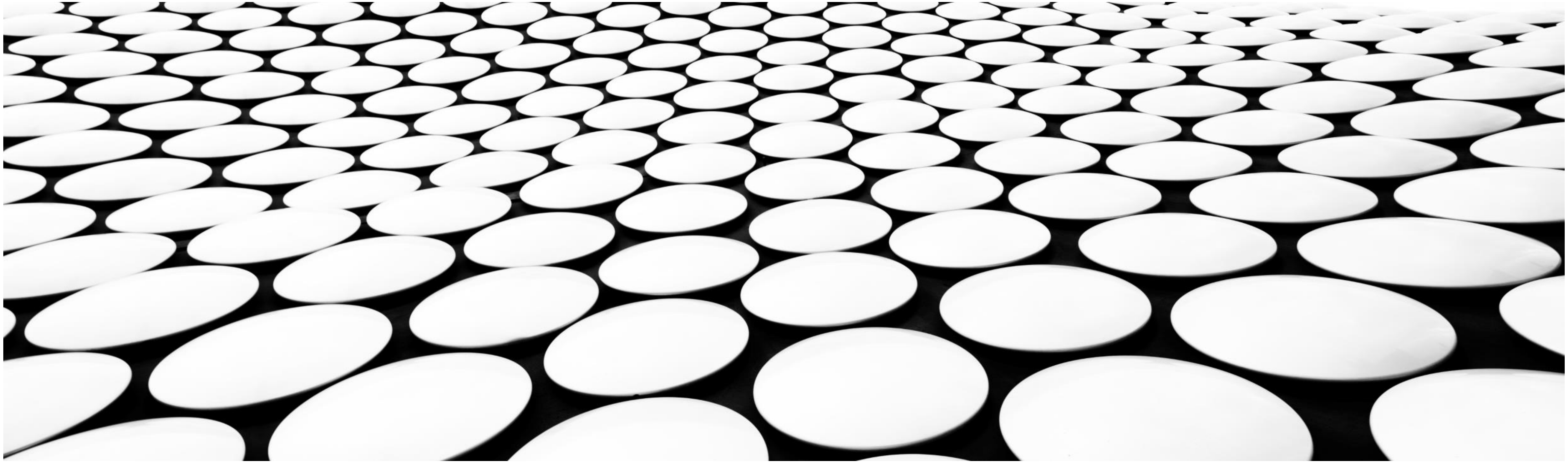
BRINGING THE FIGHT TO THE ADVERSARY

Integrating SABSA and Cyber Threat Intelligence to improve cyber security operations



/whois @beLarge

A cyber security architecture enthusiast, infrastructure tourist and "cyber hype guy"

- Operational Technology (OT) Security Team Leader at Powerlink
- Worked in IT and OT in Network & System Engineering and Cyber Security roles for 15 years
- Chartered Engineer (CPEng) and Registered Professional Engineer of Queensland (RPEQ)
- Proud member of Professional's Australia (PA) and a union delegate for PA at Powerlink
- Vice Chair of the Queensland Branch of the Australian Information Security Association (AISA) and Chair of the AISA Security Architecture Special Interest Group (SecARCH SIG)
- Bach Eng (Telecomms) QUT First Class Honours and Master Business (Applied Finance) with Distinction QUT

SABSA
FOUNDATION LEVEL SCF
GIAC RESPONSE AND INDUSTRIAL DEFENSE
GRID
GIAC SECURITY OPERATIONS MANAGER
GSOM
ISA/IEC 62443
CYBERSECURITY
EXPERT
ISA
alc
Cyber Security Foundation+Practitioner
CERTIFIED

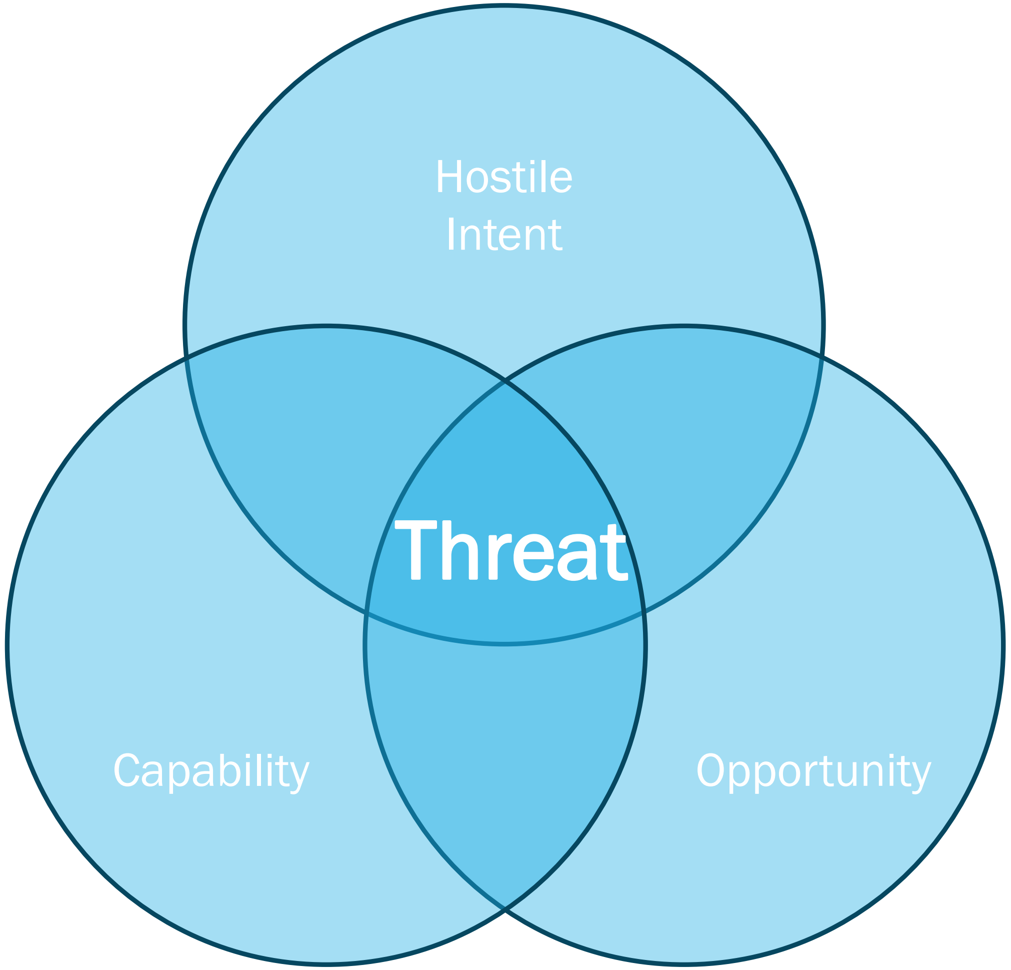
Agenda

1. Why this presentation?
2. An overview of Military Intelligence and applying it to Cyber Threat Intelligence
3. Aligning CTI and SABSA
4. Worked Example
5. Further Resources

Why *this* presentation?

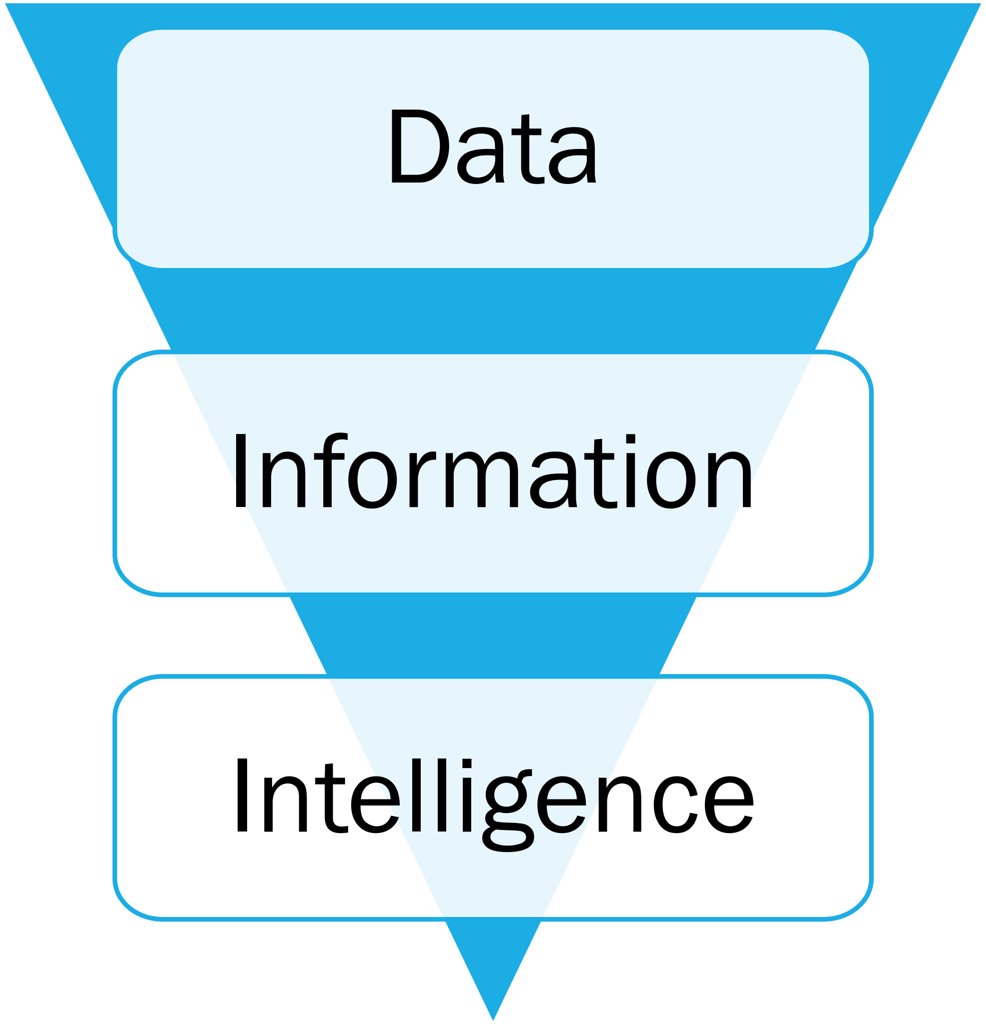
AN OVERVIEW OF MILITARY INTELLIGENCE AND CYBER THREAT INTELLIGENCE

WHAT IS A THREAT?



Ref – SANS ICS515

THREAT DATA, INFORMATION AND INTELLIGENCE

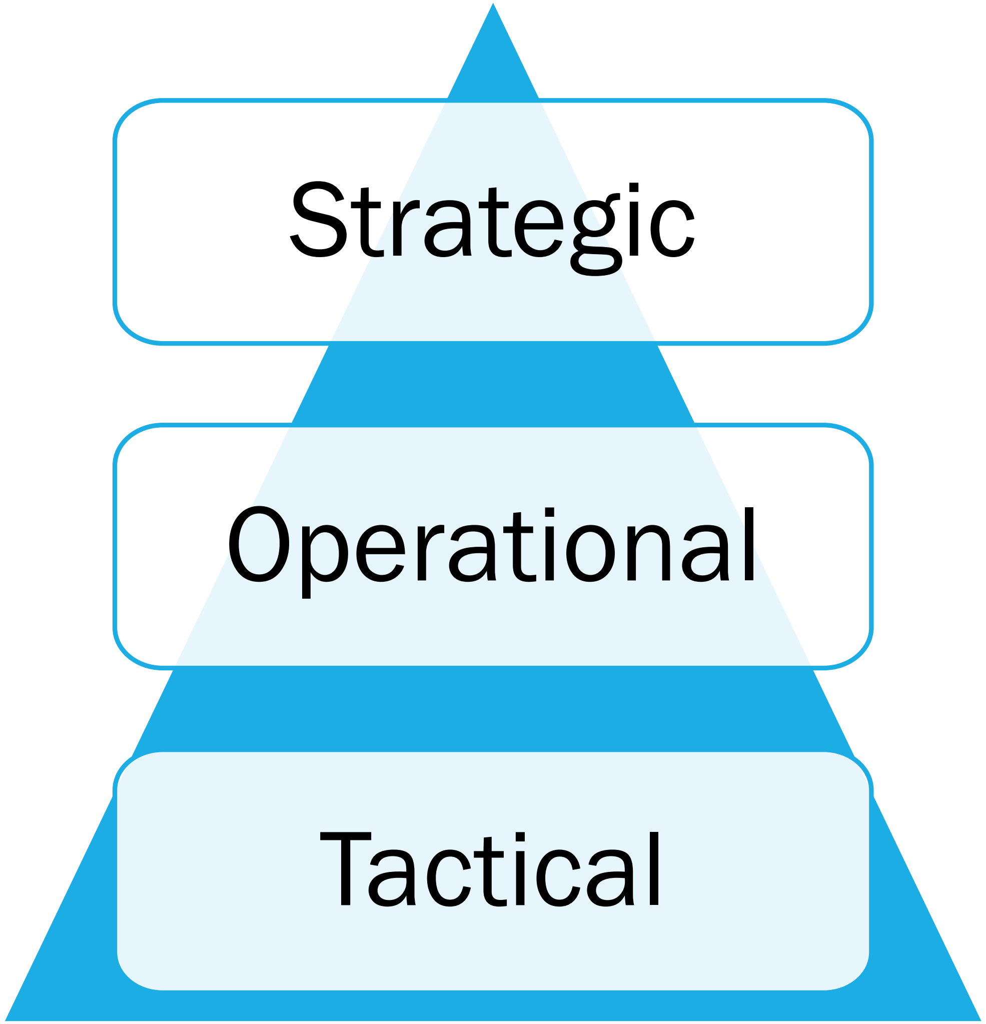


Raw Sensor Data, Indicators of Compromise (IoC), Network Telemetry, Endpoint Telemetry

Has been processed to add some context to the data – "What has happened"

Adds human analysis to derive insight – "Why this happened" and "What may happen"

