Egypt’s Digital Cyber Transformation Workshop

Workshop Agenda

Introduction
Egypt's Recent Security Breaches
Global Breaches Report
Kaspersky Threats Realtime Map
Security Services Transformation
Enterprise Security Architecture
Security Solutions Differentiation
Data Centre Security
Integration of People, Process, Technology
Component Security
Security Community Relations
Strategic Research and Development
Quick Wins

Egypt Breaches in 2018 and early 2019

Kaspersky World Threats Heat Map

What a security incident costs

Opportunity

IT incurs significant opportunity costs as a security incident pulls resources away from IT deliverables.

Your business loses productivity and incurs lost sales activity and other revenue-driven opportunity costs.

Reputation

A security incident incurs significant damage to your brand reputation, especially when customer and/or patient records are compromised.

Time

The average security incident lasts 18 days.

A security incident involving malicious insiders averages 45 days.

Money

The cost of the average security incident is $415,748, while the median annualized cost of security breaches is estimated at $5.9M per organization. Costs include legal fees, government fines and penalties.

GLOBAL, TECHNOLOGY

Egypt accounts for 3.97M of global ransomware threats: study

ADELLE GERONIMO
JUNE 24, 2018, 5:01 PM

Egypt continues to face a growing threat from cyber-attacks with malware detections in Q1 of 2018 reaching 253,995, the second highest figure in the North African region.

According to a newly-released report by Trend Micro, the country accounted for 0.23 percent of global ransomware threats, or 3.97 million, in the same period.

Cyber attack hits Careem, compromises 14M users' data

Posted by: **Ahmed Maher** - Apr 23, 2018 at 2:12 PM

A cyber attack on Careem Egypt's databases early this year compromised personal data of 14 millions users and 558 thousand captains, said the ride-hailing service in an emailed statement Monday.

Careem Egypt said the attack affects all accounts created prior to Jan. 14 this year when the company discovered the security breach. All accounts created after that date are considered safe.

20 MARCH, 2018

Egypt among most vulnerable to cyberattacks in African region

Global Ransomware Treats in 2017 stood at 1.7 billion and 0.23% of these threats were seen in Egypt

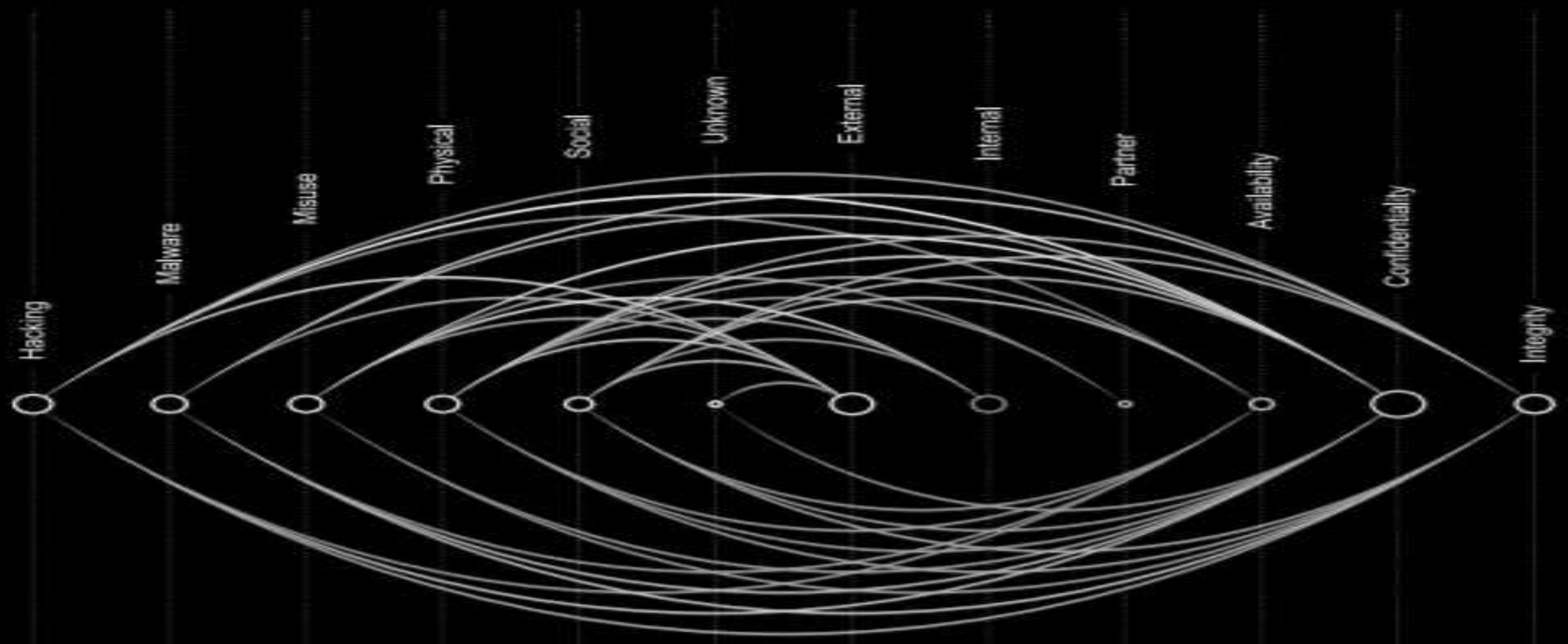
Press Release

Cairo, Egypt: Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, is concerned that Egypt is seeing a sustained rise in threat activity. Based on a newly-released report, the company detected a total of 242,411 malwares in the country in the last quarter of 2017 alone, up by 25% from the third quarter figure of 194,719. This is the third highest malware threats in the African region, with the biggest figure of 2,289,997 malware files coming from South Africa, followed by Morocco's 341,279. The same report revealed that the state's manufacturing sector was the one most affected by malware, followed by education, government, real estate and technology.

