS, THREATQUINTELLIGENCE, SensorCy, ANOMALI, Recorded Future, digital shadows, brandprotect, THREAT CONNECT, OpenDNS, FLASHPOINT, SIXGILL, CENTRIQ, RiskBased Security, SURFWATCH, electicIQ, CROWDSTRIKE, FISIRIGHT, serviceNow, Malware Patrol, Cyberbit, Infoblox, LOOKINGGLASS, Intsig, WEBROOT, Blueliv, 4iQ, and VERIMON.

Specialized Threat Analysis & Protection

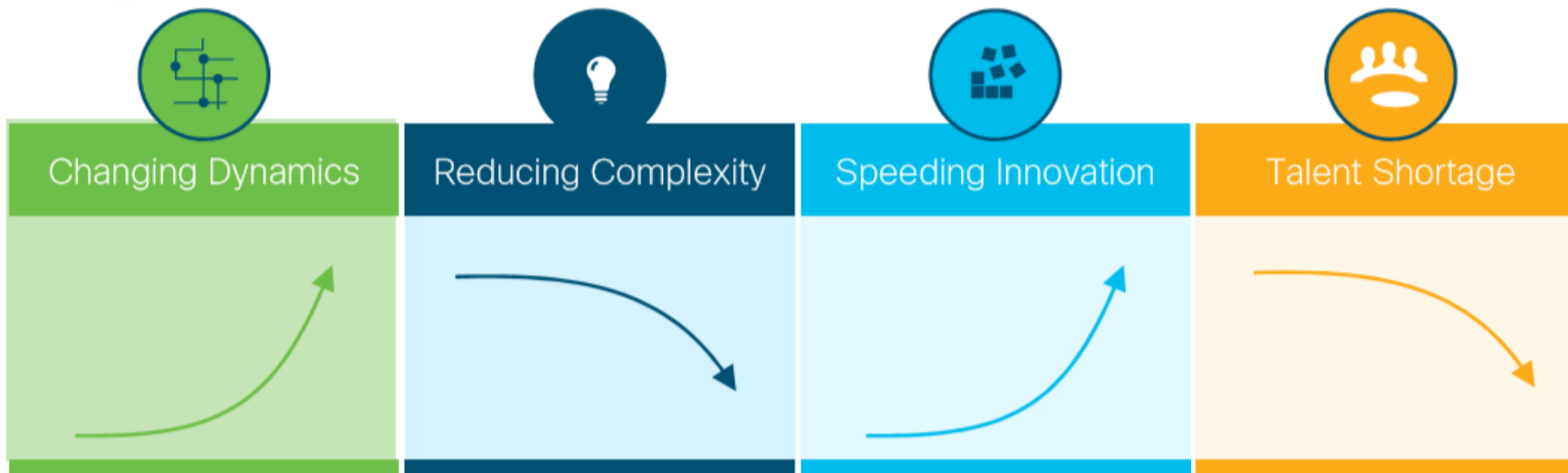
IronNet Cybersecurity | FORTSCALE | niara | Bay Dynamics | invincea | sparkcognition | TRAPX SECURITY | exabeam | ZEROFox | Invision | INTERSET | Guardico | SEC3 | observable | BehavioSec | Attivo | JASK | SSR | Mobile System | TEMPERED | MYOTRON | ABA1 | VECTRA | VENAFI | LIGHTCYBER | Palantir | sqrrl | ACALVIO | dataphy | networks | PROTECTWISE | fireglass | Symmetria | SKYPORT | lastline | Avecto | instruct | SECURONIX | REDOWL | VOTIRO | Seculert | preler | DARKTRACE | NOVETTA | datavisor | pattern8 | CYCLANCE | VIDDER | pocel | SOLEBT | Bromium | CYPHORT | SPARK | namogoo | IGNIS | esentire | illusive | Menlo Security

# Identity & Access Management

A collage of various Identity and Access Management (IAM) company logos, including Covisint, Wheel Labs, Nok Nok Labs, Oracle, Uniken, CloudWay, Okta, WISEkey, GIGYA, UnboundID, CORE SECURITY, TruLoo, SAP PASSPORT, VIRGIL ID, iPi CLEF, SailPoint, PingIdentity, IBM, SECURE KEY, FORGEROCK, INTRINSIC ID, BeyondTrust, EXOSTAR, experts, onelogin, RSA, SAVANT, BALABIT, fox technologies, BITIUM, welcome, DEVISE AUTHORITY, Auth0, AVERON, simeio, PIREAN, tascent, verato, BUE, bluebird, imprivata, Centrify, Duo Security, SaferPass, SECUREAUTH, AXIOMATICS, janrain, Avecto, iD.me, ilantus, CYBERARK, gemalto, iovation, ca, and thycotic.