THE THREE TIERS OF INTELLIGENCE

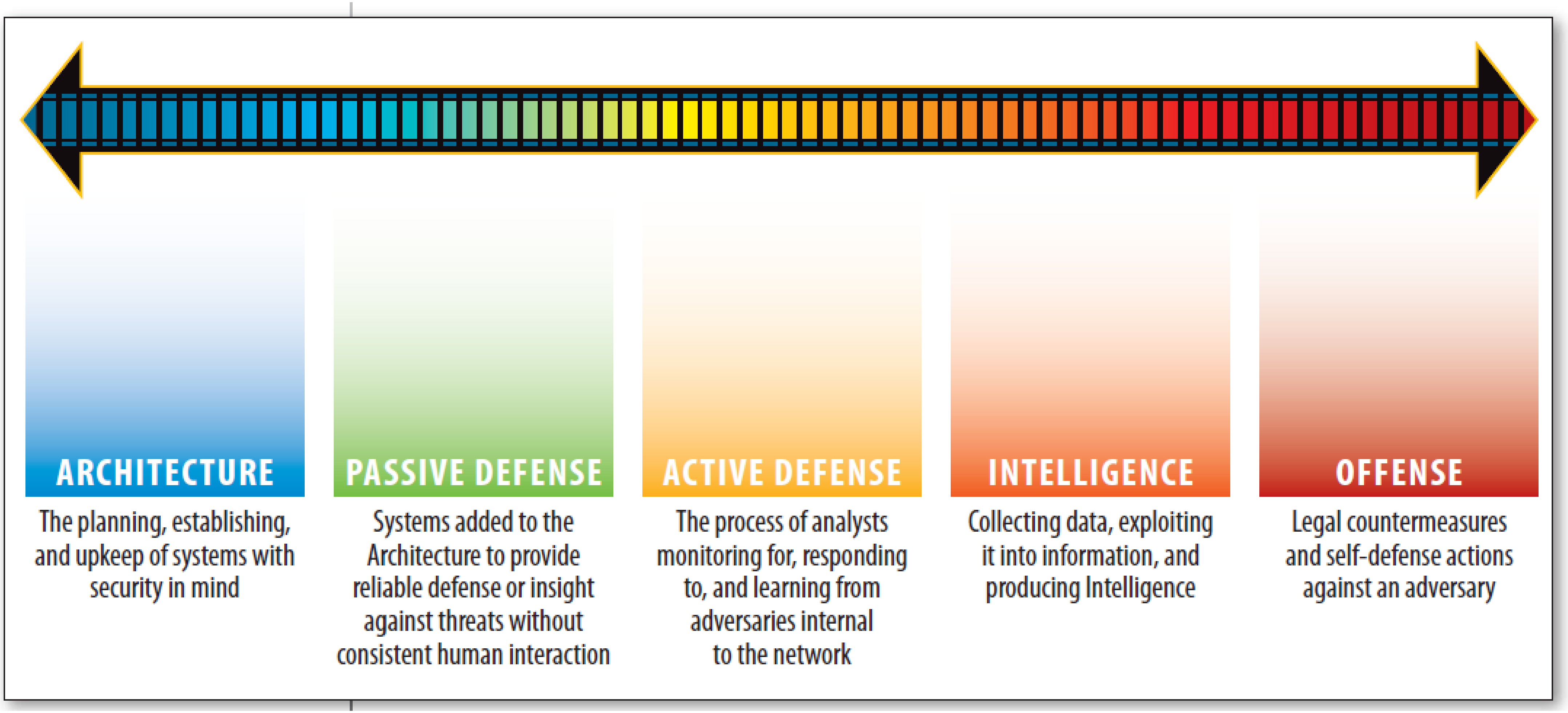


What are the Geopolitical trends? What is happening in my industry? What Business Assets are they targeting?

What Tactics, Techniques and Procedures are adversaries using? Do I have appropriate controls to counter the threats?

Specific Technical Indicators of Compromise (IoC) with Context (!) – Are controls enriched with threat data?

CYBER THREAT INTELLIGENCE IS A KEY COMPONENT OF ACTIVE DEFENCE



ARCHITECTURE

The planning, establishing, and upkeep of systems with security in mind

PASSIVE DEFENSE

Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction

ACTIVE DEFENSE

The process of analysts monitoring for, responding to, and learning from adversaries internal to the network

INTELLIGENCE

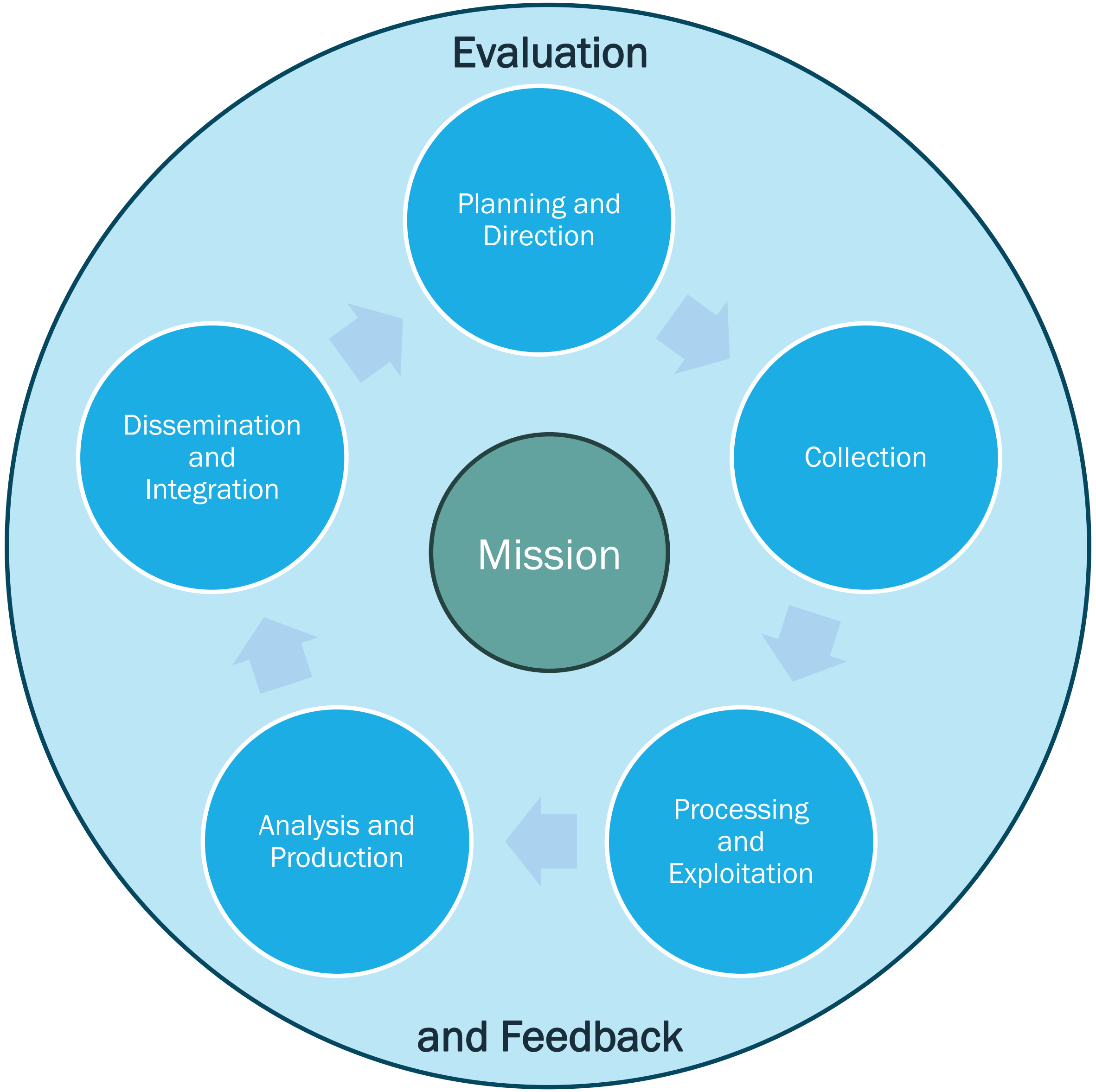
Collecting data, exploiting it into information, and producing Intelligence

OFFENSE

Legal countermeasures and self-defense actions against an adversary

Ref - SANS Sliding Scale of Cyber Security (https://www.sans.org/white-papers/36240/)

THE INTELLIGENCE PLANNING LIFE CYCLE



Ref – US DoD JP 2-0

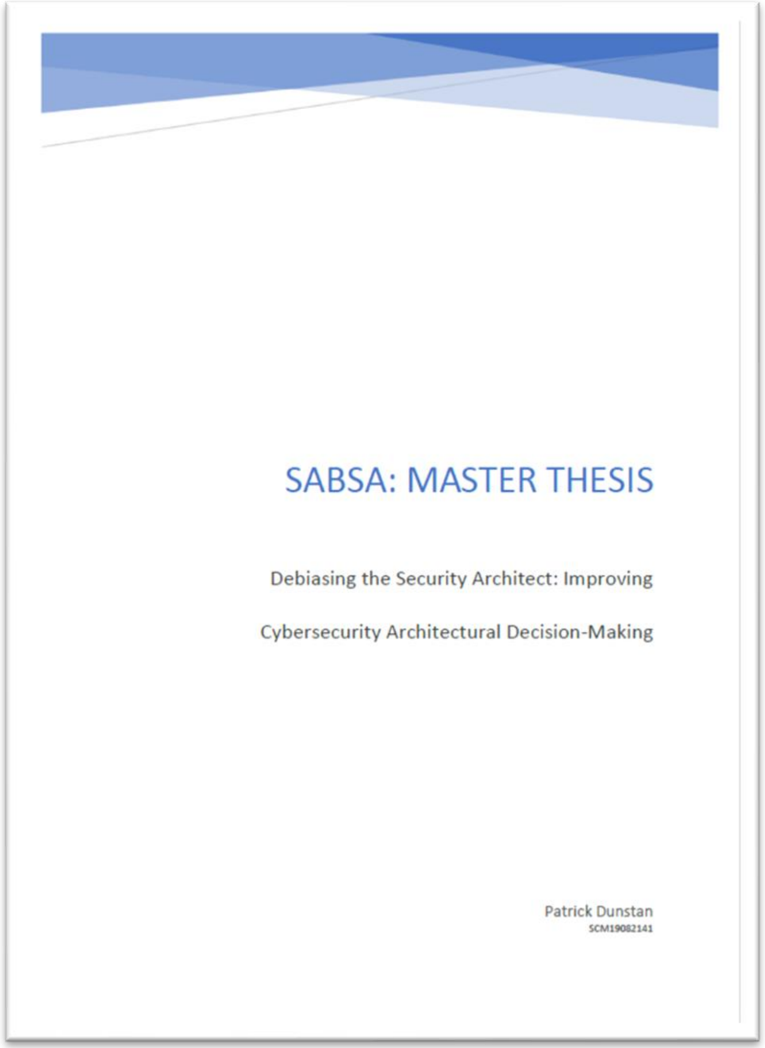
RELATIONSHIP BETWEEN INTELLIGENCE REQUIREMENTS AND INFORMATION REQUIREMENTS

- Intelligence Requirement
  - *“Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence.”*
- Priority Intelligence Requirement
  - *“An intelligence requirement stated as a priority for intelligence support, that the commander and staff need to understand the adversary or operational environment."*
- Information Requirements
  - *“In intelligence usage, those items of information regarding the adversary and other relevant aspects of the operational environment that need to be collected and processed in order to meet the intelligence requirements of a commander.”*
- Essential Element of Information (EEI)
  - *“The most critical information requirements regarding the adversary and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to reach a logical decision."*

Ref – US DoD JP 2-0

A NOTE ON BIASES

- Given the human analysis it is critical that Cyber Threat Intelligence processes considers and manages potential biases of analysts
- Example Biases:
  - **Confirmation Bias**
  - Mirroring
  - Recency Bias
  - Causality Bias (The illusion of causality)
  - And many more …
- Huer’s *Psychology of Intelligence Analysis* is a must read
- An excellent paper on this topic is Patrick Dunstan’s SABSA Master Thesis – please reach out to him to request if it if you are interested



SABSA: MASTER THESIS

Debiasing the Security Architect: Improving

Cybersecurity Architectural Decision-Making

Patrick Dunstan
SCM19082141

THE INTELLIGENCE PREPARATION OF THE OPERATIONAL ENVIRONMENT

- A structured process to determine the Operational Environment and the Adversary Capabilities and courses of action

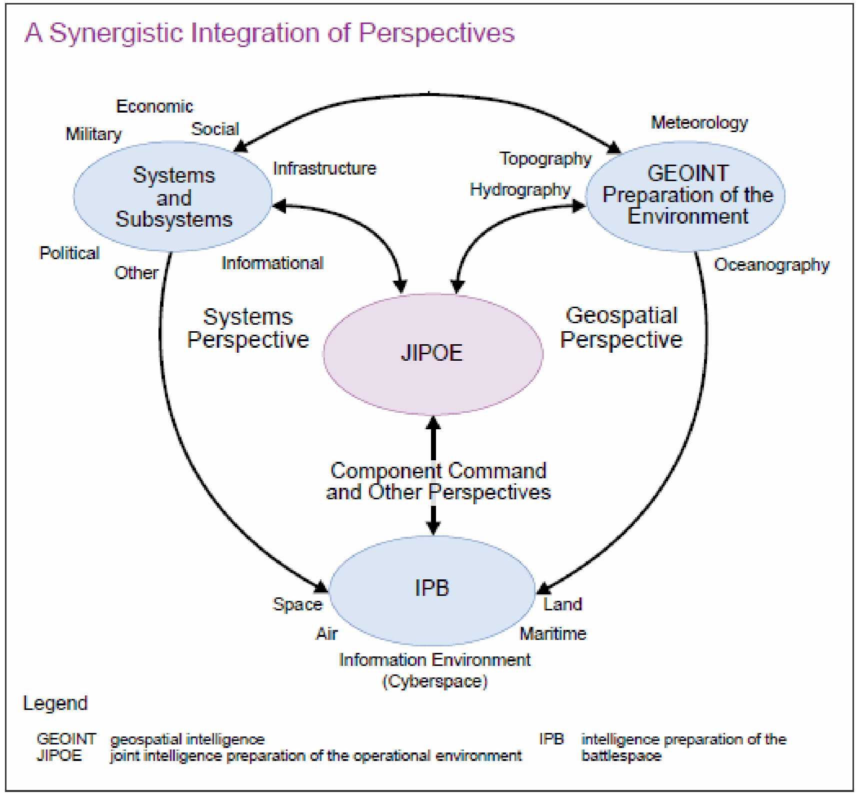
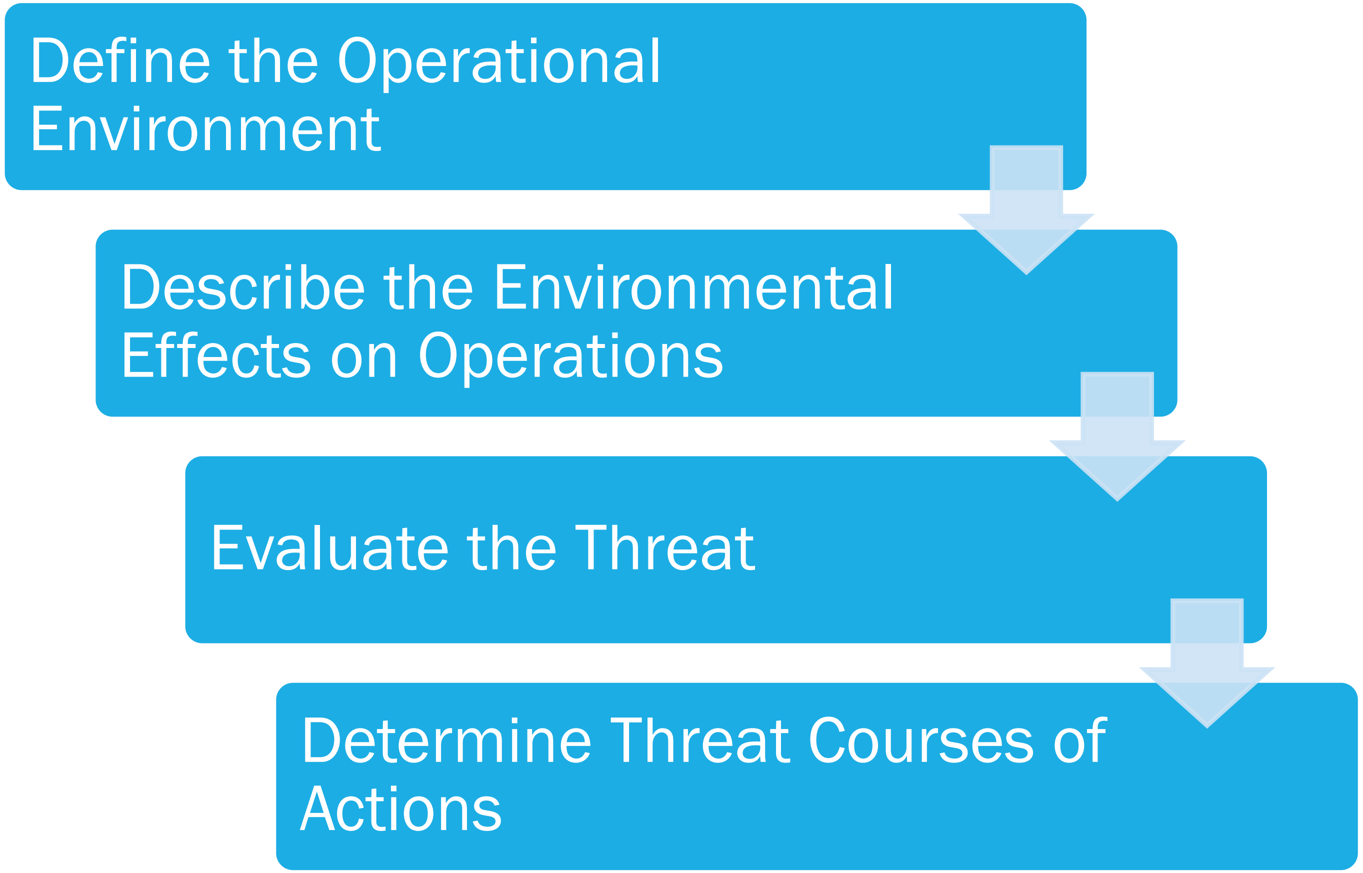