Research report

2018 Data Breach Investigations Report

11th edition



verizon

CYBERTHREAT REAL-TIME MAP

EN

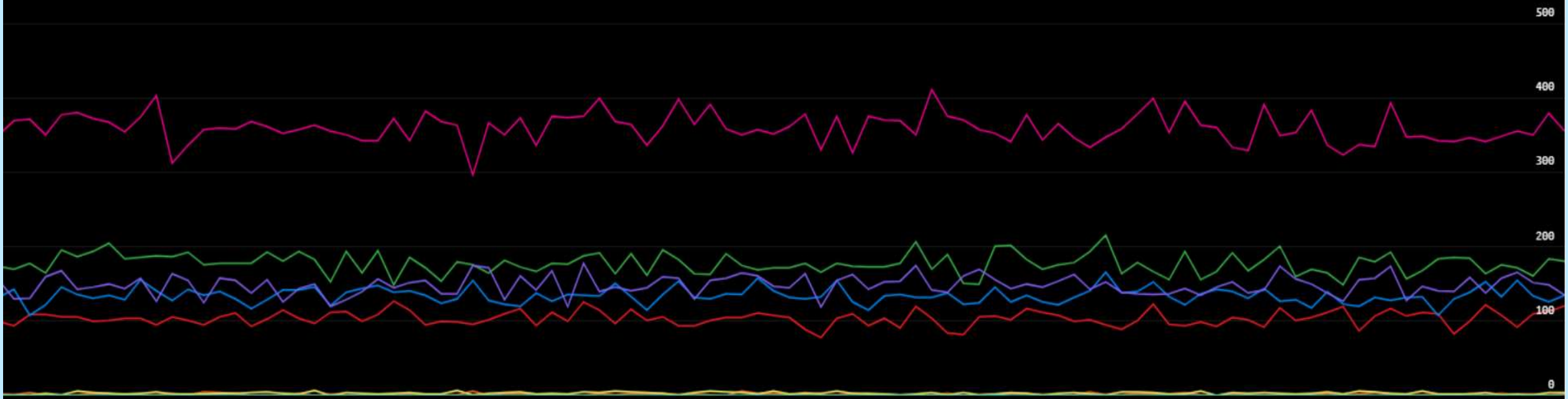
Download Trial

MAP STATISTICS DATA SOURCES BUZZ WIDGET

Share

REAL-TIME

DETECTIONS PER SECOND

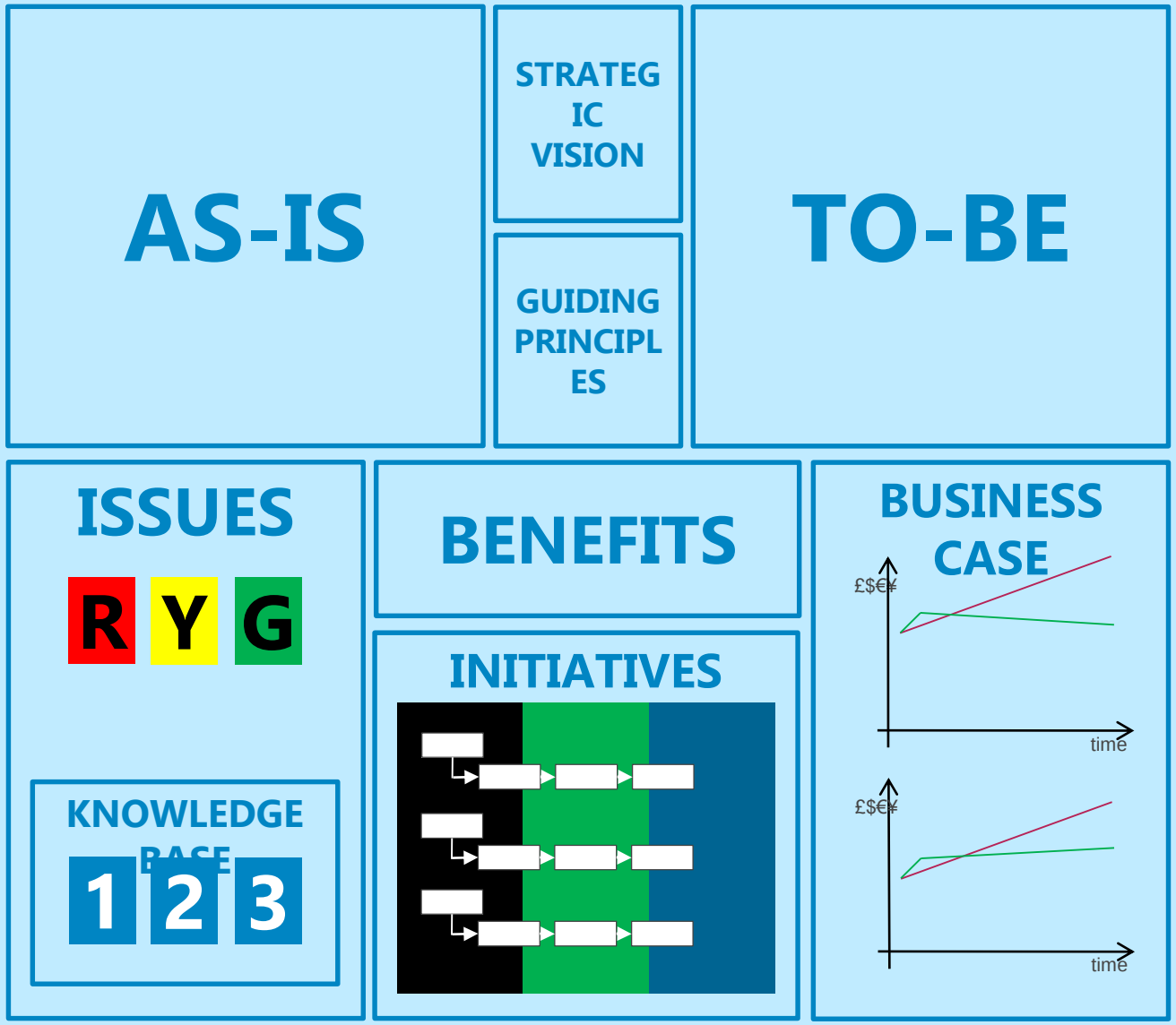


OAS	ODS	MAV	WAV	IDS	VUL	KAS	BAD
12177619	6266743	142270	6570858	22596868	192072	7842478	1070

MOST INFECTED TODAY

Services and Processes Modelling Approach

IT Security Services Transformation Approach



The Architecture Matrix

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
Conceptual	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
Logical	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