SAVVYNT CloudPassage StratoSuite Illumio  
 QUALYS Threat Stack CloudLock Managed Methods  
 EnCrypted Cloud Zscaler Bitglass Evidence10  
 AVANAN Panda SOHA BRACKET  
 Vaultive VERA RedLock CODE42  
 CLOUDWAY CloudBee Covata Microsoft  
 HITRUST ORACLE palerra ARIKORP  
 guardtime FIBERLAYERS Dome3 CATO  
 Fortinet ClearDATA WhiteHat  
 skyhigh netskope VIM ARMOUR boxcryptor  
 BLUE COAT BetterCloud Trustlock CipherCloud  
 Trust in the Cloud

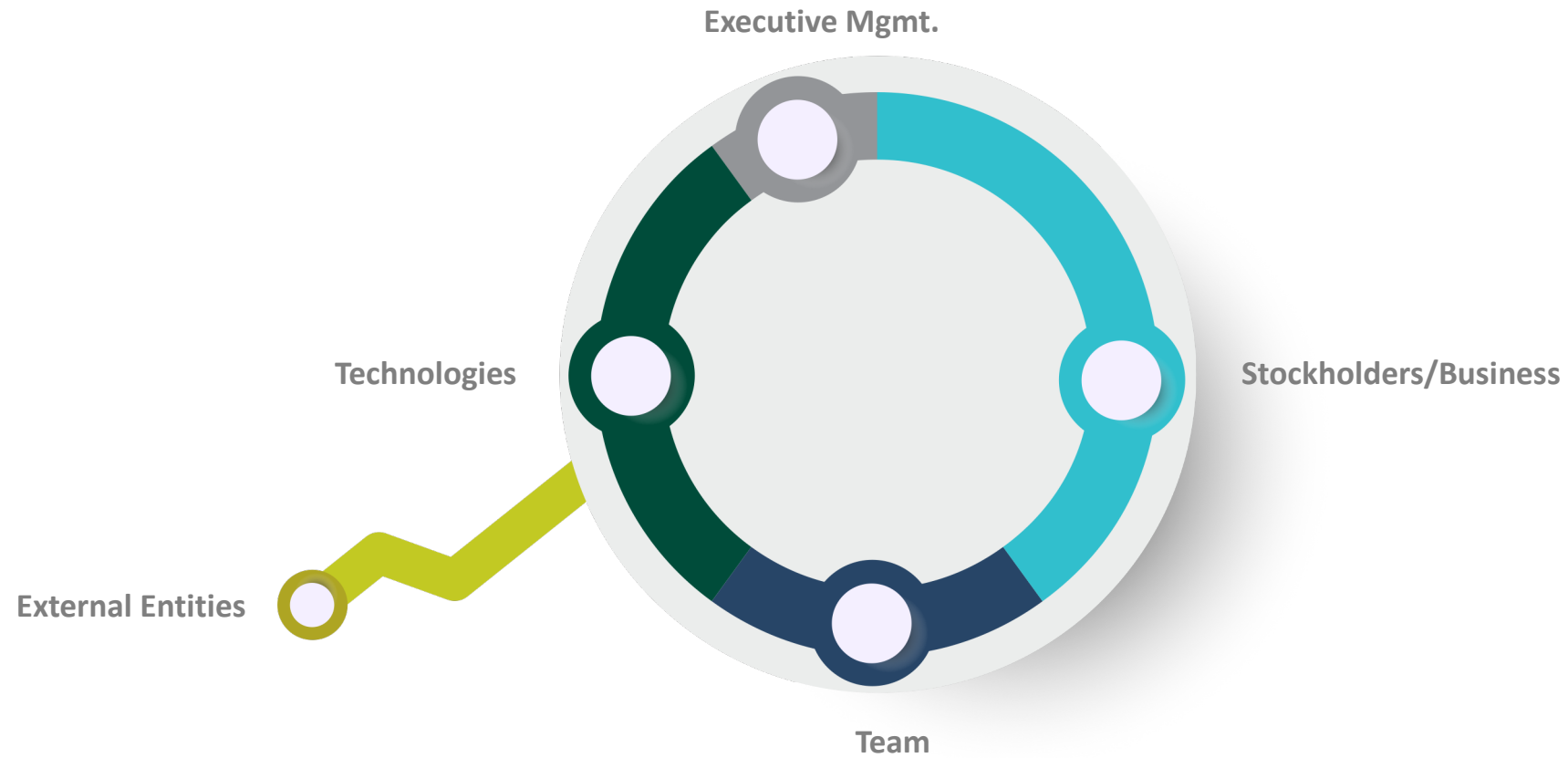
# CISO in Digital Transformation



A photograph of two white unicorns with long, flowing manes and single horns, standing in a lush, green forest. The scene is slightly misty or rainy, with water droplets visible in the air. The unicorns are facing forward, with one slightly ahead of the other. The background is a dense forest with tall trees and green foliage.