A Synergistic Integration of Perspectives
Economic
Military
Social
Meteorology
Systems and Subsystems
Infrastructure
Topography
Hydrography
GEOINT Preparation of the Environment
Political
Other
Informational
Oceanography
Systems Perspective
JIPOE
Geospatial Perspective
Component Command and Other Perspectives
IPB
Space
Land
Air
Maritime
Information Environment (Cyberspace)
Legend
GEOINT geospatial intelligence
JIPOE joint intelligence preparation of the operational environment
IPB intelligence preparation of the battlespace

Figure I-2. A Synergistic Integration of Perspectives



Define the Operational Environment

Describe the Environmental Effects on Operations

Evaluate the Threat

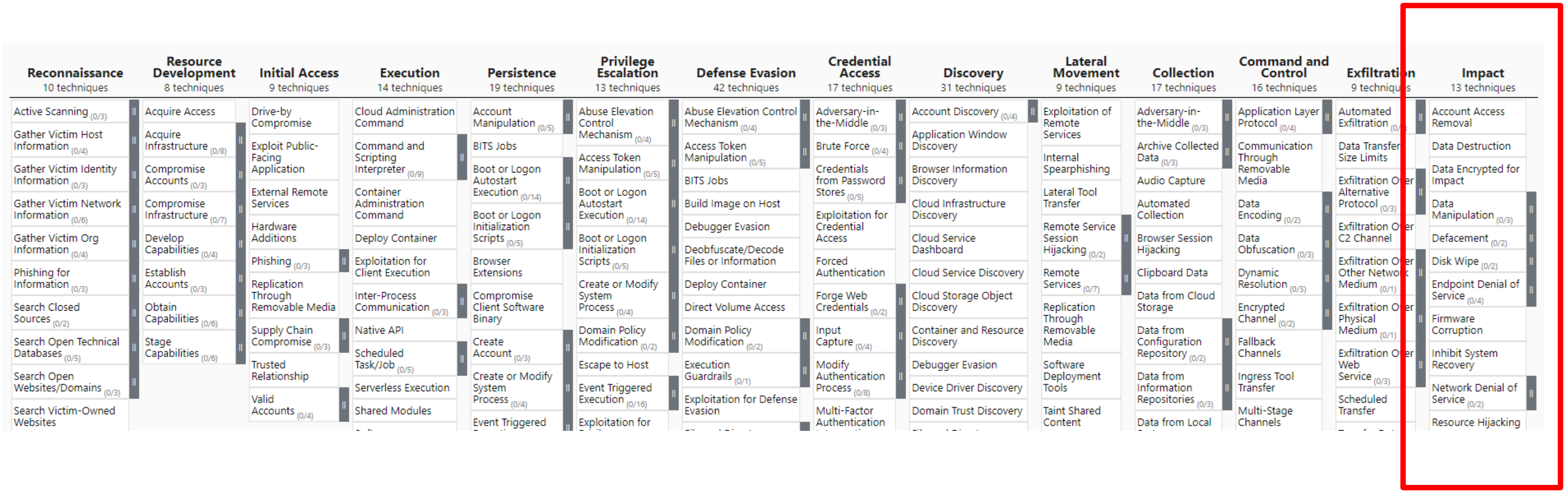
Determine Threat Courses of Actions

WHAT ARE COURSES OF ACTION?

Kill Chains and

MITRE ATT&CK

- A *Course of Action* is an option that the adversary has
- For Cyber Security CoAs can be expressed as “Cyber Kill Chains”
  - Can be expressed as MITRE ATT&CK TTPs and consider the *Impact* techniques effecting Attributes
- The key is to understand **Most Likely** and **Most Dangerous CoA** as scoping to ensure you have appropriate control coverage and defence in depth



Reconnaissance
10 techniques

- Active Scanning (0/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/3)
- Search Victim-Owned Websites

Resource Development
8 techniques

- Acquire Access
- Acquire Infrastructure (0/8)
- Compromise Accounts (0/3)
- Compromise Infrastructure (0/7)
- Develop Capabilities (0/4)
- Establish Accounts (0/3)
- Obtain Capabilities (0/6)
- Stage Capabilities (0/6)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (0/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/4)

Execution
14 techniques

- Cloud Administration Command
- Command and Scripting Interpreter (0/9)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (0/3)
- Native API
- Scheduled Task/Job (0/5)
- Serverless Execution
- Shared Modules

Persistence
19 techniques

- Account Manipulation (0/5)
- BITS Jobs
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/4)
- Event Triggered

Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Domain Policy Modification (0/2)
- Escape to Host
- Event Triggered Execution (0/16)
- Exploitation for

Defense Evasion
42 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (0/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion

Credential Access
17 techniques

- Adversary-in-the-Middle (0/3)
- Brute Force (0/4)
- Credentials from Password Stores (0/5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (0/2)
- Input Capture (0/4)
- Modify Authentication Process (0/8)
- Multi-Factor Authentication

Discovery
31 techniques

- Account Discovery (0/4)
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (0/7)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content

Collection
17 techniques

- Adversary-in-the-Middle (0/3)
- Archive Collected Data (0/3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository (0/2)
- Data from Information Repositories (0/3)
- Data from Local

Command and Control
16 techniques

- Application Layer Protocol (0/4)
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (0/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (0/2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels

Exfiltration
9 techniques

- Automated Exfiltration (0/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (0/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (0/3)
- Scheduled Transfer

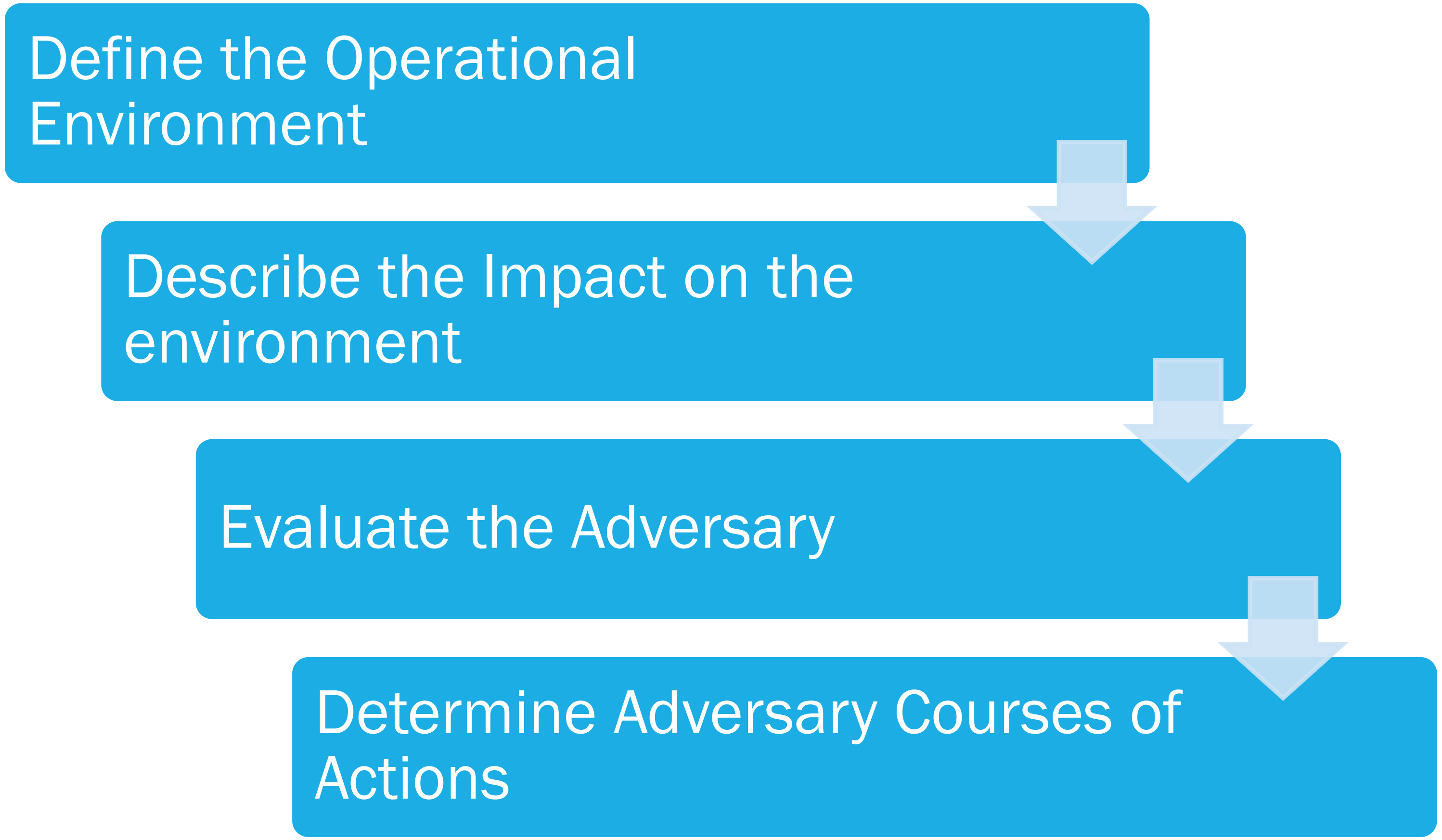
Impact
13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (0/3)
- Defacement (0/2)
- Disk Wipe (0/2)
- Endpoint Denial of Service (0/4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (0/2)
- Resource Hijacking

Ref - https://mitre-attack.github.io/attack-navigator/

INTELLIGENCE PREPARATION OF THE CYBER ENVIRONMENT

- IPCE applies Intelligence Preparation of the Operational Environment to the Cyber Domain, The Fifth Domain of Warfare
- Modifies key concepts like Terrain and Weather and links to Computer Network Operations concepts like Network and Traffic
- Provides a framework for how to apply cyber security controls based on intelligence collection plans (ICP) and defined responses for indicators and warnings



Define the Operational Environment

Describe the Impact on the environment

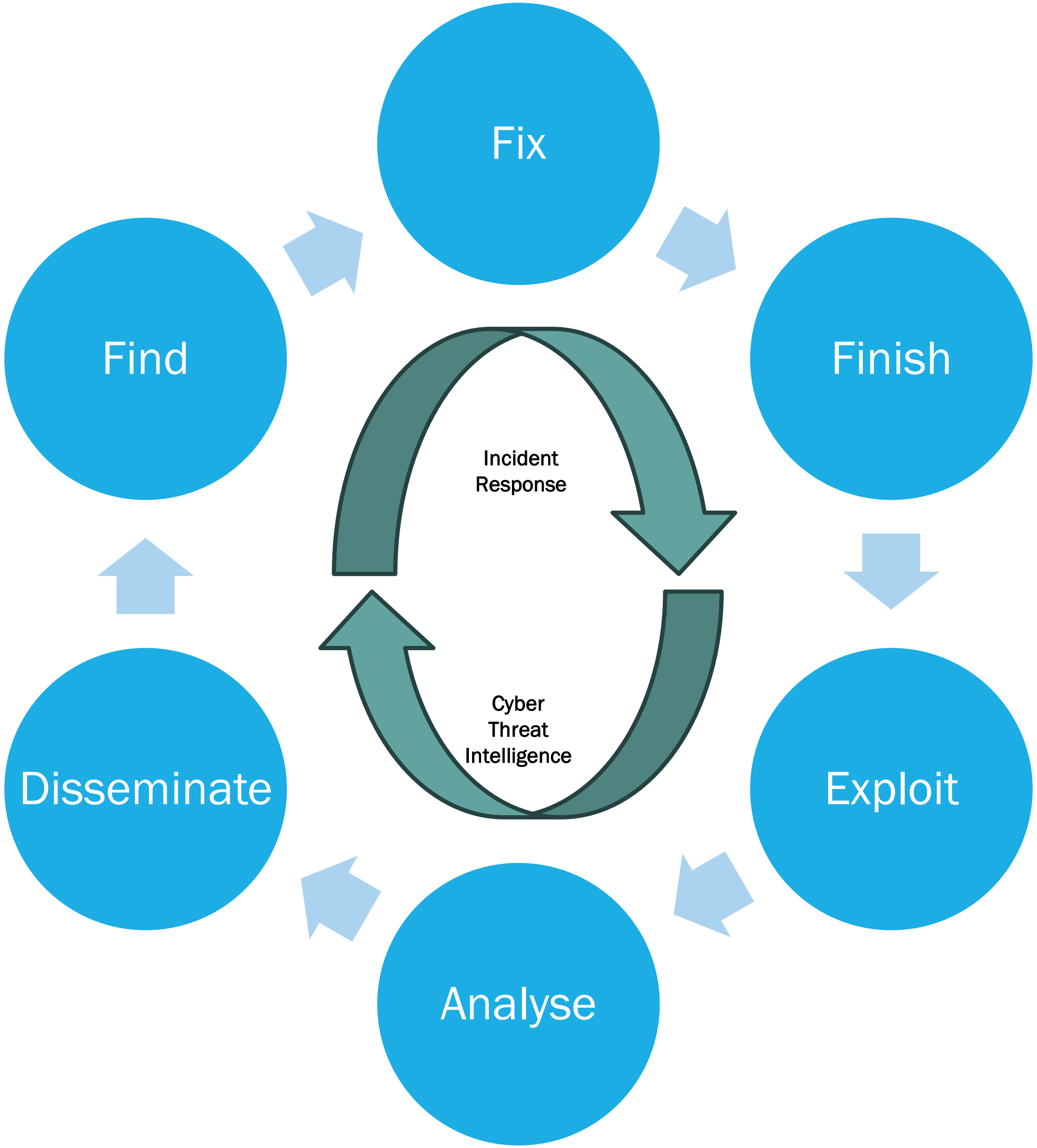
Evaluate the Adversary

Determine Adversary Courses of Actions

Ref - https://www.jinfowar.com/journal/volume-13-issue-3/intelligence-preparation-cyber-environment-ipce-finding-high-ground

F3EAD

A fusion of Operations and Threat Intelligence applied to Cyber Security Operations



TYING IT ALL TOGETHER – CYBER THREAT PROFILE

- A living document that articulates:
  - Critical Business Assets
  - Feasible Threat and Threat Actors
  - Most likely and most dangerous Courses of Actions and/or Tactics, Techniques and Procedures
- *“A characterization of the likely intent, capability, and targets for threats to the function. It is the result of one or more threat assessments across the range of feasible threats to the IT, OT, and information assets of an organization and to the organization itself, identifying feasible threats, describing the nature of the threats, and evaluating their severity.” (Ref C2M2 v2.1)*
- The C2M2 team are releasing an example threat profile but the SANS paper is a great reference as well

SANS | GIAC CERTIFICATIONS

WHITE PAPER

Creating a Threat Profile for Your Organization

Stephen Irwin

Copyright SANS Institute 2021. Author Retains Full Rights.