Physical	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
Component	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Management Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
Service Management	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management

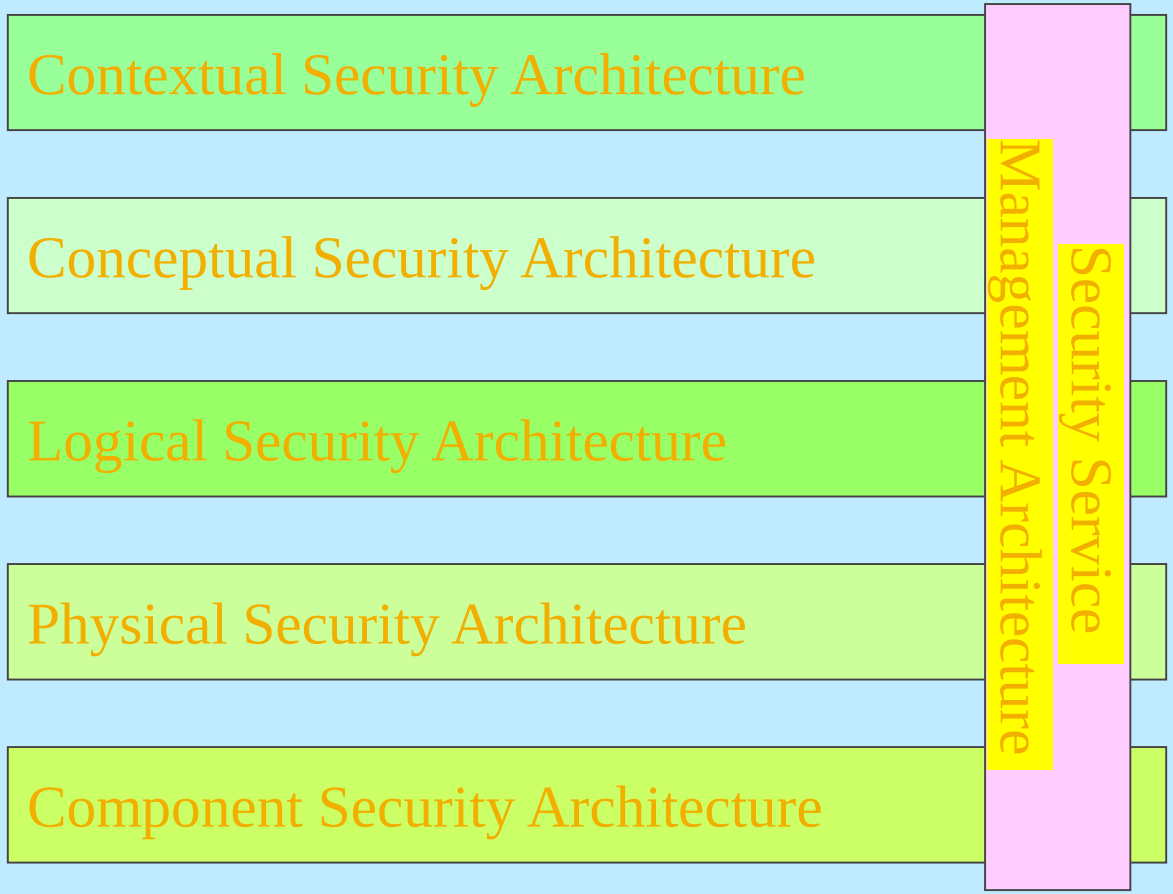
Architecture Strategy & Planning Phase

	Assets (what)	Motivation (why)	Process (how)	People (who)	Location (where)	Time (when)
Contextual	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, Jurisdictions etc.	Time Dependencies of Business Objectives
Conceptual	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians & Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-life Risk Management Framework

