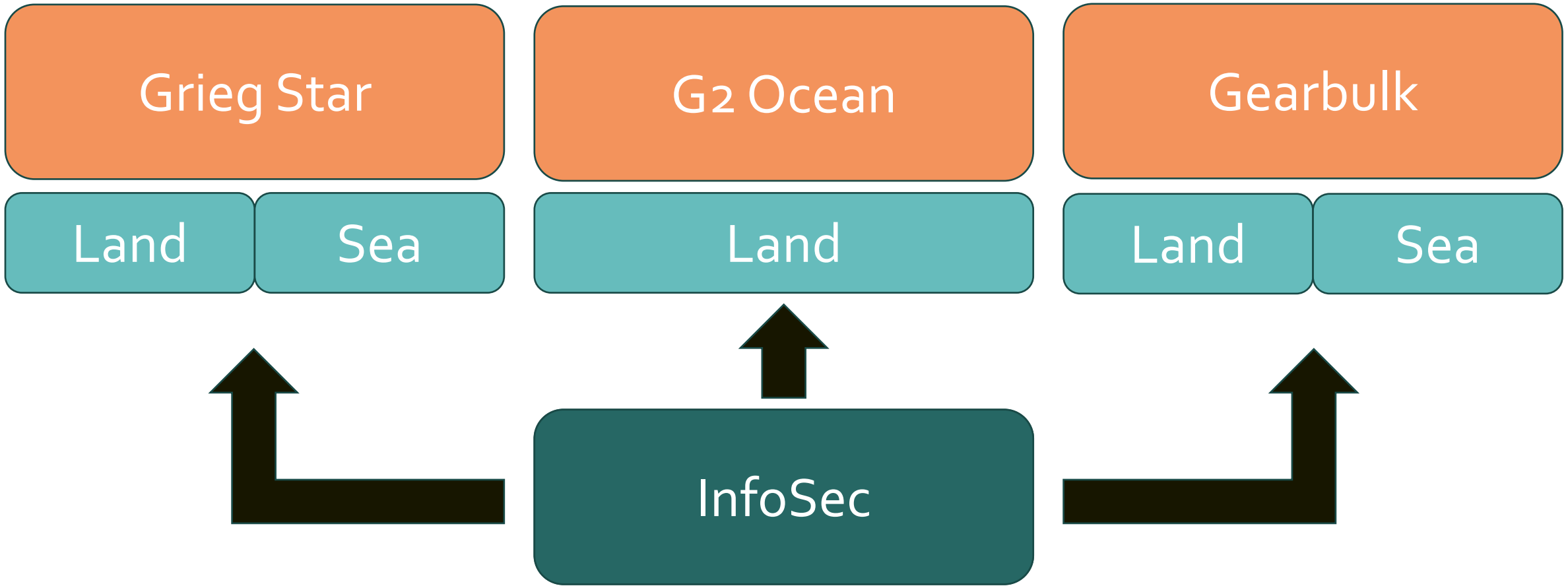
UnITy - Information Security Program

OLEKSANDR KAZYMYROV

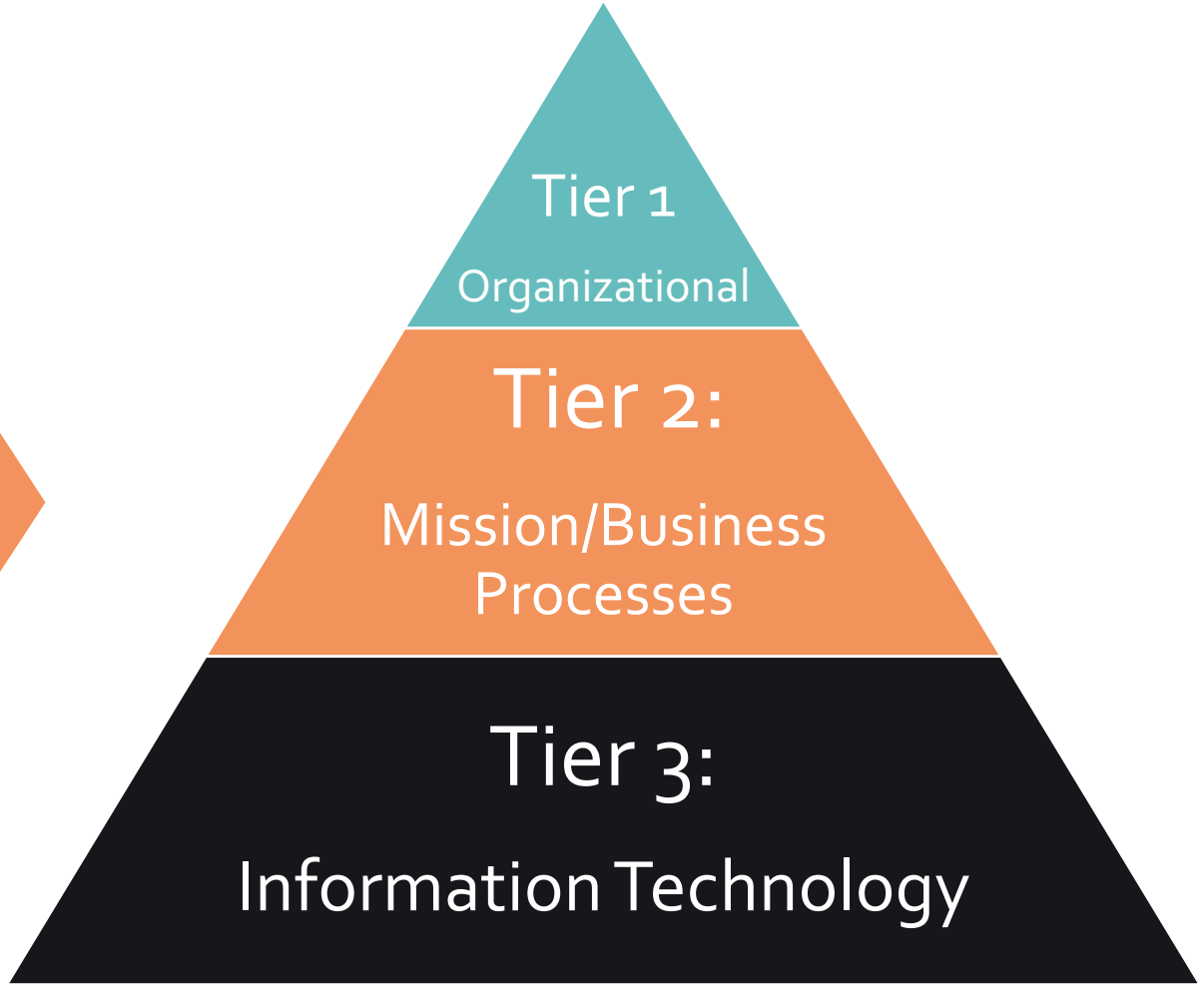
11.09.19

What is UnITy?