This paper was published by SANS Institute. Reposting is not permitted without express written permission.

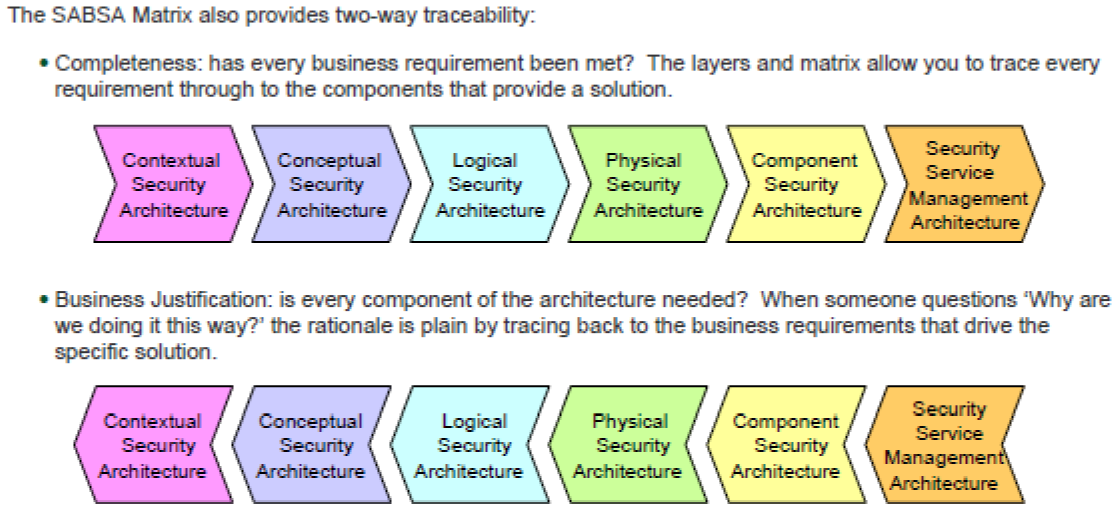
Ref - https://www.sans.org/white-papers/35492/

NEW

QUICK OVERVIEW OF SABSA

SABSA 101

- SABSA has its origins as the Enterprise Security Architecture for the SWIFT Payments Network
- Business Aligned, Top Down and Deliberate, not just *best practice*
- Focus on *Attributes* which are security goals/objectives/requirements
- Two Way Traceability



The SABSA Matrix also provides two-way traceability:

- Completeness: has every business requirement been met? The layers and matrix allow you to trace every requirement through to the components that provide a solution.

Contextual Security Architecture
Conceptual Security Architecture
Logical Security Architecture
Physical Security Architecture
Component Security Architecture
Security Service Management Architecture

- Business Justification: is every component of the architecture needed? When someone questions ‘Why are we doing it this way?’ the rationale is plain by tracing back to the business requirements that drive the specific solution.

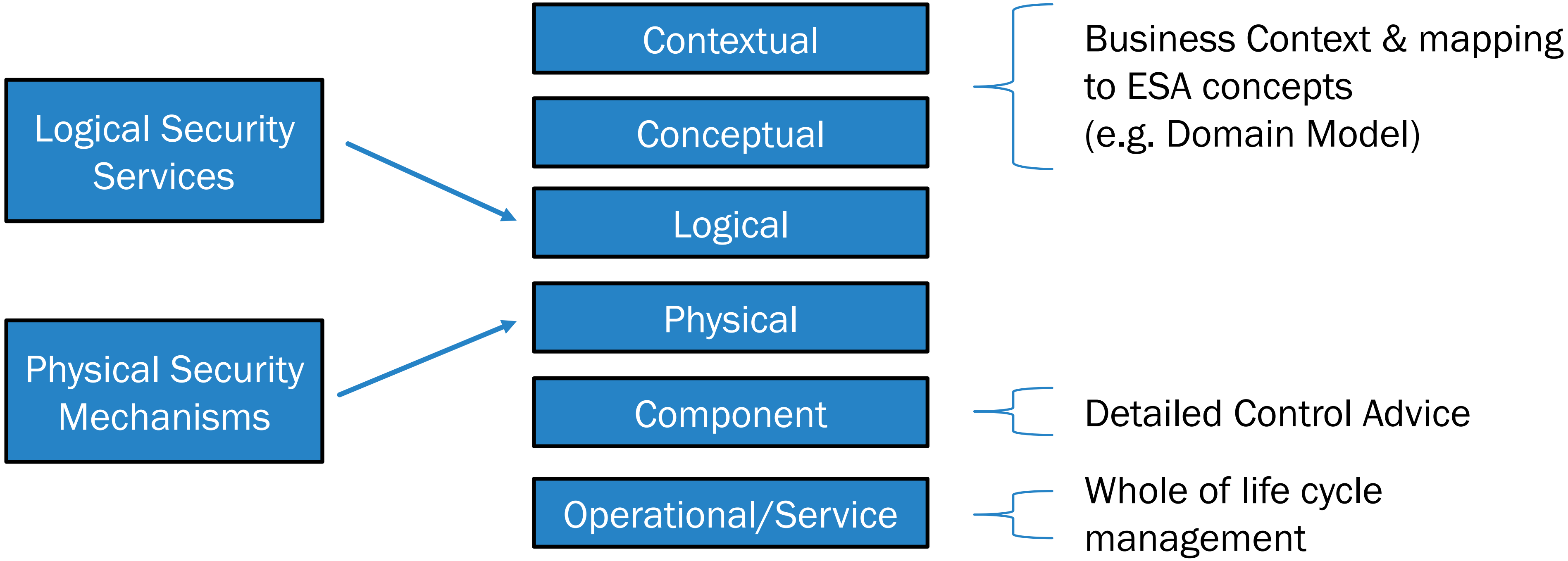
Contextual Security Architecture
Conceptual Security Architecture
Logical Security Architecture
Physical Security Architecture
Component Security Architecture
Security Service Management Architecture

SABSA MATRIX

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)		PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Decisions	Business Risk	Business Process	The Business View	Business Governance	Business Geography	Business Time Dependence
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Project Assurance	The Architect's View	Roles & Responsibilities	Domain Framework	Time Management Framework
LOGICAL ARCHITECURE	Information Assets	Risk Management Policies	Process Maps & Services	The Designer's View	Entity & Trust Framework	Domain Maps	Calendar & Timetable
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	The Builder's View	Human Interface	ICT Infrastructure	Process Schedule
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	The Tradesman's View	Personnel Mgmt, Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
SERVICE MGMT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	The Service Manager's View	Personnel Management	Management of Environment	Time & Performance Management

https://sabsa.org/white-paper-requests/

WHY 6 LAYERS?


Logical Security Services
Physical Security Mechanisms
Contextual
Conceptual
Logical
Physical
Component
Operational/Service
Business Context & mapping to ESA concepts (e.g. Domain Model)
Detailed Control Advice
Whole of life cycle management

SABSA MATRIX (CONT.)

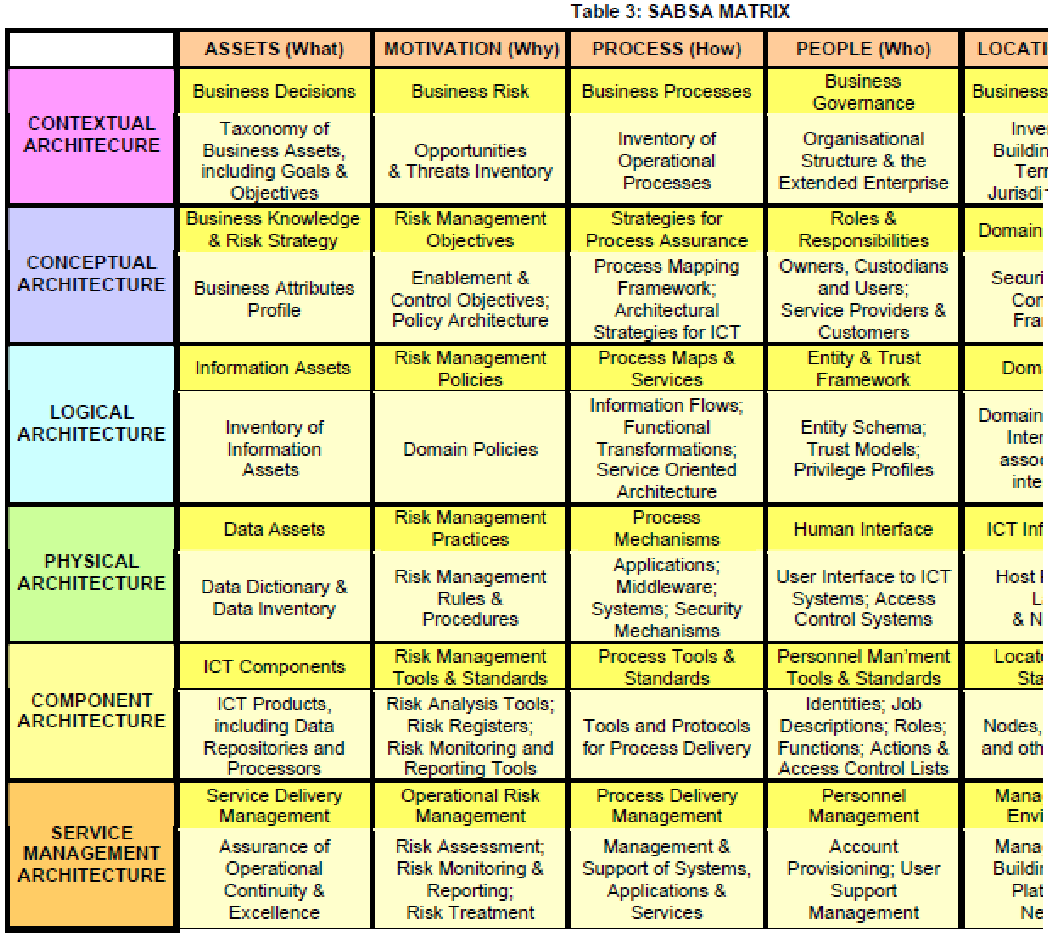


Table 3: SABSA MATRIX

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdi	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain	
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Securi Cor Fra	
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Dom	
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Inter asso inte	
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Inf	
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host I L & N	
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment Tools & Standards	Locat Sta	
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, and oth	
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Mana Envi	
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Mana Buildi Plat Ne	