# Does Modern CISO Exist?

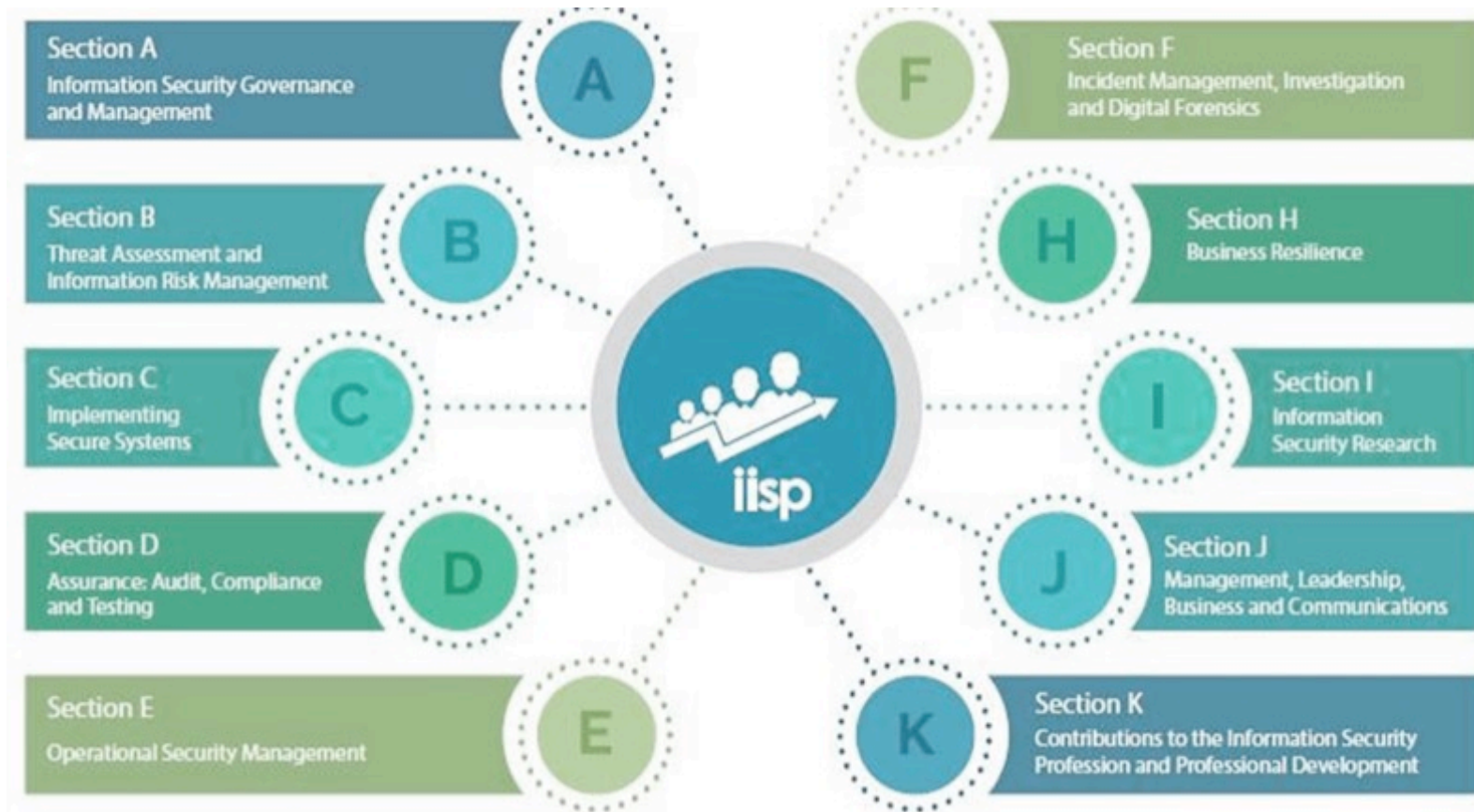
# CISO 360 Role



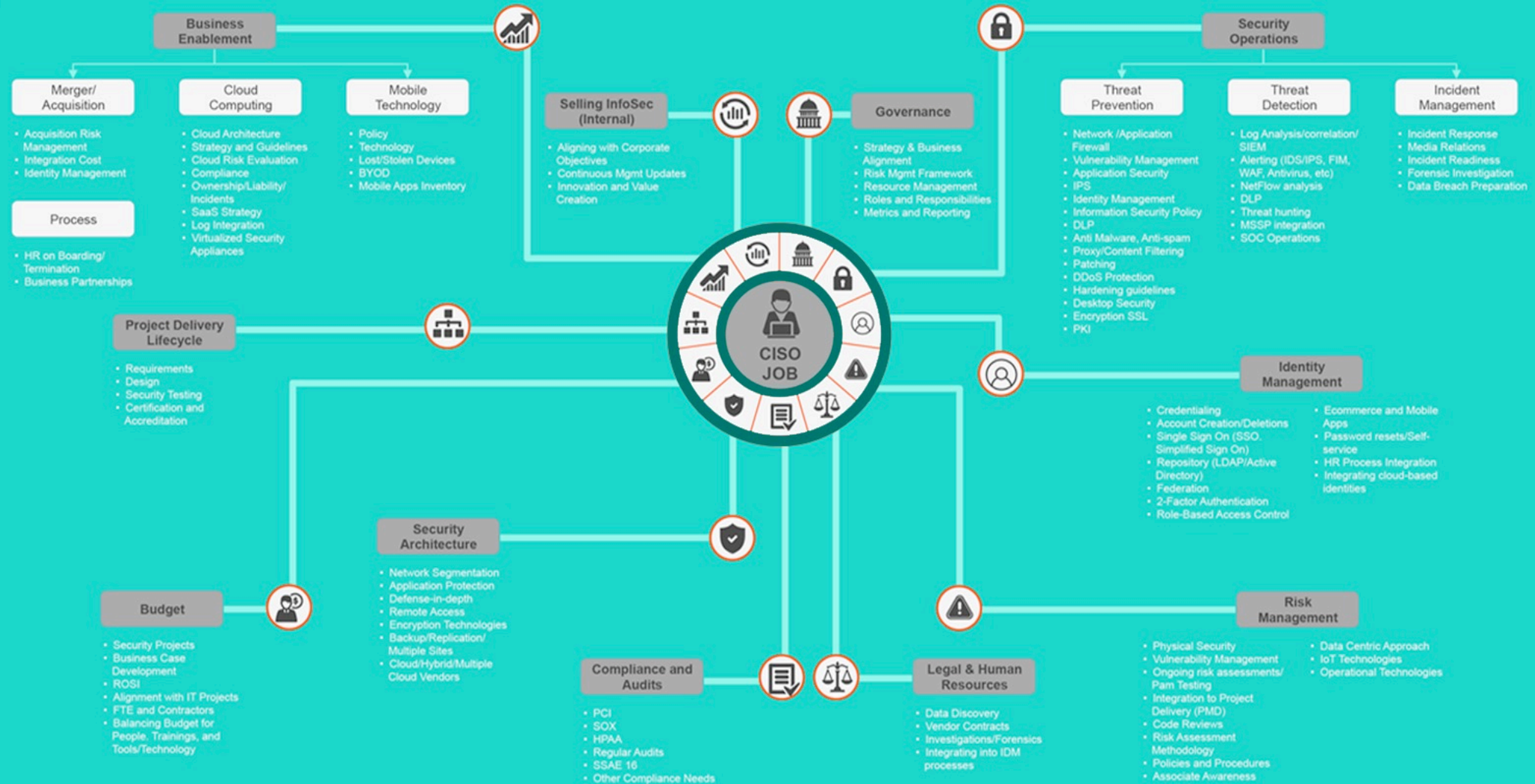
# 100 First Days of Everything



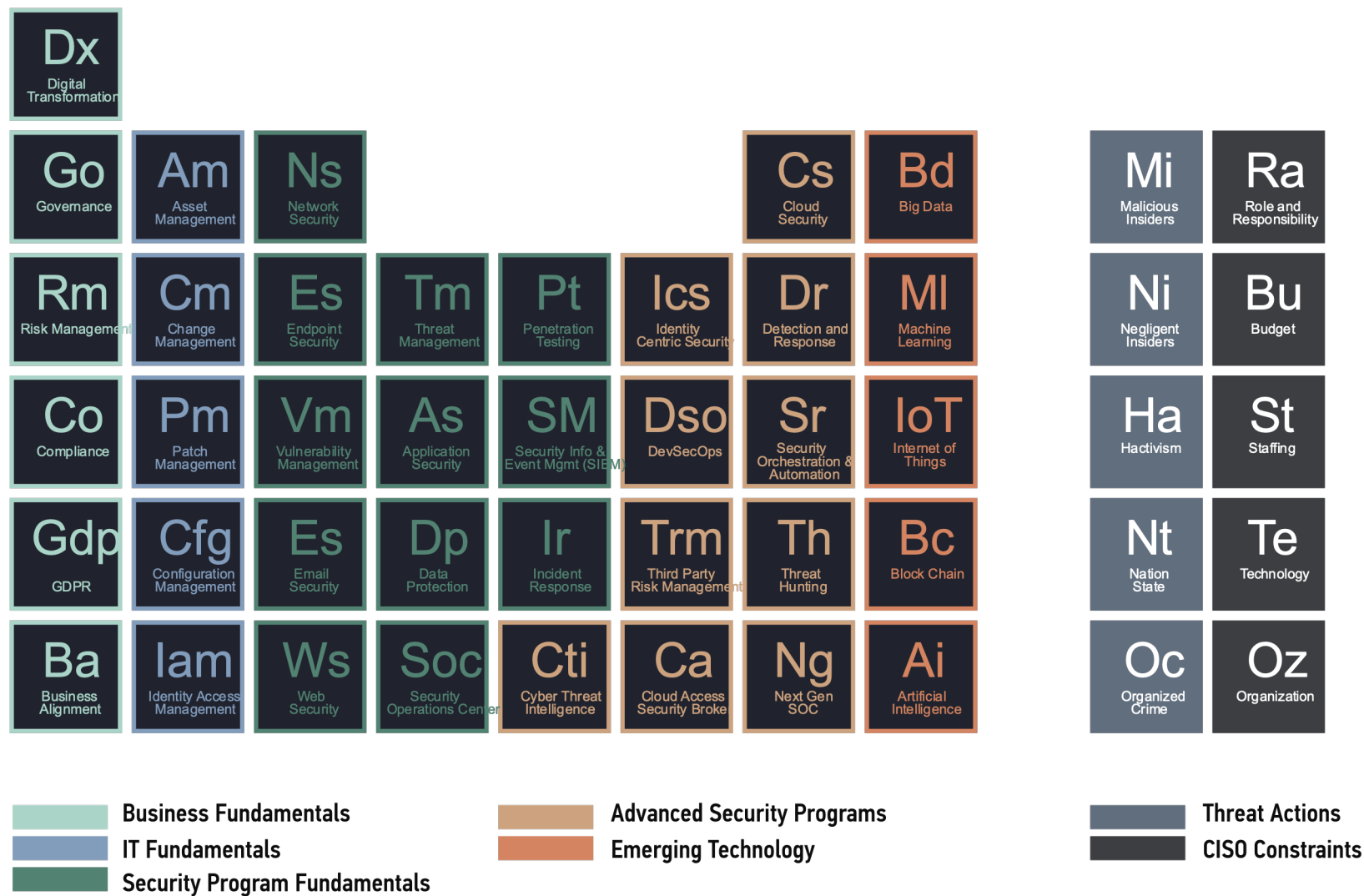
# IISP Skills Framework



# CISO Mind Map



# CISO PERIODIC TABLE



# Unique Selling Proposition

## Security can be a hard sell

- because it adds cost
- because our "clients" see our programs as adding inconvenience or cumbersome steps in business processes

## Show the real value of Information Security

- provide services that allow the enterprise to meet business risk with its eyes wide open. Its value is in managing risk