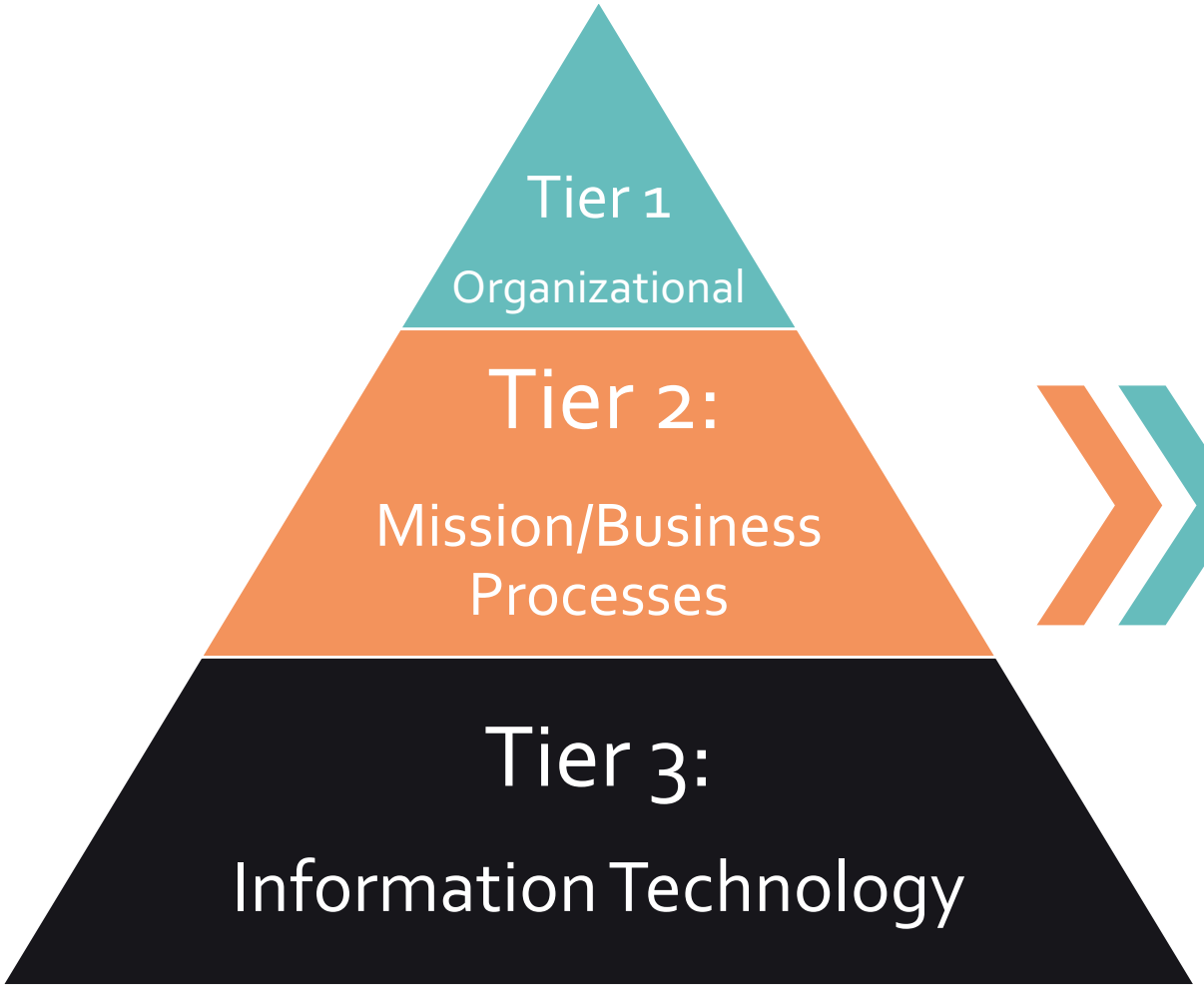


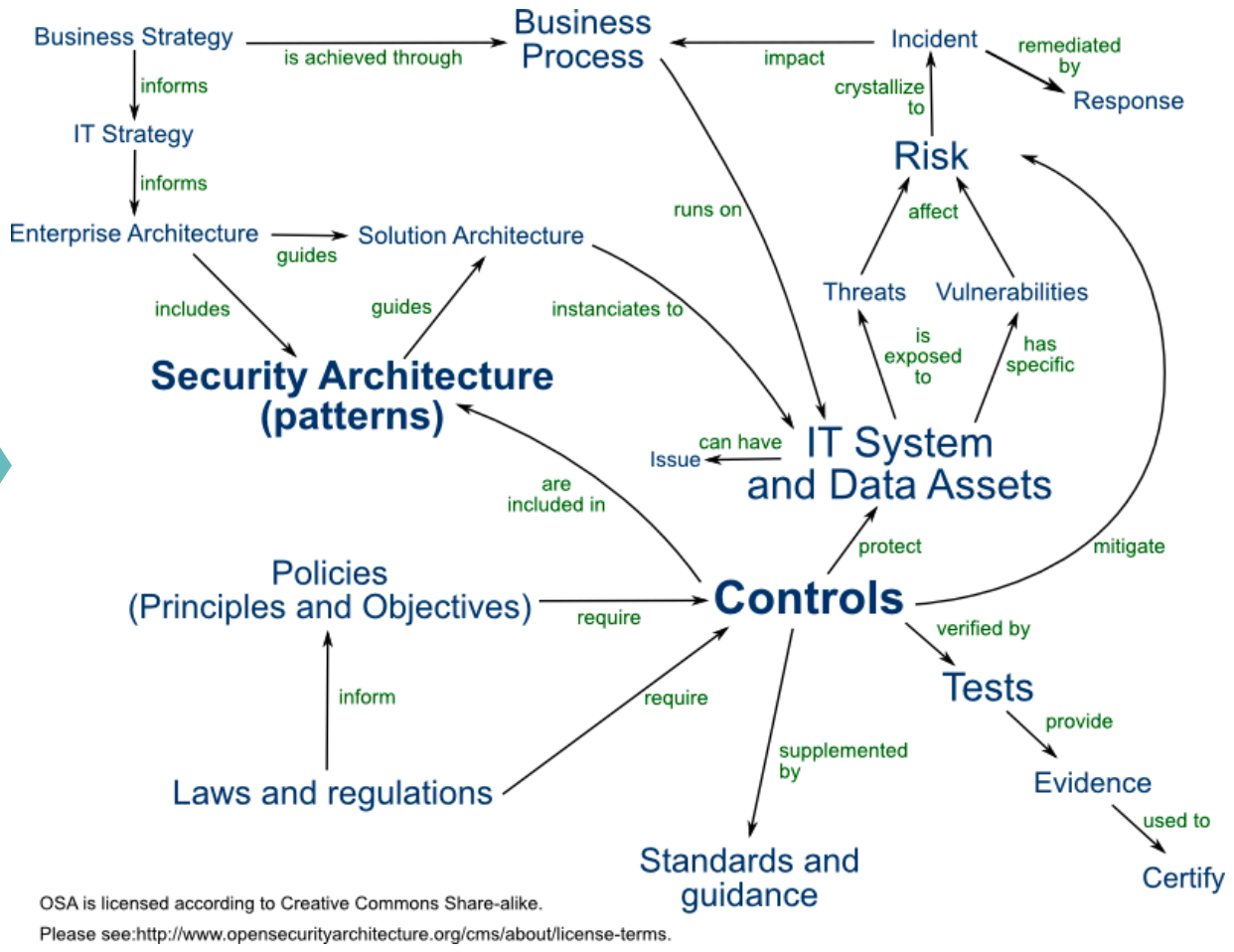
Metamorphosis

Status H1 2019