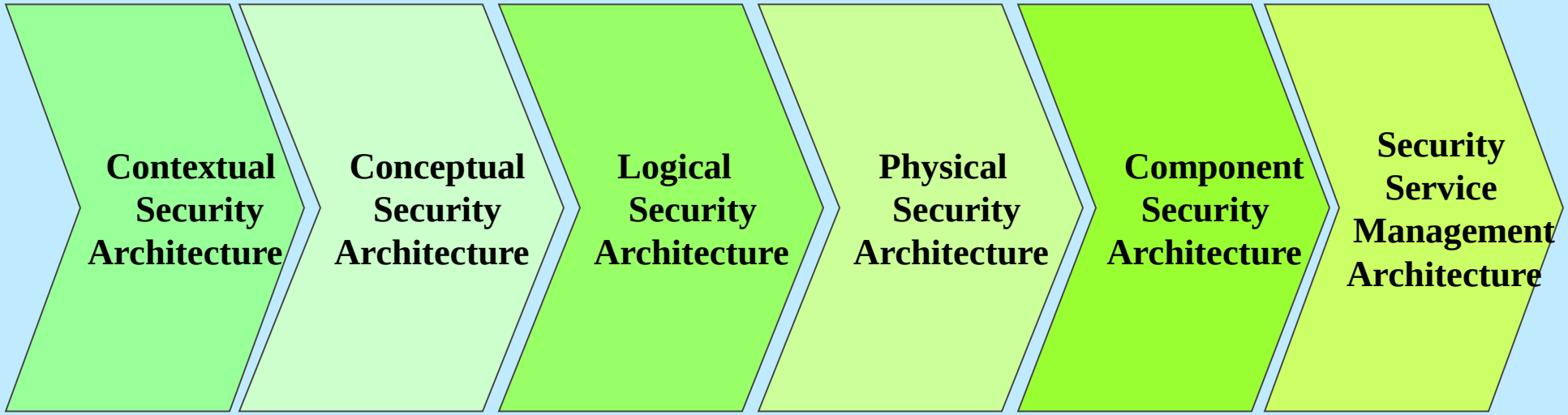
Architecture Design Phase

	Assets (what)	Motivation (why)	Process (how)	People (who)	Location (where)	Time (when)
Logical	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; SOA	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain Associations & Inter-actions	Start Times, Lifetimes & Deadlines
Physical	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications, Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms & Networks Layout	Timing & Sequencing of Processes & Sessions
Component	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'nt Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, Data Repositories & Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring, Reporting & Treatment	Tools & Protocols for Process Delivery	Identities, Job Descriptions; Roles; Functions; Actions & ACLs	Nodes, Addresses & Other Locators	Time Schedules; Clocks; Timers & Interrupts

Design Framework
(Service Management View)

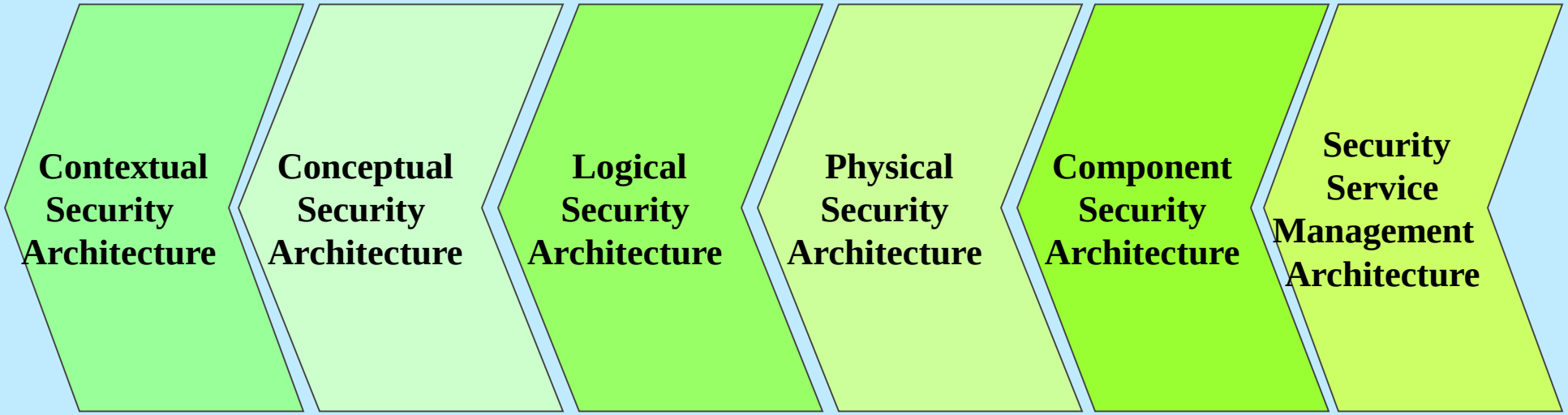


Traceability For Completeness



Every business requirement for security is met and the residual risk is acceptable to the business appetite

Traceability For Justification



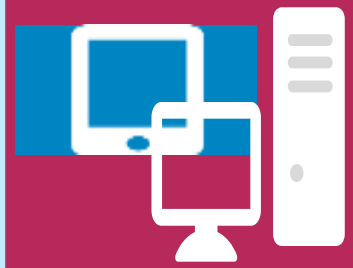
Every operational or technological security element can be justified by reference to a risk-prioritised business requirement.