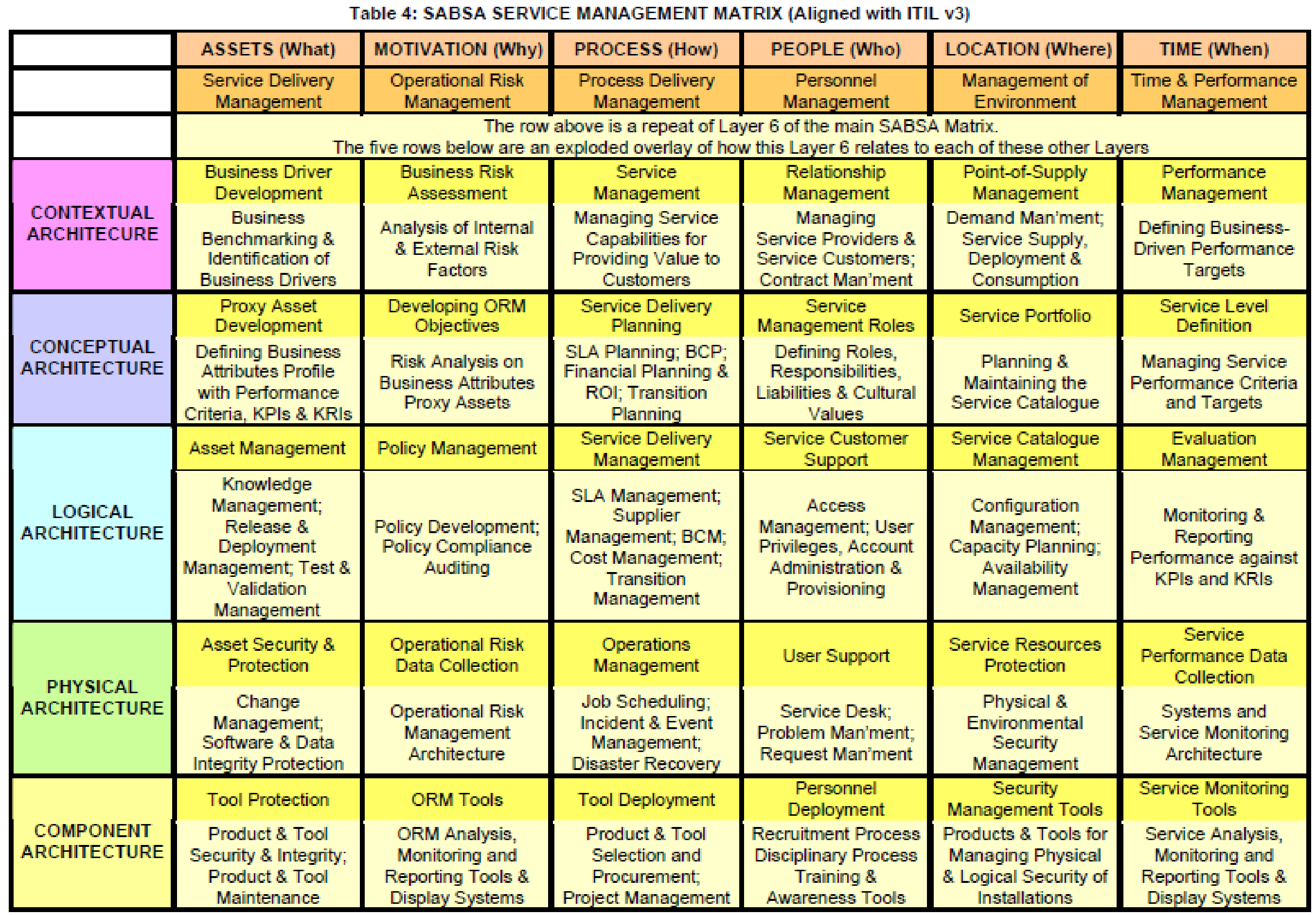
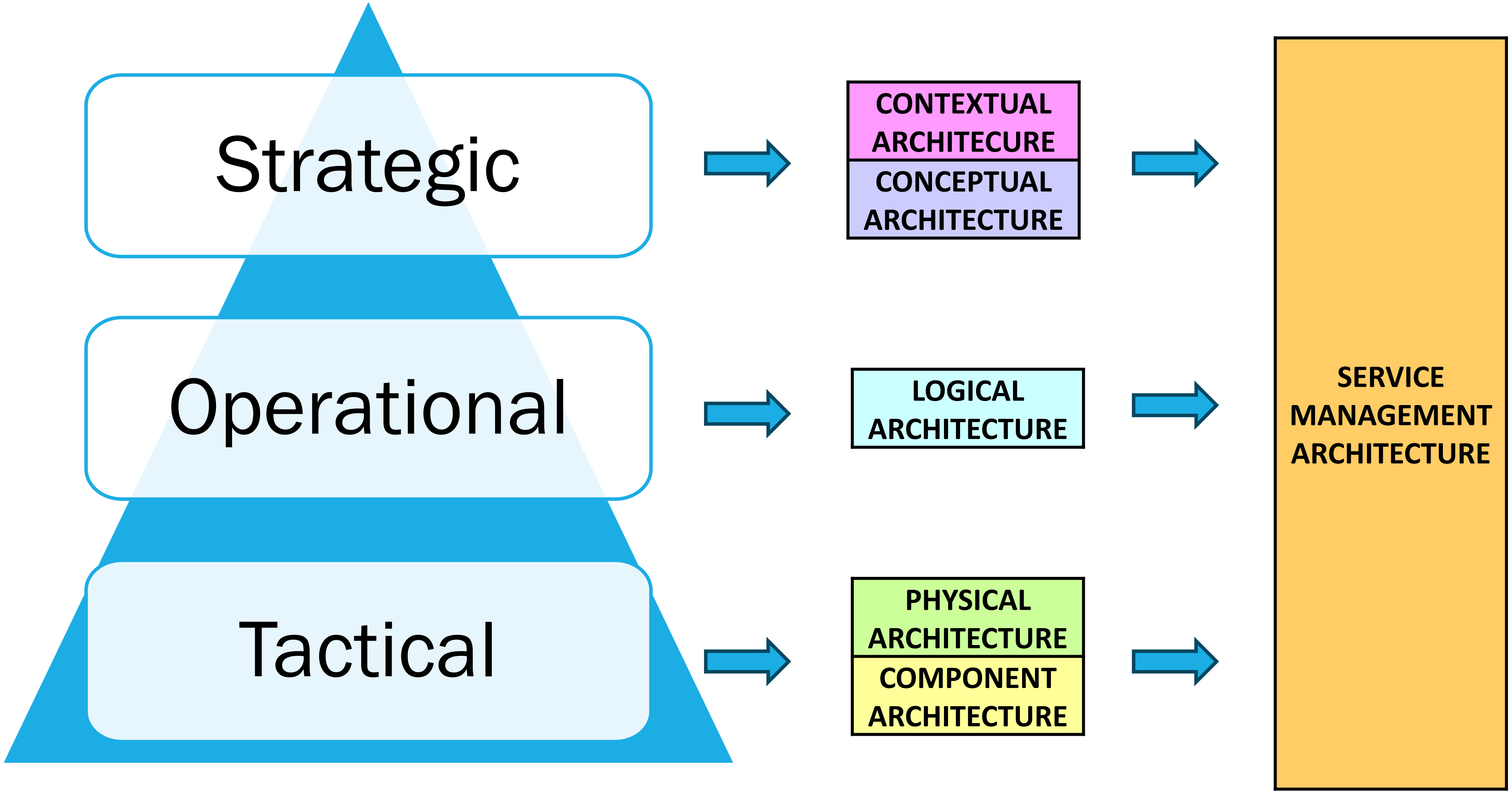


Table 4: SABSA SERVICE MANAGEMENT MATRIX (Aligned with ITIL v3)

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	The row above is a repeat of Layer 6 of the main SABSA Matrix. The five rows below are an exploded overlay of how this Layer 6 relates to each of these other Layers					
CONTEXTUAL ARCHITECURE	Business Driver Development	Business Risk Assessment	Service Management	Relationship Management	Point-of-Supply Management	Performance Management
	Business Benchmarking & Identification of Business Drivers	Analysis of Internal & External Risk Factors	Managing Service Capabilities for Providing Value to Customers	Managing Service Providers & Service Customers; Contract Man'ment	Demand Man'ment; Service Supply, Deployment & Consumption	Defining Business-Driven Performance Targets
CONCEPTUAL ARCHITECTURE	Proxy Asset Development	Developing ORM Objectives	Service Delivery Planning	Service Management Roles	Service Portfolio	Service Level Definition
	Defining Business Attributes Profile with Performance Criteria, KPIs & KRIs	Risk Analysis on Business Attributes Proxy Assets	SLA Planning; BCP; Financial Planning & ROI; Transition Planning	Defining Roles, Responsibilities, Liabilities & Cultural Values	Planning & Maintaining the Service Catalogue	Managing Service Performance Criteria and Targets
LOGICAL ARCHITECTURE	Asset Management	Policy Management	Service Delivery Management	Service Customer Support	Service Catalogue Management	Evaluation Management
	Knowledge Management; Release & Deployment Management; Test & Validation Management	Policy Development; Policy Compliance Auditing	SLA Management; Supplier Management; BCM; Cost Management; Transition Management	Access Management; User Privileges, Account Administration & Provisioning	Configuration Management; Capacity Planning; Availability Management	Monitoring & Reporting Performance against KPIs and KRIs
PHYSICAL ARCHITECTURE	Asset Security & Protection	Operational Risk Data Collection	Operations Management	User Support	Service Resources Protection	Service Performance Data Collection
	Change Management; Software & Data Integrity Protection	Operational Risk Management Architecture	Job Scheduling; Incident & Event Management; Disaster Recovery	Service Desk; Problem Man'ment; Request Man'ment	Physical & Environmental Security Management	Systems and Service Monitoring Architecture
COMPONENT ARCHITECTURE	Tool Protection	ORM Tools	Tool Deployment	Personnel Deployment	Security Management Tools	Service Monitoring Tools
	Product & Tool Security & Integrity; Product & Tool Maintenance	ORM Analysis, Monitoring and Reporting Tools & Display Systems	Product & Tool Selection and Procurement; Project Management	Recruitment Process Disciplinary Process Training & Awareness Tools	Products & Tools for Managing Physical & Logical Security of Installations	Service Analysis, Monitoring and Reporting Tools & Display Systems

ALIGNING TO SABSA

ALIGNING THE TIERS OF CTI AND THE SABSA MATRIX



Strategic

Operational

Tactical

CONTEXTUAL ARCHITECURE

CONCEPTUAL ARCHITECTURE

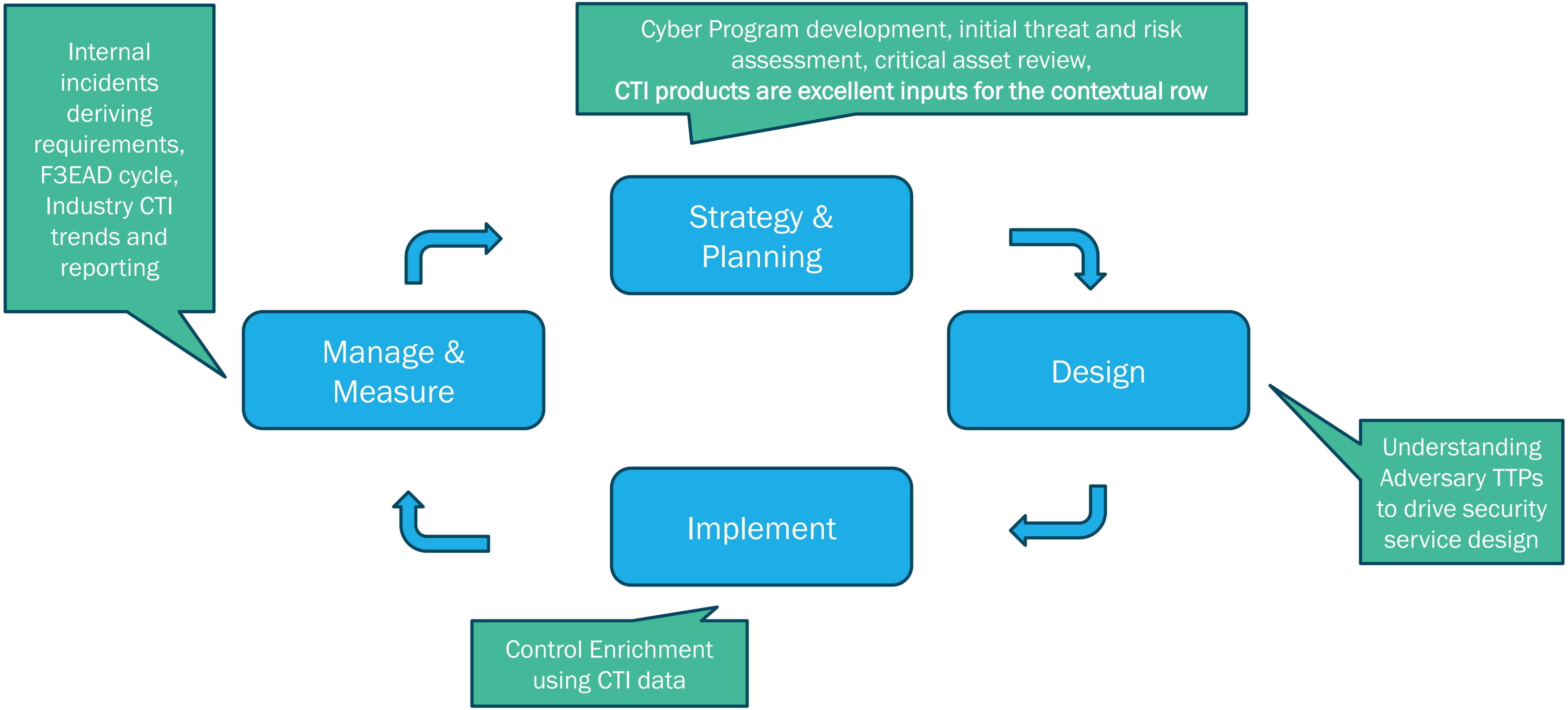
LOGICAL ARCHITECTURE

PHYSICAL ARCHITECTURE

COMPONENT ARCHITECTURE

SERVICE MANAGEMENT ARCHITECTURE

WHERE DOES CTI INTEGRATE IN THE SABSA LIFE CYCLE?



Cyber Program development, initial threat and risk assessment, critical asset review,
CTI products are excellent inputs for the contextual row

Strategy & Planning

Design

Understanding Adversary TTPs to drive security service design

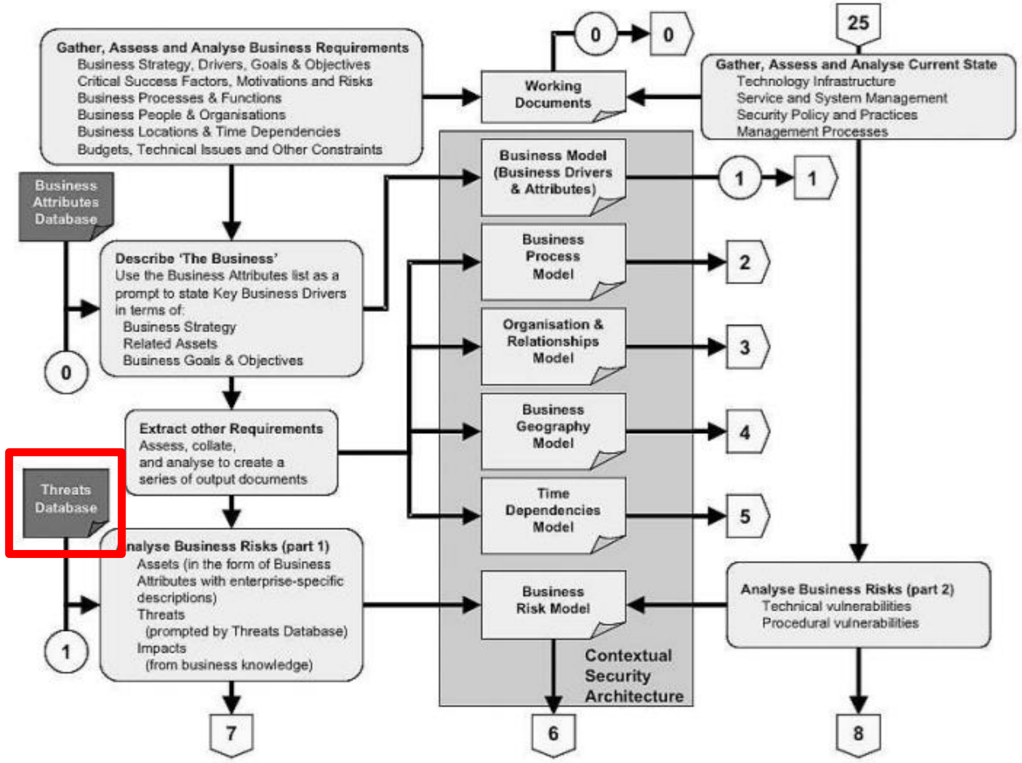
Implement

Control Enrichment using CTI data

Manage & Measure

Internal incidents deriving requirements, F3EAD cycle, Industry CTI trends and reporting

WHERE DOES CTI MAP TO THE BLUE BOOK PROCESSES



Gather, Assess and Analyse Business Requirements
Business Strategy, Drivers, Goals & Objectives
Critical Success Factors, Motivations and Risks
Business Processes & Functions
Business People & Organisations
Business Locations & Time Dependencies
Budgets, Technical Issues and Other Constraints

Working Documents

Gather, Assess and Analyse Current State
Technology Infrastructure
Service and System Management
Security Policy and Practices
Management Processes

Business Attributes Database

Describe 'The Business'
Use the Business Attributes list as a prompt to state Key Business Drivers in terms of:
Business Strategy
Related Assets
Business Goals & Objectives

Extract other Requirements
Assess, collate, and analyse to create a series of output documents

Threats Database

nalyse Business Risks (part 1)
Assets (in the form of Business Attributes with enterprise-specific descriptions)
Threats
(prompted by Threats Database)
Impacts
(from business knowledge)

Business Model (Business Drivers & Attributes)