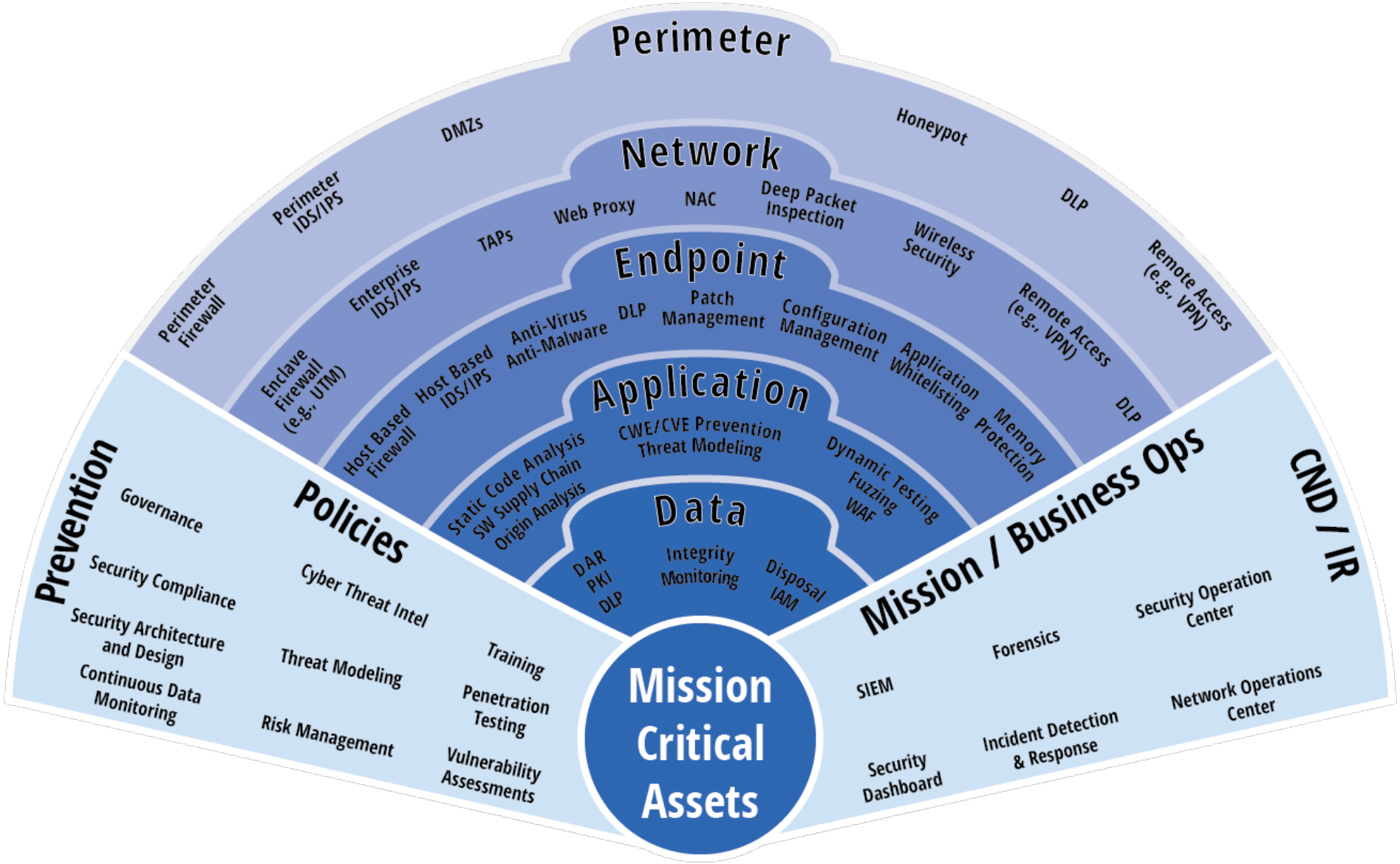
Open Security Architecture





G2 OCEAN

Layered Security (Defense in Depth)