Solutions And Technology Modelling Approach

Security Solutions Differentiation

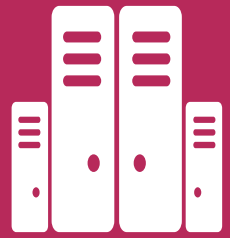
Driving greater **operational efficiency** and **accelerating results**

Business-class connected solutions



Empowering secure access to data and information anytime, anywhere

Integrated, optimized enterprise



Integrated, optimized systems that speed time-to-value & simplify tools/tasks

Software that simplifies IT and mitigates risk

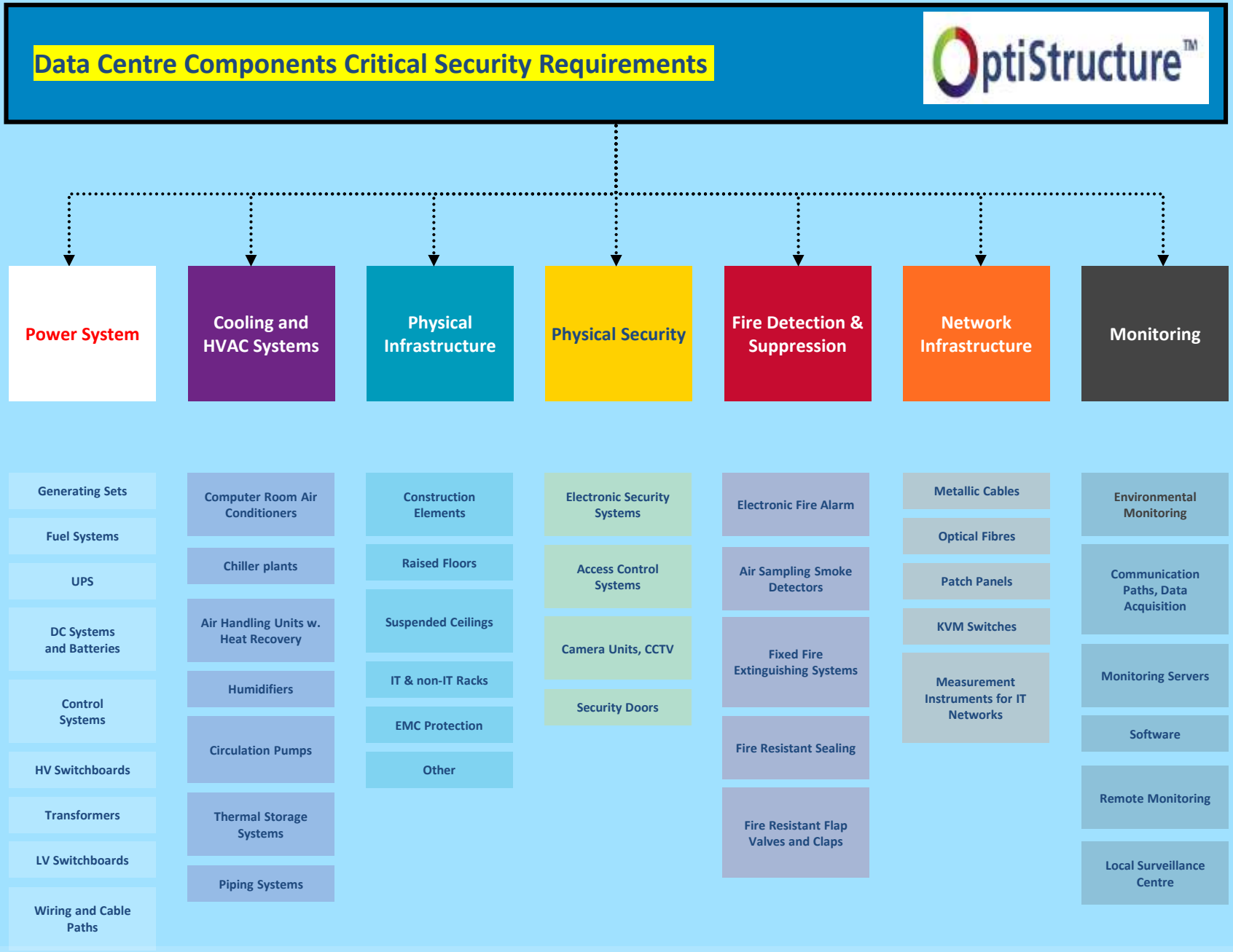
Simplify and manage data, infrastructure & end points in diverse & heterogeneous environments