Business Process Model

Organisation & Relationships Model

Business Geography Model

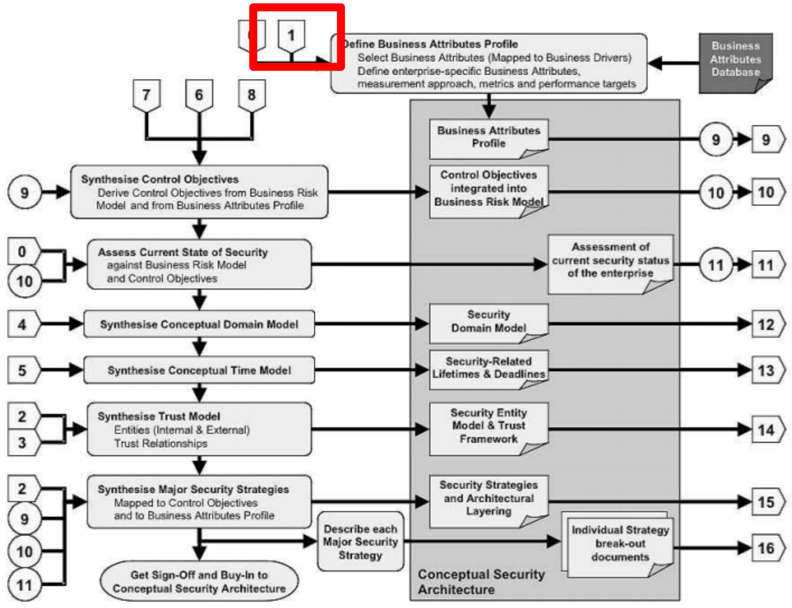
Time Dependencies Model

Business Risk Model

Contextual Security Architecture

Analyse Business Risks (part 2)
Technical vulnerabilities
Procedural vulnerabilities

Figure 7-4: Developing the Contextual Security Architecture



Define Business Attributes Profile
Select Business Attributes (Mapped to Business Drivers)
Define enterprise-specific Business Attributes, measurement approach, metrics and performance targets

Business Attributes Database

Synthesise Control Objectives
Derive Control Objectives from Business Risk Model and from Business Attributes Profile

Assess Current State of Security
against Business Risk Model
and Control Objectives

Synthesise Conceptual Domain Model

Synthesise Conceptual Time Model

Synthesise Trust Model
Entities (Internal & External)
Trust Relationships

Synthesise Major Security Strategies
Mapped to Control Objectives
and to Business Attributes Profile

Describe each Major Security Strategy

Get Sign-Off and Buy-In to Conceptual Security Architecture

Business Attributes Profile

Control Objectives integrated into Business Risk Model

Assessment of current security status of the enterprise

Security Domain Model

Security-Related Lifetimes & Deadlines

Security Entity Model & Trust Framework

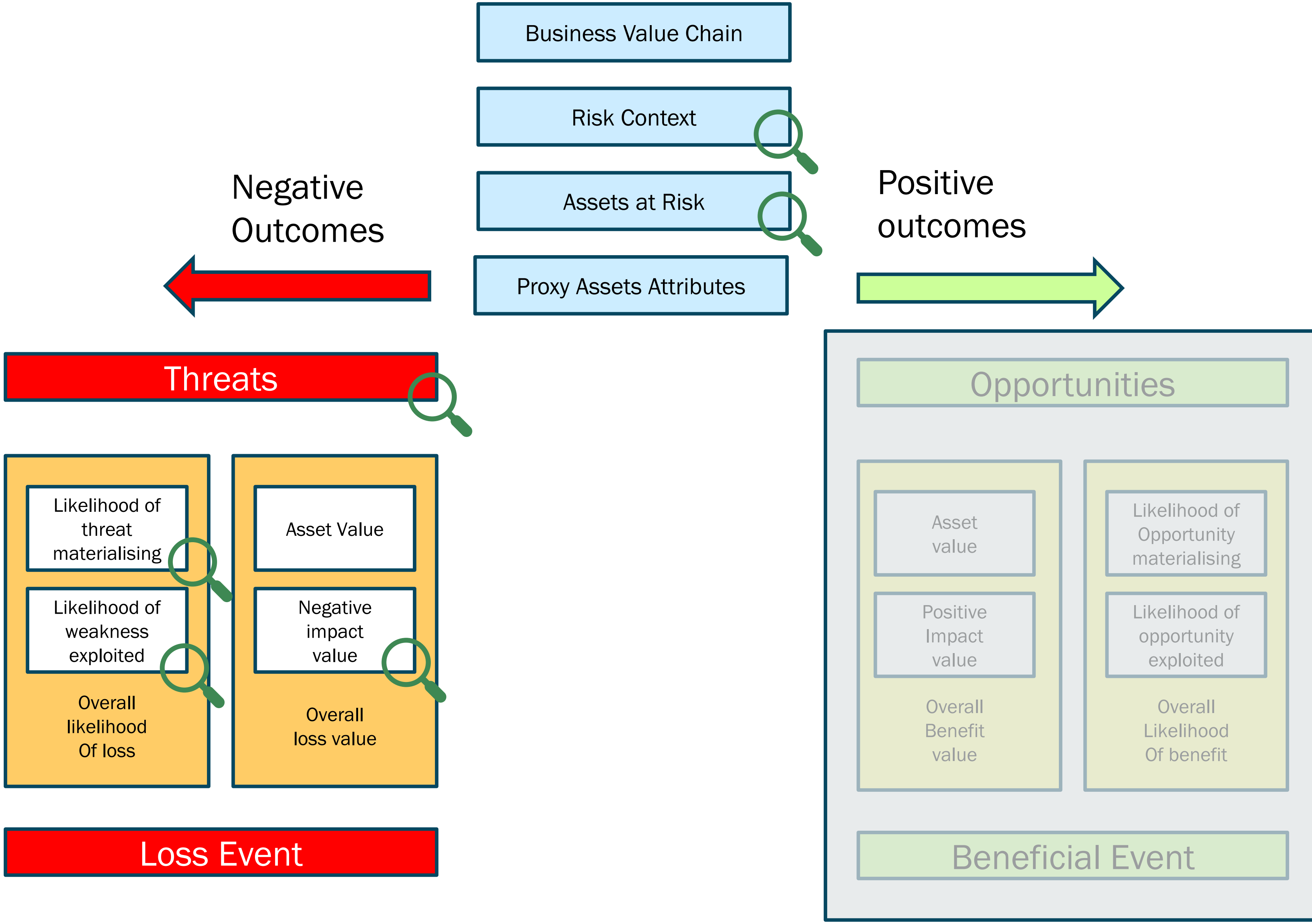
Security Strategies and Architectural Layering

Individual Strategy break-out documents

Conceptual Security Architecture

Figure 7-5: Developing the Conceptual Security Architecture

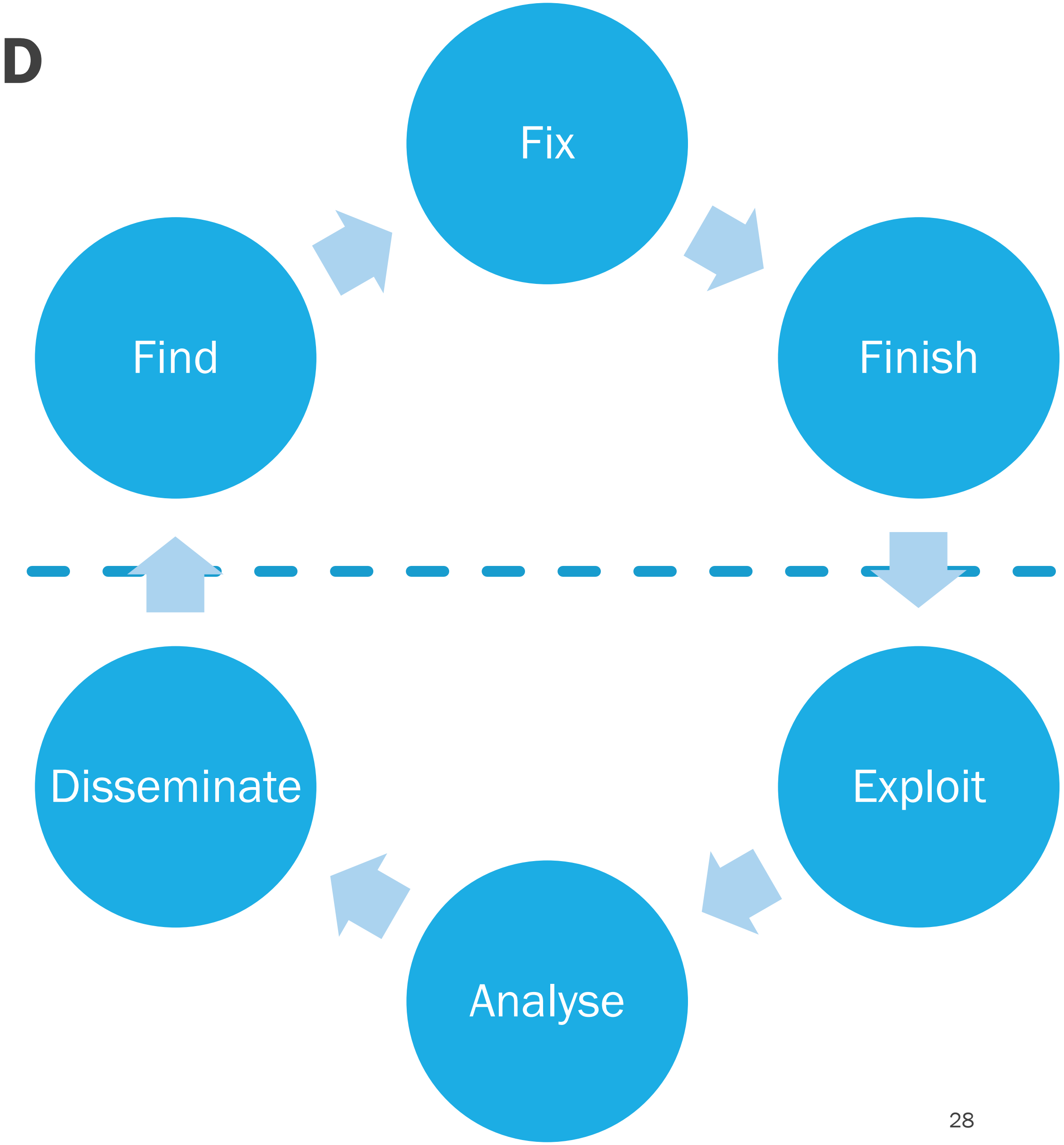
ALIGNING THE CTI LIFECYLE TO THE SABSA RMP



HOW ARCHITECTS ALIGN WITH F3EAD

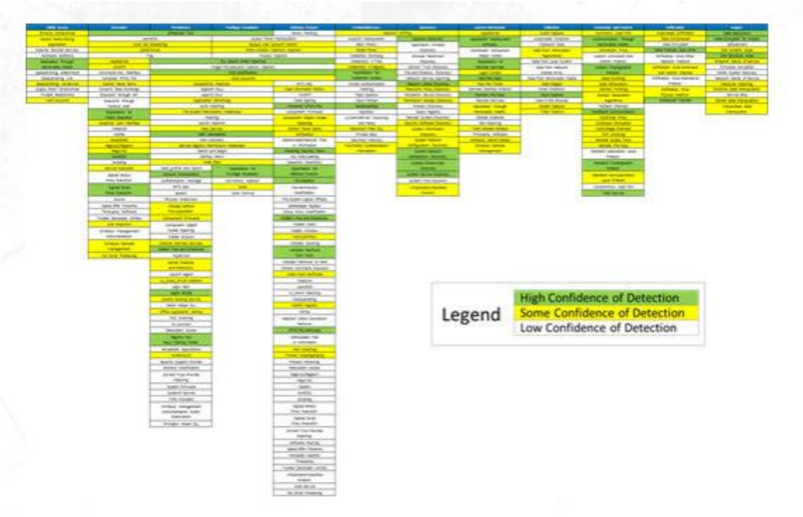
- Architects must develop Logical Services and Physical Mechanisms that support cyber security Incident Response

- Architects must use the Cyber Threat Intelligence Products of the Enterprise to ensure that they are aware of current state of the threat landscape
- Architects should be involved in the Cyber Threat Intelligence Development activities in the Enterprise
- Architects should be involved in Lessons Learnt following any cyber security incidents to understand control failure(s)



ALIGNING CTI AND MTCS

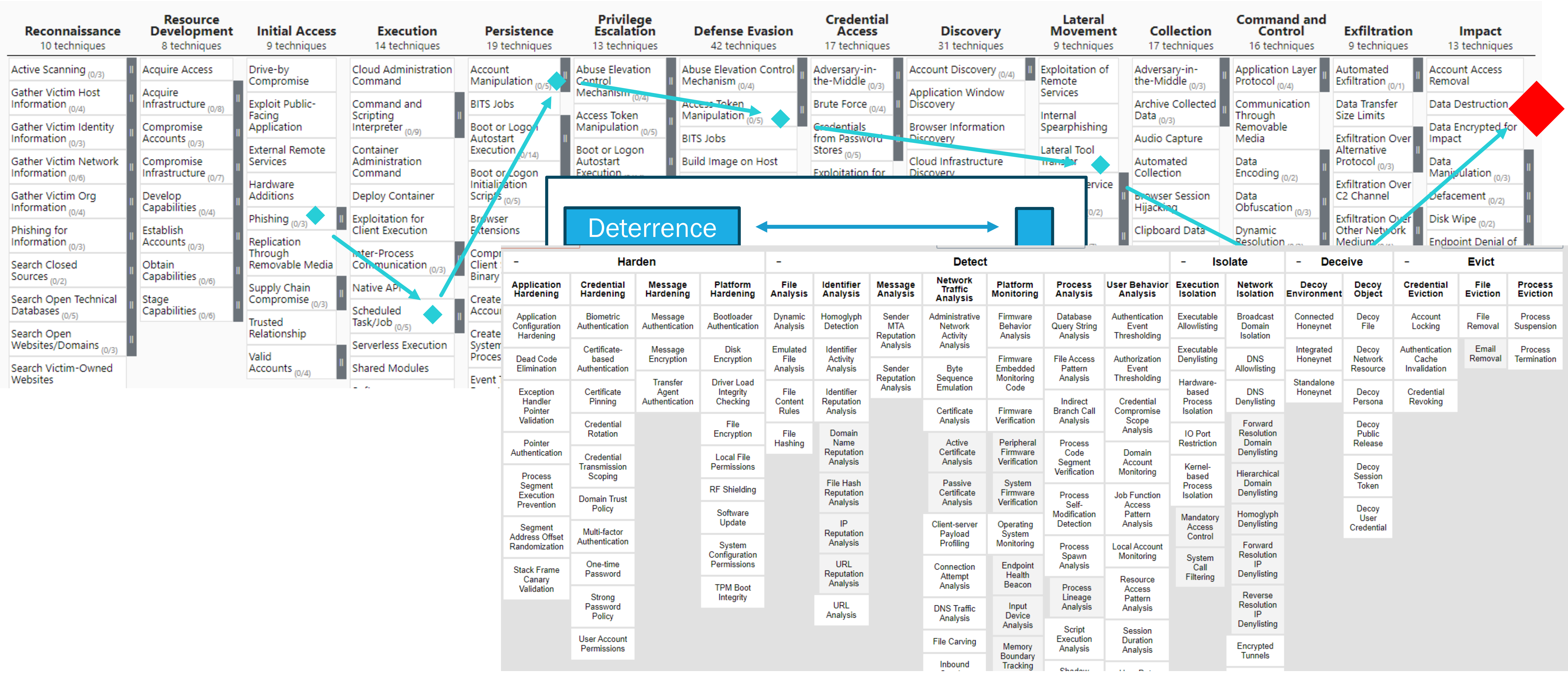
- Consider attack paths or CoA (most likely and most dangerous)
- Do you have Defense-in-Depth (e.g. a mix of Multi-Tiered Control Strategy across the kill chain)?
- An opportunity for a project to map MITRE D3FEND (https://d3fend.mitre.org/) to SABSA?