Source: https://www.tmctechnologies.com/cyber/

The Cyber Kill Chain

A **Advanced**

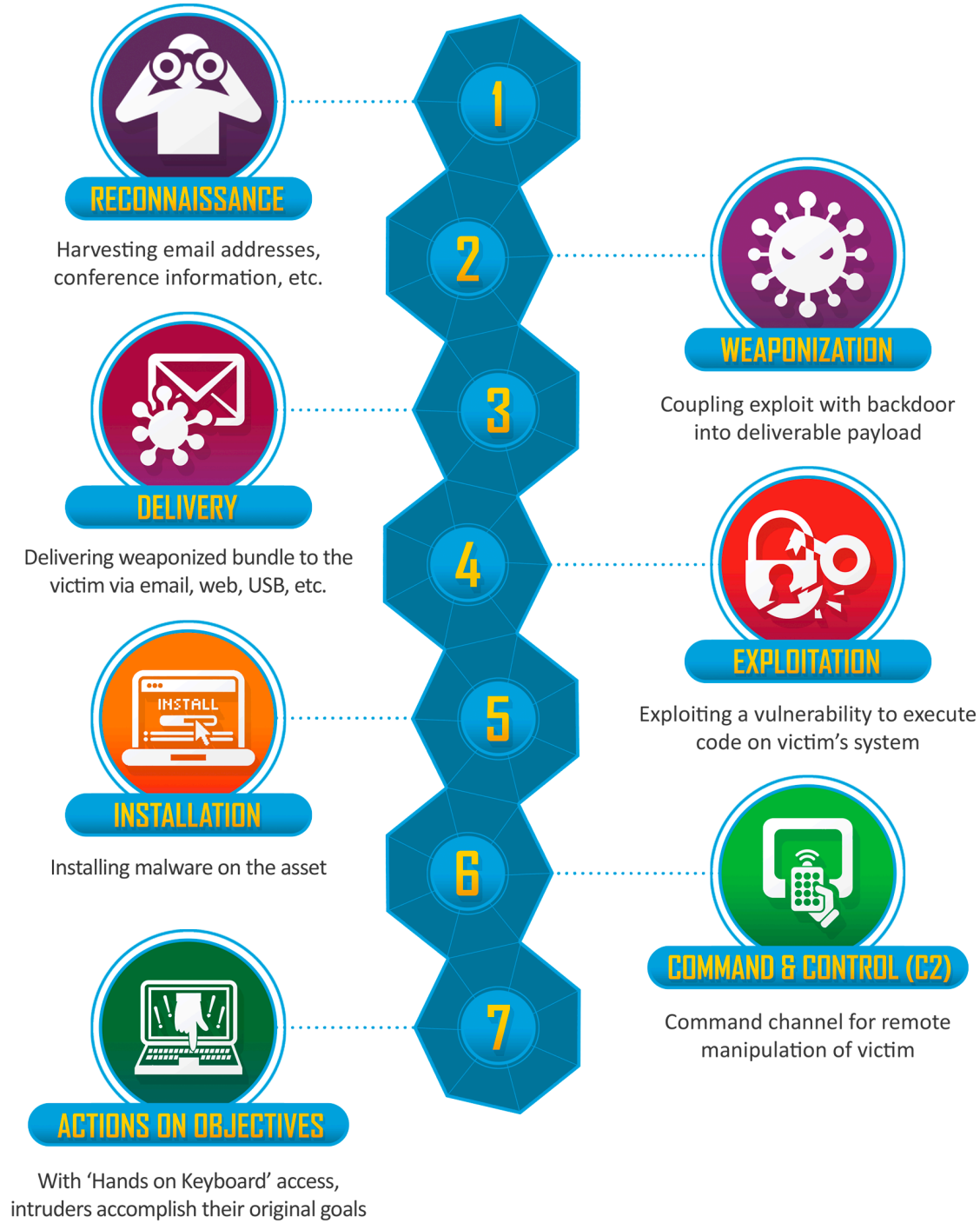
Targeted, Coordinated, Purposeful

P **Persistent**

Month after Month, Year after Year

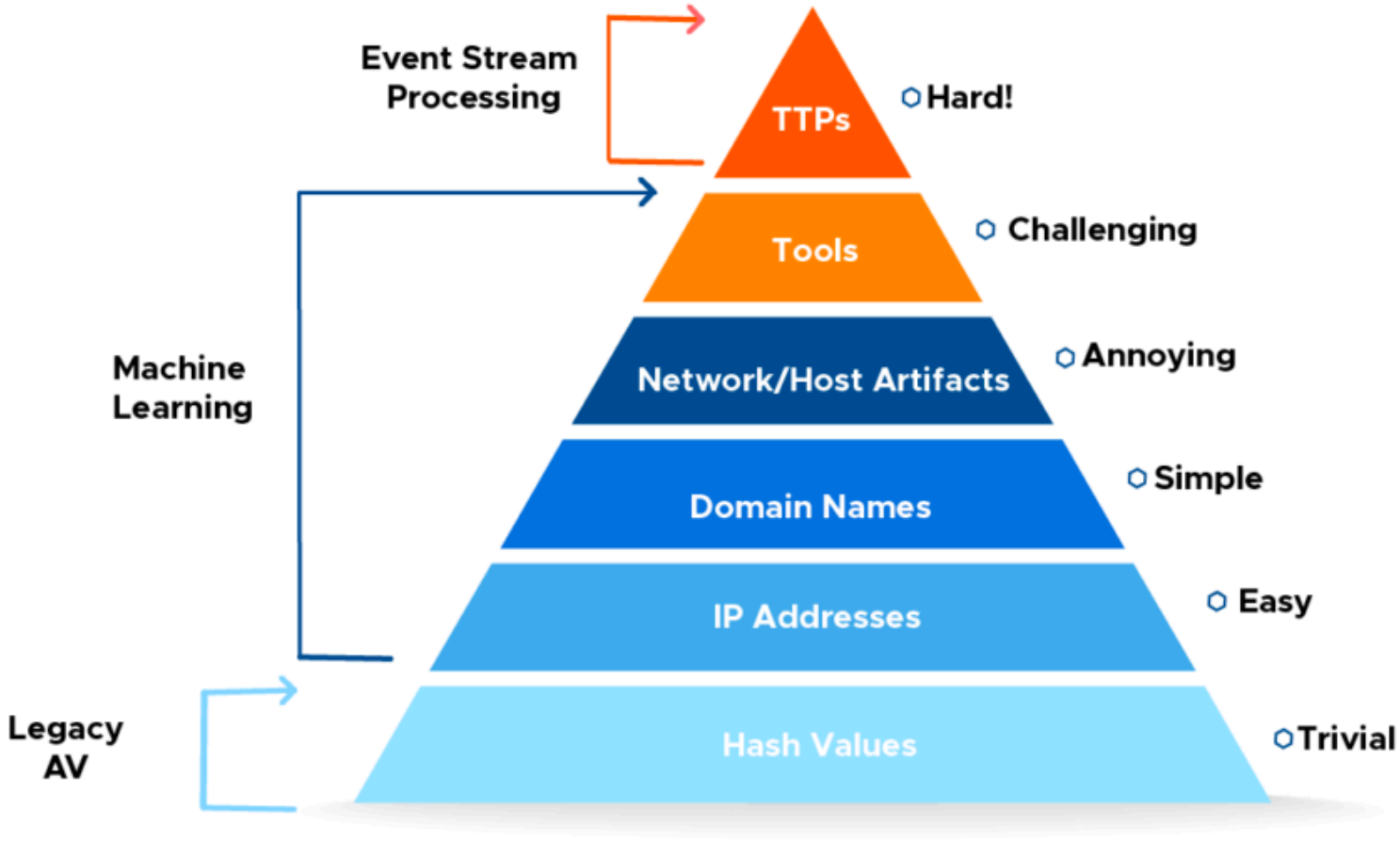
T **Threat**