Flexible, next-generation services

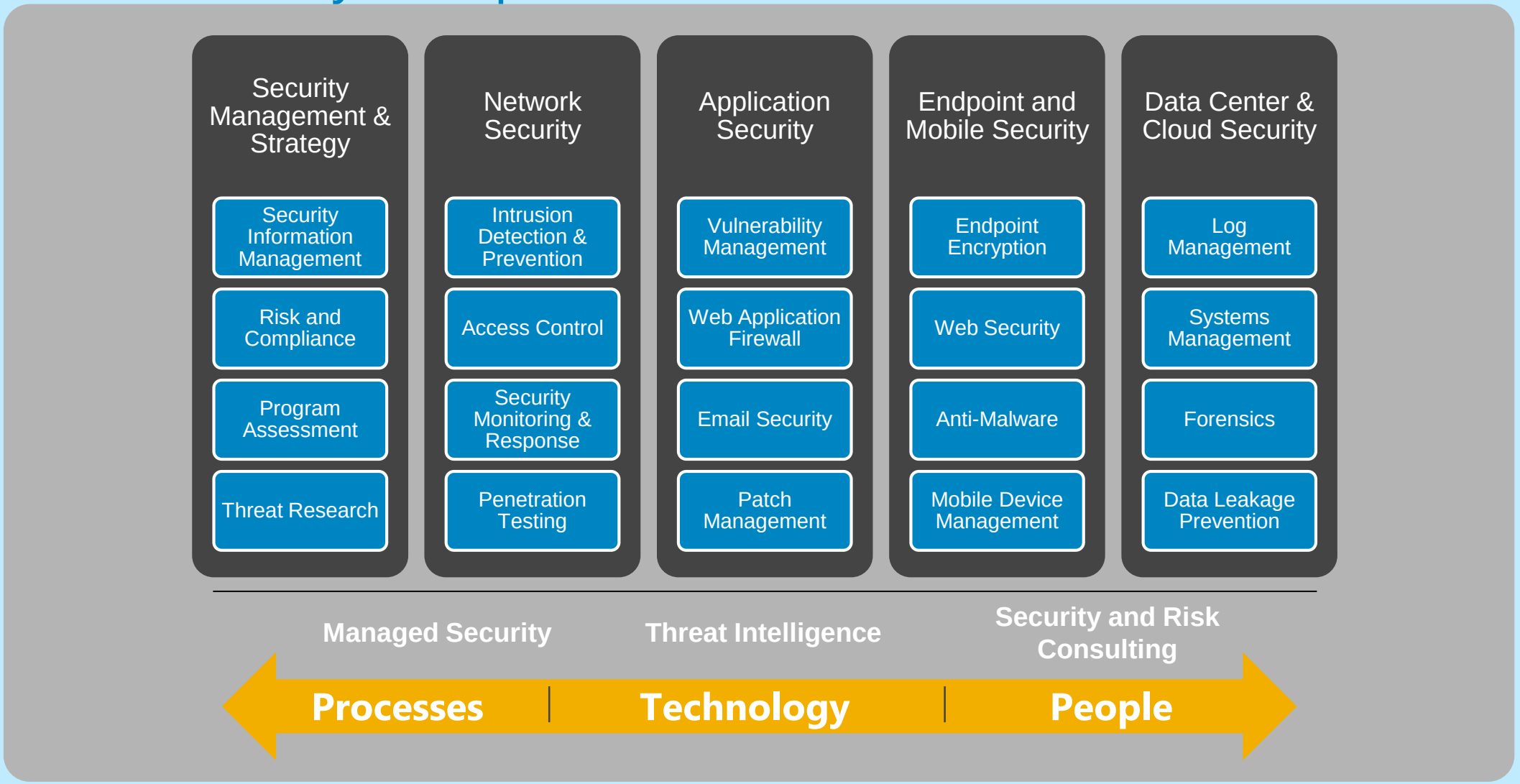
Configurable modular service offerings enabling modernization, cloud, mobility, social & analytics