Legend
High Confidence of Detection
Some Confidence of Detection
Low Confidence of Detection

SAMPLE FOR WHAT A FINAL ASSESSMENT MIGHT LOOK LIKE

Ref - https://www.mitre.org/sites/default/files/2021-11/getting-started-with-attack-october-2019.pdf

ALIGNING CTI AND MTCS (CONT.)



Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 9 techniques	Execution 14 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 31 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/3)	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Exploit Public-Facing Application	Command and Scripting Interpreter (0/9)	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Accounts (0/3)	External Remote Services	Container Administration Command	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution	BITS Jobs	Credentials from Password Stores (0/5)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/7)	Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (0/5)		Build Image on Host	Exploitation for	Cloud Infrastructure Discovery	ervice	Automated Collection	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Phishing (0/3)	Exploitation for Client Execution	Browser Extensions					(0/2)	Browser Session Hijacking	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement (0/2)
Phishing for Information (0/3)	Establish Accounts (0/3)	Replication Through Removable Media	ter-Process Communication (0/3)	Compr Client Binary						Clipboard Data			Disk Wipe (0/2)
Search Closed Sources (0/2)	Obtain Capabilities (0/6)	Supply Chain Compromise (0/3)	Native API	Create Accou									Endpoint Denial of
Search Open Technical Databases (0/5)	Stage Capabilities (0/6)	Trusted Relationship	Scheduled Task/Job (0/5)	Create System Proces									
Search Open Websites/Domains (0/3)		Valid Accounts (0/4)	Serverless Execution	Event									
Search Victim-Owned Websites			Shared Modules										

Deterrence

Harden				Detect							Isolate		Deceive		Evict		
Application Hardening	Credential Hardening	Message Hardening	Platform Hardening	File Analysis	Identifier Analysis	Message Analysis	Network Traffic Analysis	Platform Monitoring	Process Analysis	User Behavior Analysis	Execution Isolation	Network Isolation	Decoy Environment	Decoy Object	Credential Eviction	File Eviction	Process Eviction
Application Configuration Hardening	Biometric Authentication	Message Authentication	Bootloader Authentication	Dynamic Analysis	Homoglyph Detection	Sender MTA Reputation Analysis	Administrative Network Activity Analysis	Firmware Behavior Analysis	Database Query String Analysis	Authentication Event Thresholding	Executable Allowlisting	Broadcast Domain Isolation	Connected Honeynet	Decoy File	Account Locking	File Removal	Process Suspension
Dead Code Elimination	Certificate-based Authentication	Message Encryption	Disk Encryption	Emulated File Analysis	Identifier Activity Analysis	Sender Reputation Analysis	Byte Sequence Emulation	Firmware Embedded Monitoring Code	File Access Pattern Analysis	Authorization Event Thresholding	Executable Denylisting	DNS Allowlisting	Integrated Honeynet	Decoy Network Resource	Authentication Cache Invalidation	Email Removal	Process Termination
Exception Handler Pointer Validation	Certificate Pinning	Transfer Agent Authentication	Driver Load Integrity Checking	File Content Rules	Identifier Reputation Analysis		Certificate Analysis	Firmware Verification	Indirect Branch Call Analysis	Credential Compromise Scope Analysis	Hardware-based Process Isolation	DNS Denylisting	Standalone Honeynet	Decoy Persona	Credential Revoking		
Pointer Authentication	Credential Rotation		File Encryption	File Hashing	Domain Name Reputation Analysis		Active Certificate Analysis	Peripheral Firmware Verification	Process Code Segment Verification	Domain Account Monitoring	IO Port Restriction	Forward Resolution Domain Denylisting		Decoy Public Release			
Process Segment Execution Prevention	Credential Transmission Scoping		Local File Permissions		File Hash Reputation Analysis		Passive Certificate Analysis	System Firmware Verification	Process Self-Modification Detection	Job Function Access Pattern Analysis	Kernel-based Process Isolation	Hierarchical Domain Denylisting		Decoy Session Token			
Segment Address Offset Randomization	Domain Trust Policy		RF Shielding		IP Reputation Analysis		Client-server Payload Profiling	Operating System Monitoring	Process Spawn Analysis	Local Account Monitoring	Mandatory Access Control	Homoglyph Denylisting		Decoy User Credential			
Stack Frame Canary Validation	Multi-factor Authentication		Software Update		URL Reputation Analysis		Connection Attempt Analysis	Endpoint Health Beacon	Process Lineage Analysis	Resource Access Pattern Analysis	System Call Filtering	Forward Resolution IP Denylisting					
	One-time Password		System Configuration Permissions		URL Analysis		DNS Traffic Analysis	Input Device Analysis	Script Execution Analysis	Session Duration Analysis		Reverse Resolution IP Denylisting					
	Strong Password Policy		TPM Boot Integrity				File Carving	Memory Boundary Tracking				Encrypted Tunnels					
	User Account Permissions						Inbound										

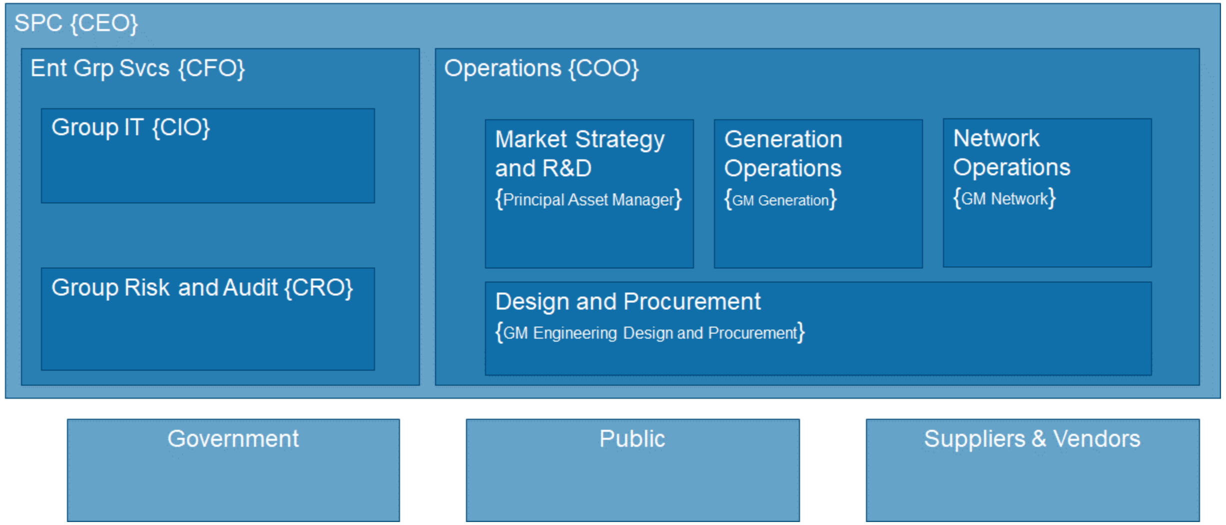
Ref - https://mitre-attack.github.io/attack-navigator/ & https://d3fend.mitre.org/ & SABSA MTCS

WORKED EXAMPLE

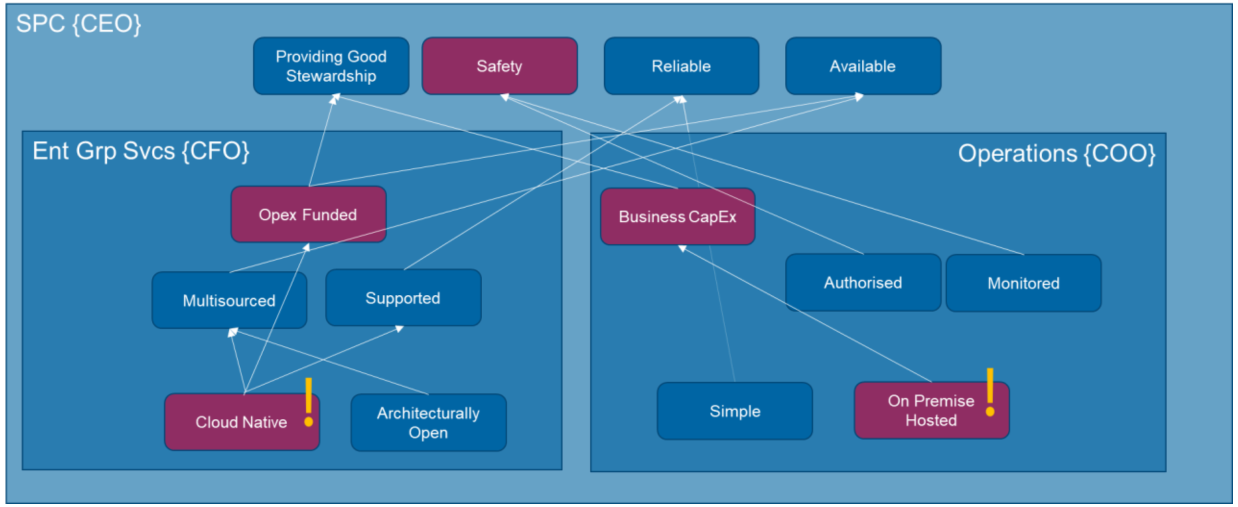
STATE POWER CORPORATION (SPC)

BACKGROUND CONTEXT OF THE STATE POWER CORPORATION

- *State Power Corporation* (SPC) owns, operates and maintains the electricity generation, transmission and distribution assets for the state
- There has been a recent cyber security incident in it's electricity generation portfolio and the organisation is looking to conduct a root cause analysis to prevent a similar incident in it's other assets
- SPC has an inflight Digital Transformation program that is delivering change in both the IT and OT environments
- We have been engaged by the SPC Group CISO to articulate the Enterprise Conceptual Security Architecture and to inform their 5 year Security Management program



SPC {CEO}
Ent Grp Svcs {CFO}
Group IT {CIO}
Group Risk and Audit {CRO}
Operations {COO}
Market Strategy and R&D {Principal Asset Manager}
Generation Operations {GM Generation}
Network Operations {GM Network}
Design and Procurement {GM Engineering Design and Procurement}
Government
Public
Suppliers & Vendors

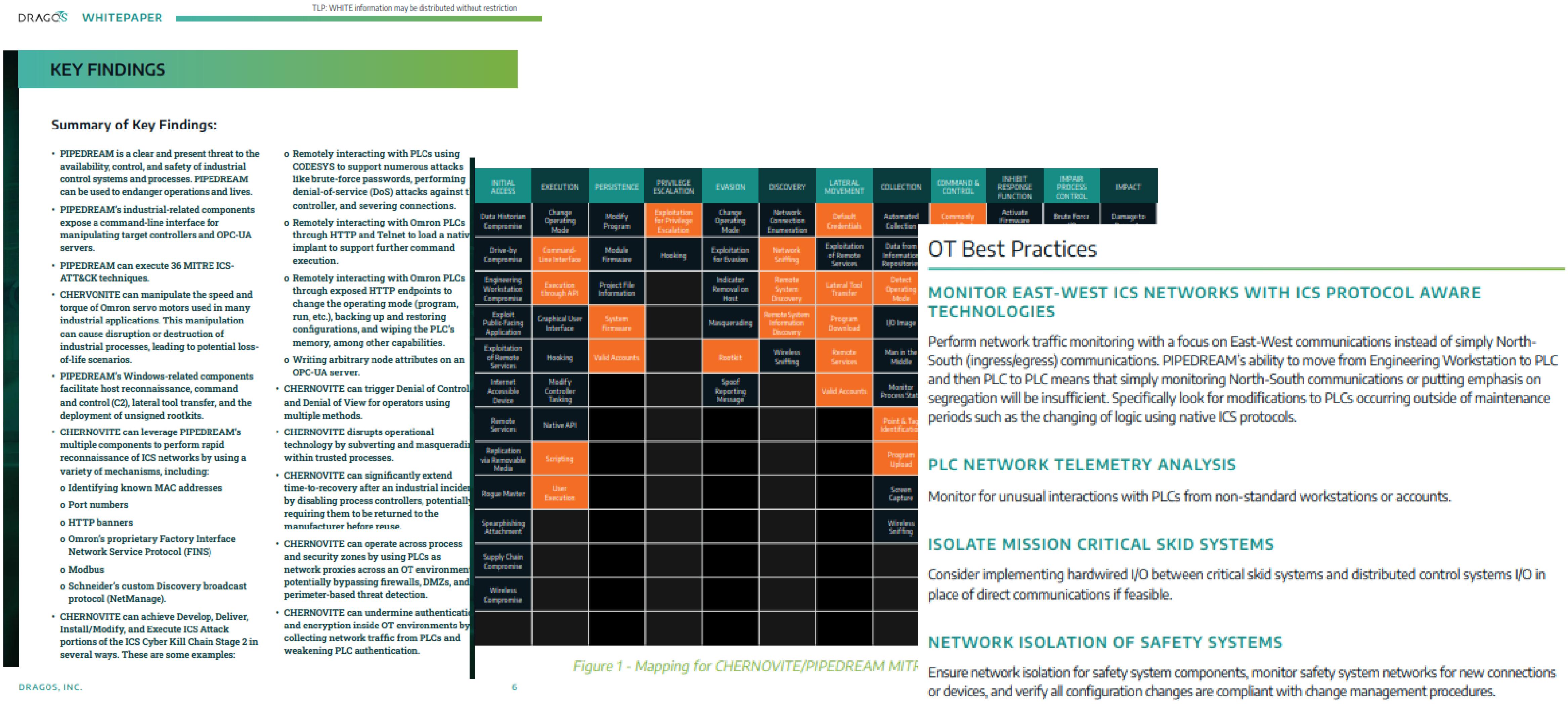


SCENARIO BACKGROUND

- The State Power Corporation (SPC) have learnt of the recently discovered PIPEDREAM Malware# and the Audit and Risk Committee have asked the group CISO for a strategic risk assessment on the issue
- The SPC Group CISO has asked the Cyber Threat Intelligence (CTI) team to see whether it is a credible threat for SPC
- The CTI team has engaged with the Enterprise Security Architecture team for support on the current state of the cyber security architecture at SPC

# https://hub.dragos.com/whitepaper/chernovite-pipedream

QUICK SUMMARY OF PIPEDREAM



DRAGOS WHITEPAPER

TLP: WHITE information may be distributed without restriction

KEY FINDINGS

Summary of Key Findings:

- PIPEDREAM is a clear and present threat to the availability, control, and safety of industrial control systems and processes. PIPEDREAM can be used to endanger operations and lives.
- PIPEDREAM's industrial-related components expose a command-line interface for manipulating target controllers and OPC-UA servers.
- PIPEDREAM can execute 36 MITRE ICS-ATT&CK techniques.
- CHERVONITE can manipulate the speed and torque of Omron servo motors used in many industrial applications. This manipulation can cause disruption or destruction of industrial processes, leading to potential loss-of-life scenarios.
- PIPEDREAM's Windows-related components facilitate host reconnaissance, command and control (C2), lateral tool transfer, and the deployment of unsigned rootkits.
- CHERNOVITE can leverage PIPEDREAM's multiple components to perform rapid reconnaissance of ICS networks by using a variety of mechanisms, including:
  - o Identifying known MAC addresses
  - o Port numbers
  - o HTTP banners
  - o Omron's proprietary Factory Interface Network Service Protocol (FINS)
  - o Modbus
  - o Schneider's custom Discovery broadcast protocol (NetManage).
- CHERNOVITE can achieve Develop, Deliver, Install/Modify, and Execute ICS Attack portions of the ICS Cyber Kill Chain Stage 2 in several ways. These are some examples:
  - o Remotely interacting with PLCs using CODESYS to support numerous attacks like brute-force passwords, performing denial-of-service (DoS) attacks against t controller, and severing connections.
  - o Remotely interacting with Omron PLCs through HTTP and Telnet to load a nativ implant to support further command execution.
  - o Remotely interacting with Omron PLCs through exposed HTTP endpoints to change the operating mode (program, run, etc.), backing up and restoring configurations, and wiping the PLC's memory, among other capabilities.
  - o Writing arbitrary node attributes on an OPC-UA server.
- CHERNOVITE can trigger Denial of Control and Denial of View for operators using multiple methods.
- CHERNOVITE disrupts operational technology by subverting and masqueradi within trusted processes.
- CHERNOVITE can significantly extend time-to-recovery after an industrial incider by disabling process controllers, potentially requiring them to be returned to the manufacturer before reuse.
- CHERNOVITE can operate across process and security zones by using PLCs as network proxies across an OT environmen potentially bypassing firewalls, DMZs, and perimeter-based threat detection.
- CHERNOVITE can undermine authenticati and encryption inside OT environments by collecting network traffic from PLCs and weakening PLC authentication.