Person(s) with Intent, Opportunity, and Capability



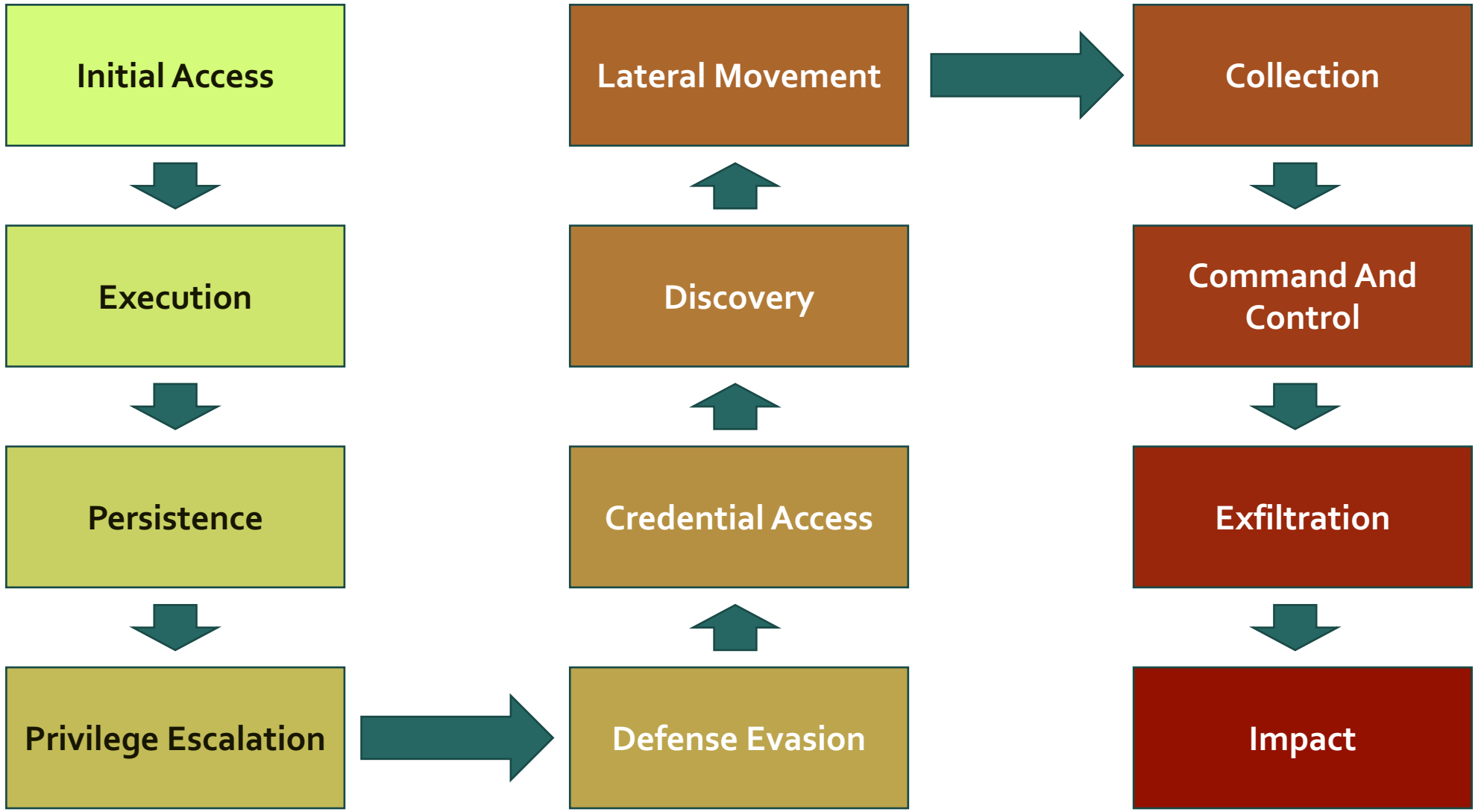
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Pyramid of Pain



Source: https://www.carbonblack.com/2019/03/12/how-to-mature-your-threat-hunting-program-with-the-att-framework/