- solid evidence that your security programs are contributing to the organization's productivity, its competitiveness and ultimately its bottom line
- demonstrate a direct contribution to the revenue stream and profit margin of the company



# Executive Sponsorship



Do a quick determination  
of commitment of executives:

- **Committed or Involved?**  
Investment in resources?  
Willingness to hold people responsible?
- **Direction will be guided by the answer**

# Make it or Break it

1. Change of management
2. Breach Detection
3. Audit / New Findings
4. Mergers & Acquisitions
5. Maturity Shift
6. Large Scale project(s)
7. Tech Replacement
8. Management briefing



## **Speak the language of business**

1. Risk
2. Revenue
3. Employee efficiency
4. Strategic value
5. Cost
6. Customer satisfaction

A silhouette of a person stands on the edge of a dark, jagged cliff. The person is reaching their right arm up towards a large, bright sun or moon that is partially obscured by the text. The sky is a warm, orange-yellow color with some wispy clouds. The overall scene conveys a sense of achievement and triumph.

# You did IT

# Panagiotis Kalantzis

Information/Cyber Security & Data Privacy Expert



[p.kalantzis@phiconsultancy.eu](mailto:p.kalantzis@phiconsultancy.eu)



+30 6980 335566 | +30 6987 323414



<http://www.linkedin.com/in/pkalantzis>