Differentiated with a **scalable design point**

Data Centre Components Critical Security Requirements

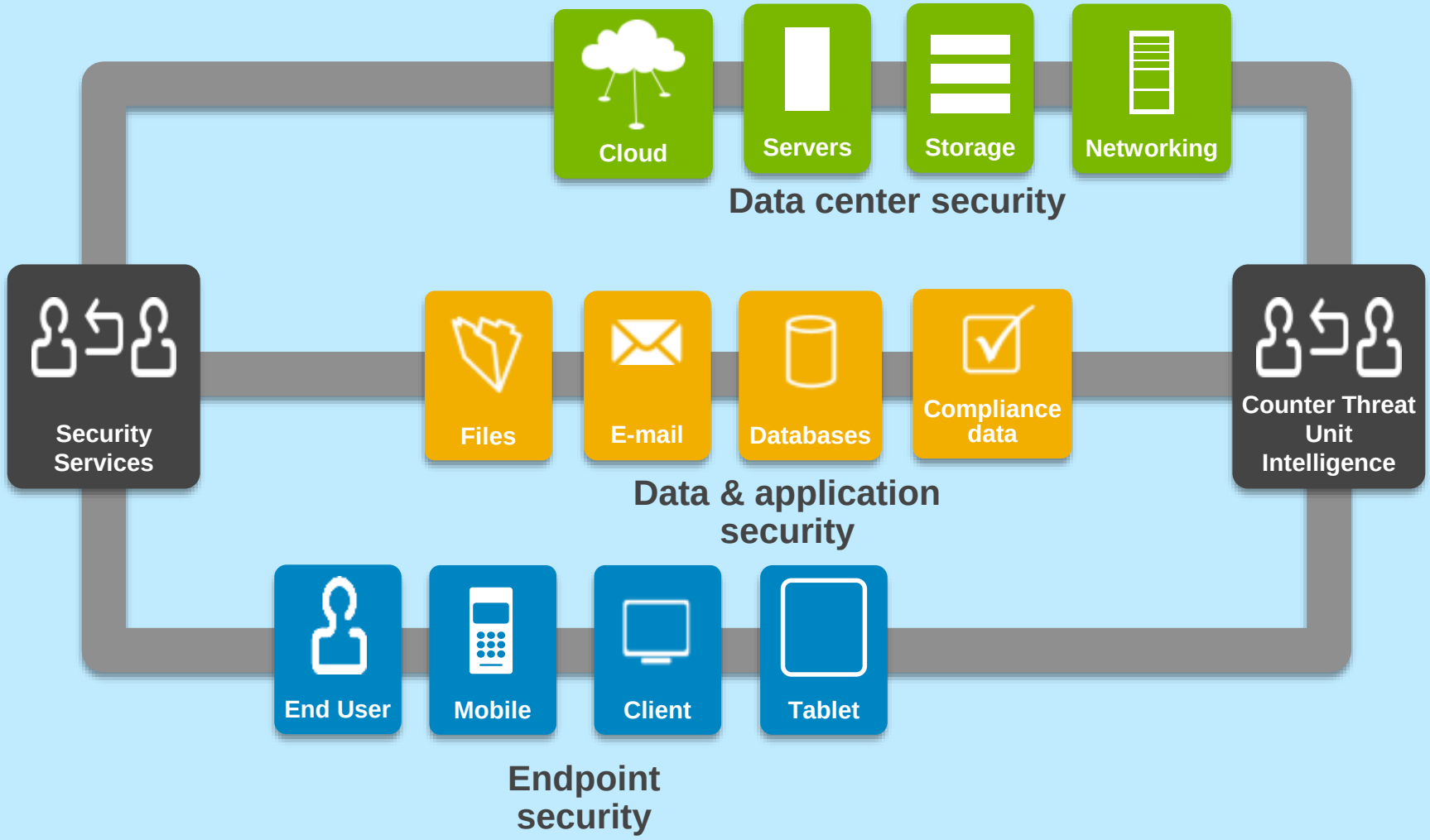


Security Components Portfolio Considerations



People’s Integration

Integration of **expertise** and **processes** with **technology** to protect systems and data



Cyber Resiliency

Cyber Resilience

THE FOUR DIMENSIONS **OF CYBER RESILIENCE**

Cyberattackers are continually evolving and adapting, and the risks get worse by the day. You need a plan to keep email flowing, business operations running and the ability to recover lost or locked data quickly after an attack. You need these four core capabilities:

1 THREAT PROTECTION

The combination of internally-developed and third-party technologies paired with dozens of internal and external threat intelligence sources provides a multi-layered inspection system. This will protect against widely-used commodity attacks and customized, highly-targeted attacks.

2 ADAPTABILITY

You need to move and adapt quickly to stay ahead of the latest attacks. But technology should be only one part of a successful approach. Your employees must become more aware of the ongoing threats to help better protect your organization. This means delivering inline user education, continually assessing and deploying leading technologies, conducting ongoing threat analysis, and automating remediation services.

3 DURABILITY

Email may be forced offline by a cyberattack, or purposely by IT to contain a current threat. This can directly impact business operations by preventing or limiting the ability to communicate. Access to files held in the email system can be impacted, too. To prevent these types of outages, you need an email system that remains 100% available while ensuring the integrity of the data stored within.

4 RECOVERABILITY

You need to keep your data protected, but accessible for users. However, many organizations are unaware of the challenges involved when malicious attacks occur and point-in-time recovery is required. Leveraging an archiving service built for this can automate and simplify the process of recovering your email and other important Exchange data.

Quick Fact: Adapting can be hard. There will be 3.5 million unfilled security positions by 2022 globally.*

* Center for Cyber Safety and Education 2018

Security Partnerships and Relationships Considerations

Security Partnerships and Relationships Considerations

- Microsoft Active Protections Program (MAPP)
- Forum of Incident Response & Security Teams (FIRST)
- Financial Services Information Sharing and Analysis Center (FS-ISAC)
- Internet Security Alliance (ISA)
- Internet Systems Consortium (ISC)
- SANS Institute
- Zero Day Initiative (ZDI)
- Anti-Phishing Working Group (APWG)
- USSS ECTF
- FBI & FBI Citizens' Academy
- Department of Defense
- Department of Energy
- InfraGard
- NATO
- Interpol
- CyberCop Secure Information Exchange Network
- Federal Trade Commission
- Cyber Security Forum Initiative (CSFI)
- National Cyber-Forensics & Training Alliance (NCFTA)

Security & Strategy Research and Development Approach

Security & Strategy Research and Development Approach

	Flexible Approach	Defined Methodology	Business Knowledge	Deep Technical Expertise	Vision for the Path Forward
Core Assets					
Services	Incident Response & Digital Forensics	Strategic Residency Services	Testing & Assessments	Compliance & Certification Services	Security & Governance
Business Value	Critical Help When It's Needed	Gain Efficiency & Effectiveness	Measure Your Current State and Articulate the Path Forward	Security Approach to Compliance	Protect Industrial Control Systems	Accelerate Maturity of Programs