MITRE ATT&CK



G2 OCEAN

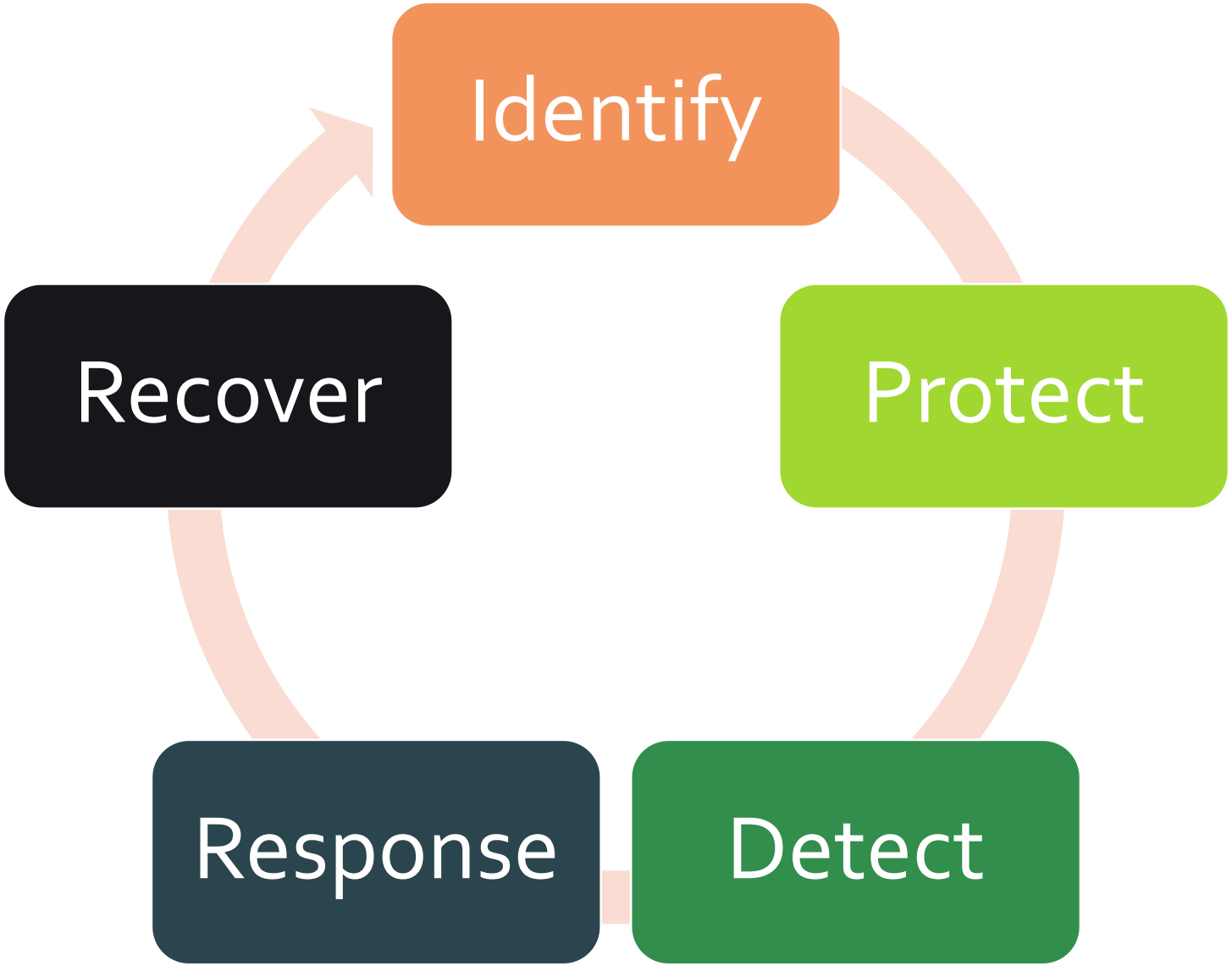
MITRE ATT&CK

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection		System Service Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Service Registry Permissions Weakness	File Deletion		System Time Discovery			Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification		Virtualization/Sandbox Evasion			Web Service		
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Startup Items	Gatekeeper Bypass							
	Source	Launch Daemon	Sudo	Group Policy Modification							
	Space after Filename	Launchctl	Sudo Caching	Hidden Files and Directories							
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Hidden Users							
	Trap	Local Job Scheduling	Web Shell	Hidden Window							
	Trusted Developer Utilities	Login Item		HISTCONTROL							
	User Execution	Logon Scripts		Image File Execution Options Injection							
	Windows Management Instrumentation	LSASS Driver		Indicator Blocking							
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception		InstallUtil							
		Plist Modification		Launchctl							
		Port Knocking		LC_MAIN Hijacking							
		Port Monitors		Masquerading							
		Rc.common		Modify Registry							
		Re-opened Applications		Mshta							
		Redundant Access		Network Share Connection Removal							
		Registry Run Keys / Startup Folder		NTFS File Attributes							
		Scheduled Task		Obfuscated Files or Information							
		Screensaver		Plist Modification							
		Security Support Provider		Port Knocking							
		Service Registry Permissions Weakness		Process Doppelgänging							
		Setuid and Setgid		Process Hollowing							
		Shortcut Modification		Process Injection							
		SIP and Trust Provider Hijacking		Redundant Access							
		Startup Items		Regsvcs/Regasm							
		System Firmware		Regsvr32							
		Systemd Service		Rootkit							
		Time Providers		Rundll32							
		Trap		Scripting							
		Valid Accounts		Signed Binary Proxy Execution							
		Web Shell		Signed Script Proxy Execution							
		Windows Management Instrumentation Event Subscription		SIP and Trust Provider Hijacking							
		Winlogon Helper DLL		Software Packing							
				Space after Filename							
				Template Injection							
				Timestomp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							

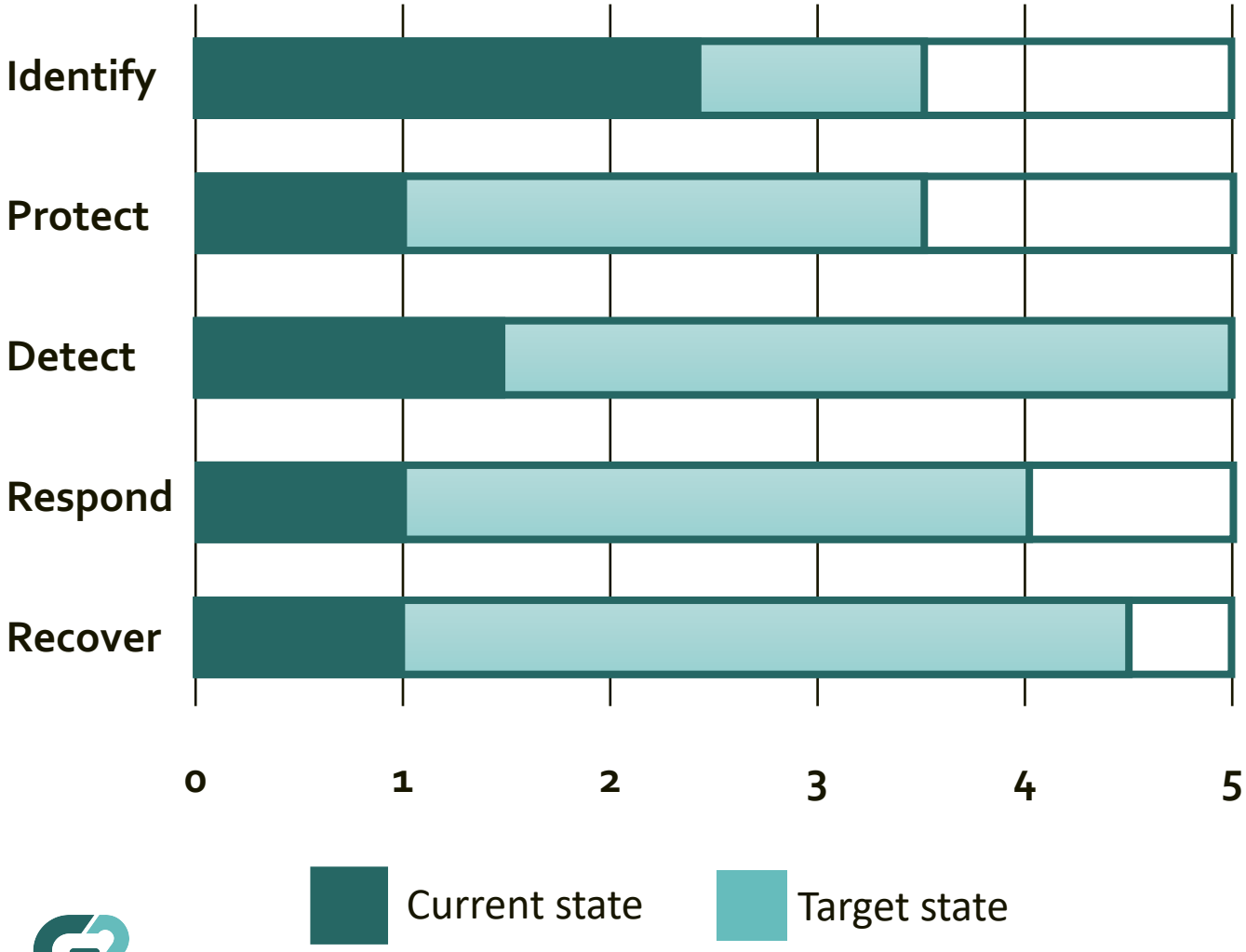
G2 OCEAN

https://mitre-attack.github.io/attack-navigator/enterprise/#

NIST Cybersecurity Framework



Measure Security by Key Performance Indicators (KPIs)