DRAGOS, INC. 6

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND & CONTROL	INHIBIT RESPONSE FUNCTION	IMPAIR PROCESS CONTROL	IMPACT
Data Historian Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly	Activate Firmware	Brute Force	Damage to
Drive-by Compromise	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositorie				
Engineering Workstation Compromise	Execution through API	Project File Information		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode				
Exploit Public-Facing Application	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image				
Exploitation of Remote Services	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle				
Internet Accessible Device	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process Stat				
Remote Services	Native API						Point & Tag Identificatio				
Replication via Removable Media	Scripting						Program Upload				
Rogue Master	User Execution						Screen Capture				
Spearphishing Attachment							Wireless Sniffing				
Supply Chain Compromise											
Wireless Compromise											

Figure 1 - Mapping for CHERNOVITE/PIPEDREAM MITR

OT Best Practices

MONITOR EAST-WEST ICS NETWORKS WITH ICS PROTOCOL AWARE TECHNOLOGIES

Perform network traffic monitoring with a focus on East-West communications instead of simply North-South (ingress/egress) communications. PIPEDREAM's ability to move from Engineering Workstation to PLC and then PLC to PLC means that simply monitoring North-South communications or putting emphasis on segregation will be insufficient. Specifically look for modifications to PLCs occurring outside of maintenance periods such as the changing of logic using native ICS protocols.

PLC NETWORK TELEMETRY ANALYSIS

Monitor for unusual interactions with PLCs from non-standard workstations or accounts.

ISOLATE MISSION CRITICAL SKID SYSTEMS

Consider implementing hardwired I/O between critical skid systems and distributed control systems I/O in place of direct communications if feasible.

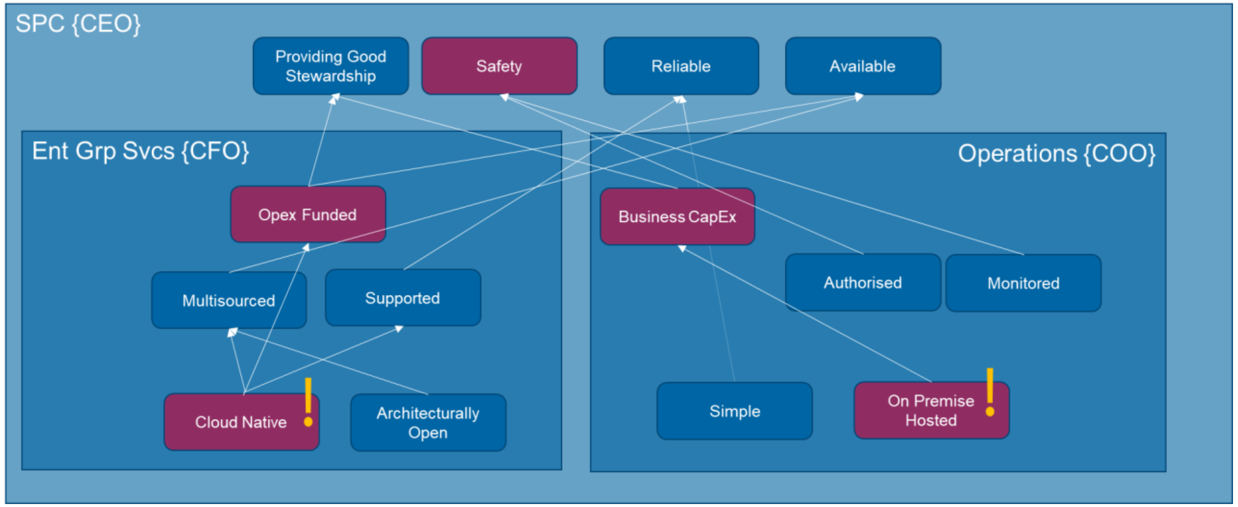
NETWORK ISOLATION OF SAFETY SYSTEMS

Ensure network isolation for safety system components, monitor safety system networks for new connections or devices, and verify all configuration changes are compliant with change management procedures.

Ref - https://hub.dragos.com/whitepaper/chernovite-pipedream

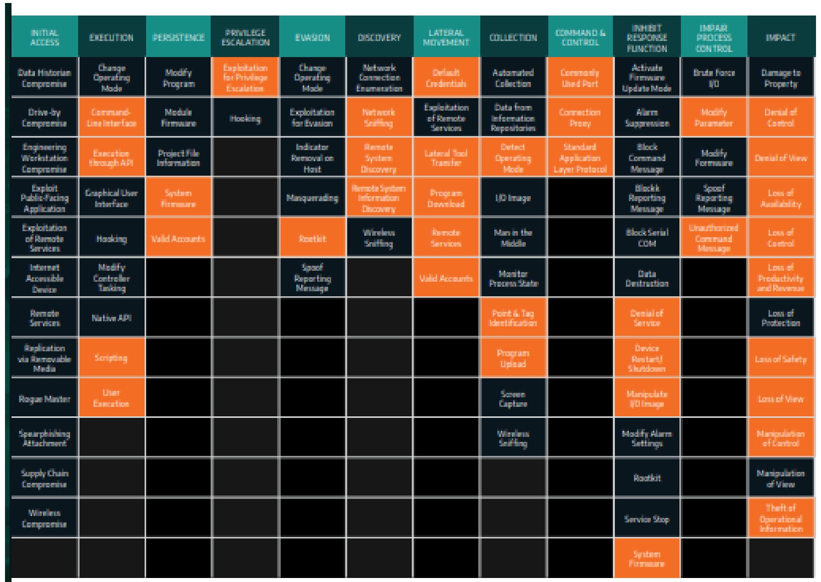
APPROACH TO SCENARIO

- This would be an operational cyber threat intelligence product
- Review and update Threat Profile if appropriate
  - Understand the assets and systems that have been targeted and if they are relevant for SPC e.g. CODESYS PLCs
- Consider impact on attributes taxonomy – a good communication tool for stakeholders for "*so what*"



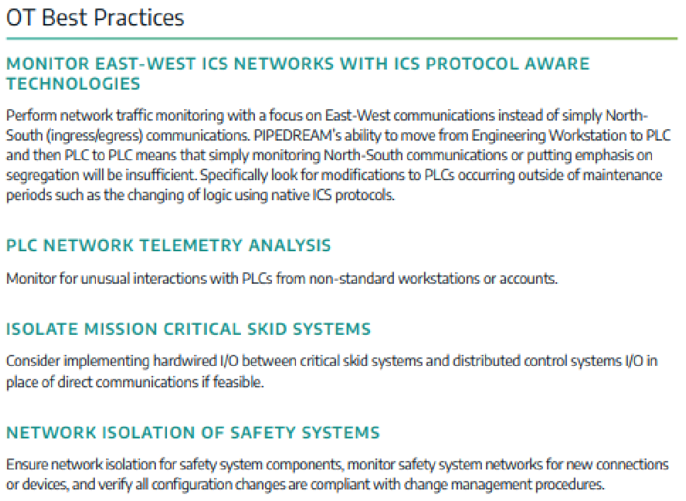
APPROACH TO SCENARIO (CONT.)

- Be informed by the Intelligence Product to determine the attack path and adversary Courses of Action. Consider the coverage of controls for SPC sites
- Consider the security control recommendations from the report, would the report change your security portfolio of works?
- Investigate Enrichment of controls opportunities using Threat Data – Think about the IPCE Indicators and Warnings



INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND & CONTROL	INHIBIT RESPONSE FUNCTION	IMPAIR PROCESS CONTROL	IMPACT
Data Historian Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Engineering Workstation Compromise	Execution through API	Project File Information		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Modify Firmware	Denial of View
Exploit Public-Facing Application	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Exploitation of Remote Services	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
Internet Accessible Device	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Remote Services	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Replication via Removable Media	Scripting						Program Upload		Device Restart/ Shutdown		Loss of Safety
Rogue Master	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Spearphishing Attachment							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Supply Chain Compromise									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

Figure 1 - Mapping for CHERNOVITE/PIPEDREAM MITRE ATT&CK for ICS Techniques



OT Best Practices

MONITOR EAST-WEST ICS NETWORKS WITH ICS PROTOCOL AWARE TECHNOLOGIES

Perform network traffic monitoring with a focus on East-West communications instead of simply North-South (ingress/egress) communications. PIPEDREAM's ability to move from Engineering Workstation to PLC and then PLC to PLC means that simply monitoring North-South communications or putting emphasis on segregation will be insufficient. Specifically look for modifications to PLCs occurring outside of maintenance periods such as the changing of logic using native ICS protocols.

PLC NETWORK TELEMETRY ANALYSIS

Monitor for unusual interactions with PLCs from non-standard workstations or accounts.

ISOLATE MISSION CRITICAL SKID SYSTEMS

Consider implementing hardwired I/O between critical skid systems and distributed control systems I/O in place of direct communications if feasible.

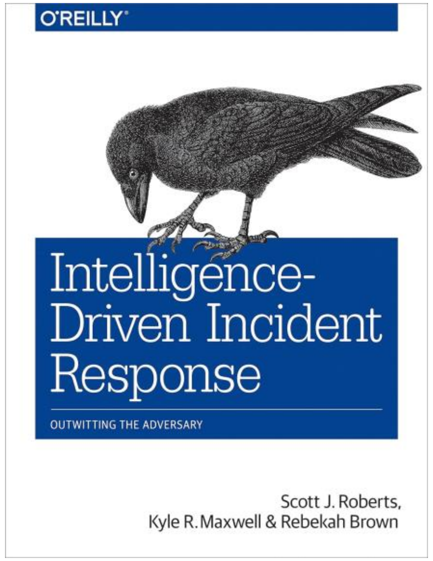
NETWORK ISOLATION OF SAFETY SYSTEMS

Ensure network isolation for safety system components, monitor safety system networks for new connections or devices, and verify all configuration changes are compliant with change management procedures.

FURTHER RESOURCES

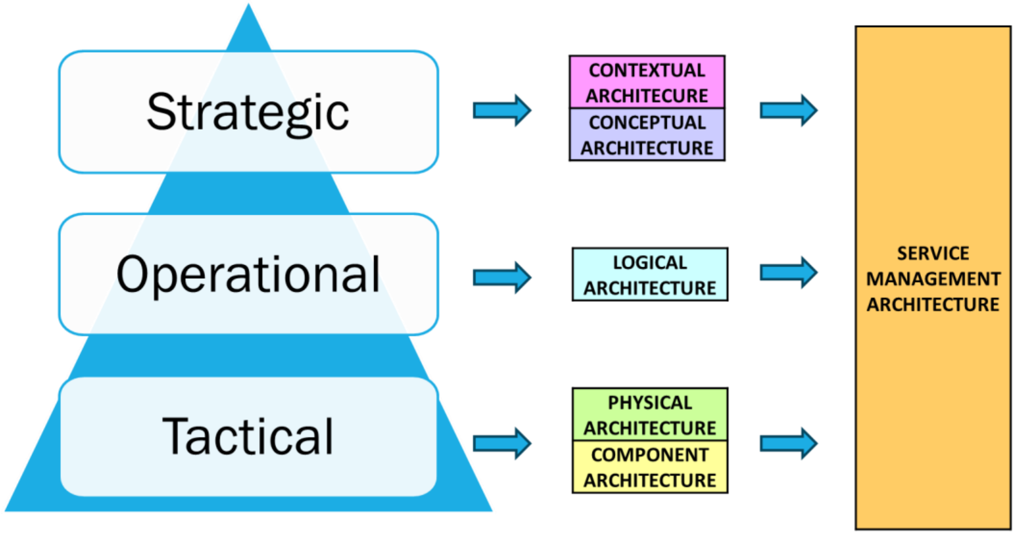
FURTHER RESOURCES

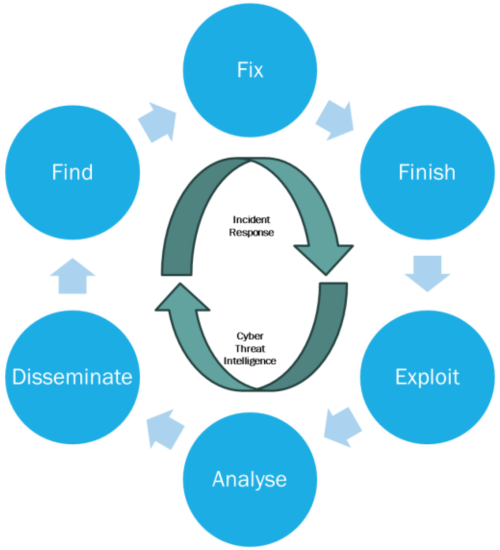
- SABSA White Paper (W100)
- Intelligence Driven Incident Response, Rebekah Brown, Scott J Roberts
- Intelligence Preparation of the Cyber Environment (IPCE): Finding the High Ground in Cyberspace, A Lemay, S Knight, JM Fernandez
- A Top 10 Reading List if you are getting started in Cyber Threat Intelligence, Katie Nickels
- US DoD JP 2-0 and US DoD JP 2-01.3


O'REILLY
Intelligence-Driven Incident Response
OUTWITTING THE ADVERSARY
Scott J. Roberts,
Kyle R. Maxwell & Rebekah Brown

SUMMARY OF PRESENTATION

- Cyber Security architectures cannot be static, they must adjust and evolve to new threats and be threat informed
- Cyber Threat Intelligence requires human analysis, and it is not just a list of IoCs
- Architects must consider Cyber Threat Intelligence products to inform threat assessments for balanced risk management
- Intelligence Preparation of the Operating Environment (IPOE) and Intelligence Preparation of the Cyber Environment (IPCE) are useful tools for architects to understand threat actor Courses of Action (CoA) to inform cyber security architectures





THANK YOU, QUESTIONS?

in https://linkedin.com/in/blargeau

https://github.com/beLarge

𝕏 @beLarge