Recommendations For C – Level Strategy & Planning Continuous Monitoring

SIX WAYS TO CLOSE THE C-LEVEL GAP

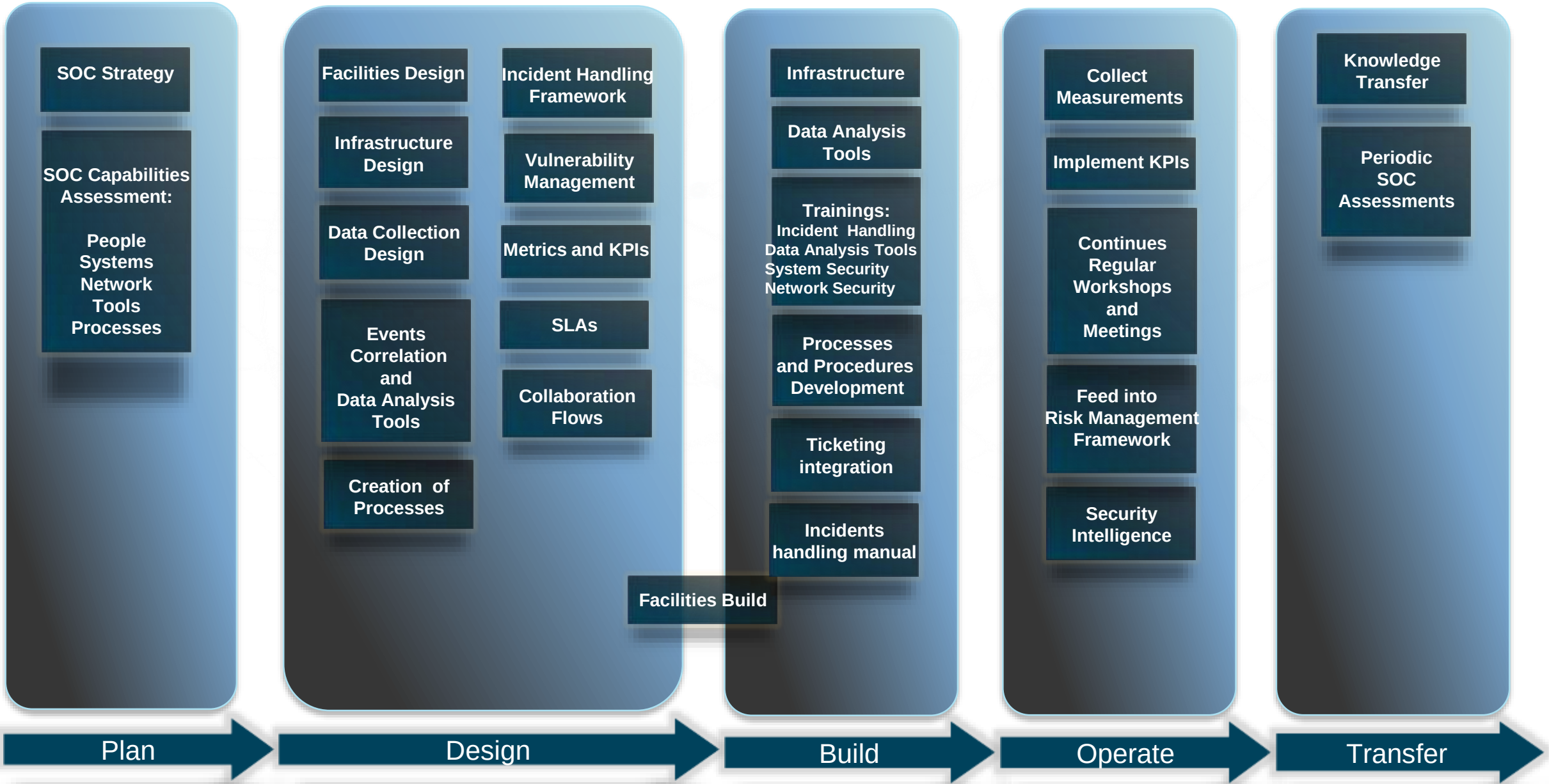
- QUICK STEPS
- 1. Ensure there is security expertise on your leadership team.
- 2. Place cybersecurity into the function that manages overall risk mitigation for the organization.
- 3. Recognize that upper management sets the tone of the company’s culture – this includes security culture.
- 4. Benchmark your security controls and risk management programs against peer organizations on a regular basis.
- 5. Constructively engage the appropriate regulators on your security program and their specific requirements.
- 6. Leverage internal marketing to communicate that security is not exclusively an IT problem.

EIGHT STEPS TO CLOSE THE STRATEGIC APPROACH

EXPERT ADVICE: AVOID A PLANNING HEADACHE

1. **DEVELOP A STRATEGIC PLAN** for cyber resilience that considers broad business objectives.
2. Don't put the onus on IT: **ENGAGE LEADERS ACROSS THE BUSINESS**.
3. Communicate planning to all staff, and **EDUCATE AND ENGAGE** them on a regular basis.
4. **DON'T OVER-ENGINEER** your plan.
5. **CLEARLY DEFINE THE RISK AND THE SCOPE OF THE PROBLEM TO THE BOARD** to secure their buy-in and funding.
6. **INVEST!** Threats can be costly to your brand, revenue and IP.
7. Hire a **CISO/LEADER WITH STRONG COMMUNICATIONS SKILLS**.
8. Share a **CLEAR AND LOGICAL CYBER RESILIENCE ROADMAP** with the business.

Continuous Monitoring Capability



Q & A

Thank you!