FUNCTION	CATEGORY	CIS CONTROL
Identify	Asset Management	CIS Control 1, 2
	Business Environment	
	Governance	
	Risk Assessment	CIS Control 3
	Risk Management Strategy	
	Supply Chain Risk Management	
Protect	Identity Management, Authentication, and Access Control	CIS Control 4, 9, 11, 12, 13, 14, 16
	Awareness and Training	CIS Control 4, 17
	Data Security	CIS Control 1, 2, 13, 14, 18
	Information Protection Processes and Procedures	CIS Control 3, 5, 7, 10, 11
	Maintenance	CIS Control 4, 12
	Protective Technology	CIS Control 4, 6, 8, 11, 13, 14, 16
Detect	Anomalies and Events	CIS Control 6, 9, 12, 19
	Security Continuous Monitoring	CIS Control 3, 8, 19
	Detection Processes	CIS Control 6
Respond	Response Planning	CIS Control 19
	Communications	CIS Control 19
	Analysis	CIS Control 3, 19
	Mitigation	CIS Control 3, 19
	Improvements	CIS Control 19
Recover	Recovery Planning	CIS Control 19
	Improvements	CIS Control 19
	Communications	CIS Control 19

G2 OCEAN

Vendor Risk Management

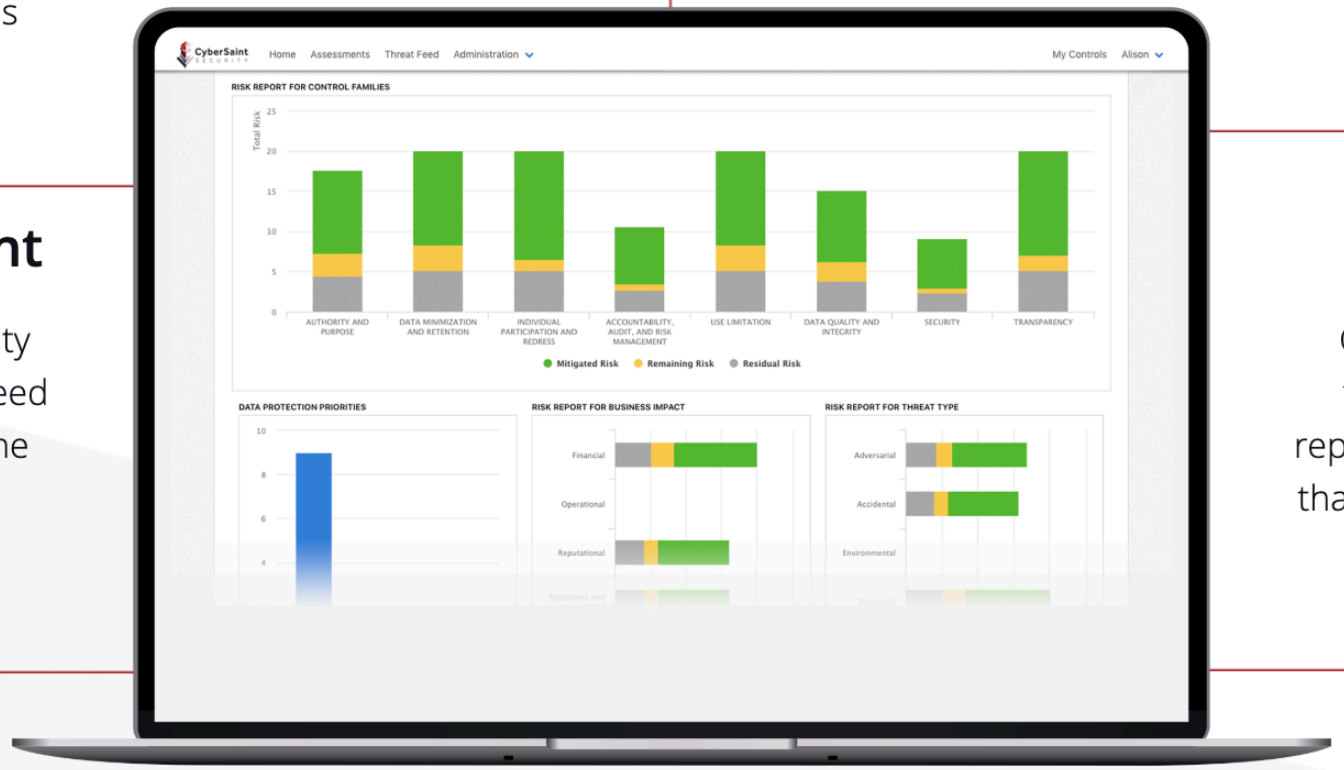
Automate the standardization of security and risk assessments, risk quantification, business impact analyses and reporting across third parties, partners, and vendors to uncover unknown risks

IT Risk Management

Protect your infrastructure with actionable threat intelligence, risk quantification, and optimized plans that provide the lowest cost, highest impact path towards your goals

Compliance Management

Get visibility into your posture projected across standards, eliminate manual effort across assessments, and focus on automated plans that will lower risk



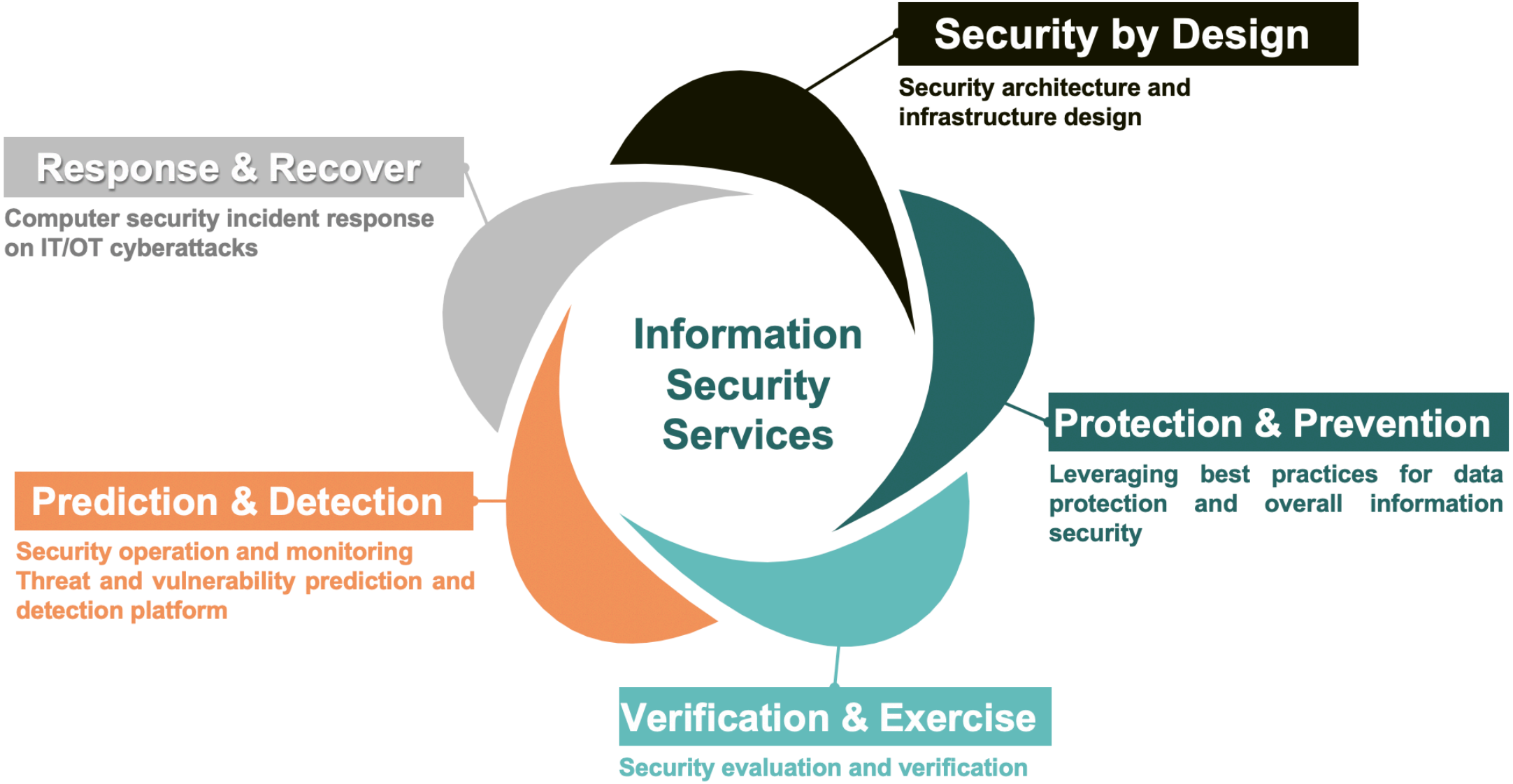
Digital Risk Management

Manage risk confidently with scalability and flexibility that keeps you up to speed with the digital transformation and the evolving risk landscape

Audit Management

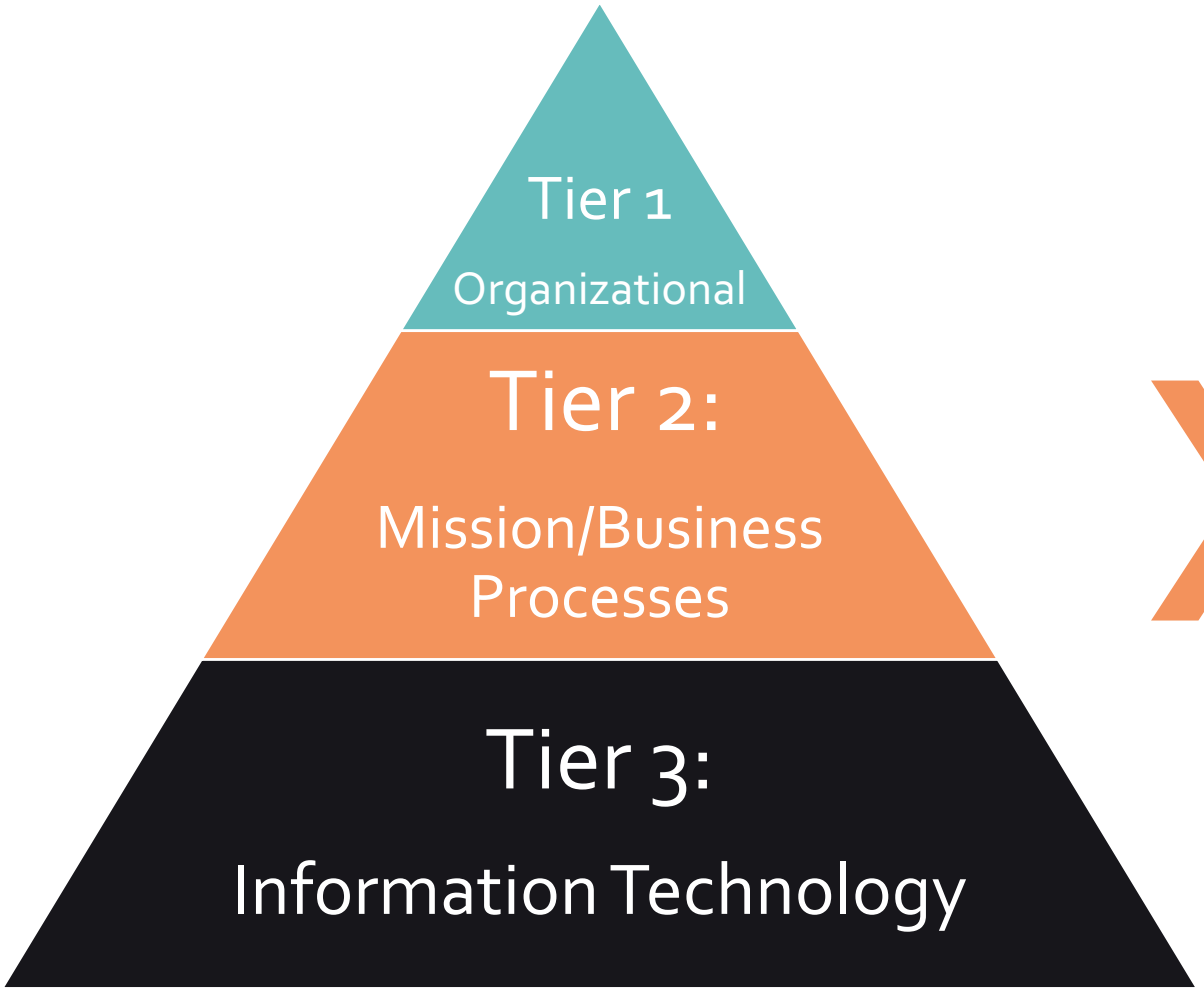
Give auditors the exact information they're looking for with audit-ready reports and optimized remediation plans that require no human effort to produce

Integrated Risk Management (CyberStrong)


Security by Design
Security architecture and infrastructure design
Response & Recover
Computer security incident response on IT/OT cyberattacks
Information Security Services
Protection & Prevention
Leveraging best practices for data protection and overall information security
Prediction & Detection
Security operation and monitoring
Threat and vulnerability prediction and detection platform
Verification & Exercise
Security evaluation and verification

G2 OCEAN

Summary



NIST CSF (tracked by CyberStrong)

Jira Cloud / Project Planner
CIS Controls / Security Domain

Jira Cases / CIS Controls

G2 OCEAN

UnITy's Security Tools Portfolio

insightIDR

SentinelOne™

insightVM

MetaCompliance®

CyberSaint SECURITY

freshservice

G2 OCEAN