CMU/ SEI DevSecOps Days, Washington DC
September 18th, 2024

- Leadership
- Technology
- Experience
- Execution

Author	Title	Contact
Nikhil Kumar	Founder & President, ApTSi Co-Chair Zero Trust, The Open Group/SABSA Co-Chair SOA4BT Project, The Open Group Co-Chair, AEA Boston Chapter	Email: nikhil@ap-tech-solns.com LinkedIn: http://www.linkedin.com/in/nikhilkumar Phone: (248) 797 8143 Boston, MA

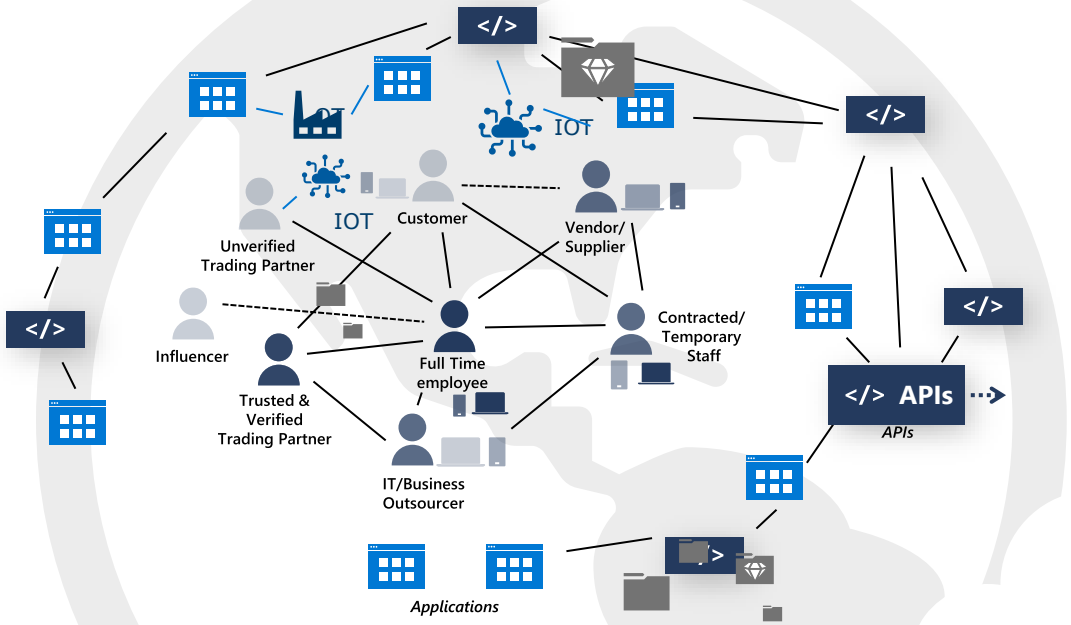
- Zero Trust/Security/ Compliance
- AI/Cognitive Solutions
- Digital Transformation
- EA & Strategy
- SOA & Cloud
- Solutions Architecture/ Development
- Big Data/ Virtualization/ Data Lakes/ Interoperability

Contributions and Acknowledgements

Norman B Anderson	Principal, Engineering and Architecture, ApTSi
Krishna Sonavane	Research Associate ApTSi
Ashish Rathod	Research Associate ApTSi
Amit Mahorkar	Research Associate ApTSi
Atharva Jadhav	Research Associate ApTSi
Pradeep Shelke	Research Associate ApTSi

What was the Business Reason for Zero Trust?

Drivers for change



Characteristics of the Digital Era

- Complexity
- Velocity
- Disruption
- Adaptability

Must adapt to continuous change from

1. Changing business models and drivers
2. Evolving ecosystems
3. Changing technology landscape
4. Regulatory, geopolitical & cultural forces
5. Disruptive events
6. Hybrid/Remote work & online learning

"You cannot operate if you aren't secure"…

"Zero Trust" has been around for a while

2004 Jericho Forum® Formally Established

2014 Microsoft Advocates "Assume Breach"

2016 Conditional Access Released

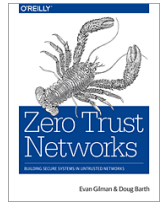
Ongoing Passwordless Authentication

~2004 Network Access Control (NAC) Architectures

2010 Forrester coins "Zero Trust" Term

2014 BeyondCorp Published

2017



Today
Consensus on End to End approach

The Open Group
(Home of the Jericho Forum®, TOGAF®, and more)

Executive Order
on Improving the Nation's Cybersecurity - The White House

NIST

Forrester
ZTX Model

World Economic Forum

Historically: *Slow mainstream adoption for both network-only & identity centric models:*

Network – Expensive and challenging to implement
Google's BeyondCorp success is rarely replicated

Identity – Natural resistance to big changes
Security has a deep history/affinity with networking

Today: Increasing consensus and convergence (though still some variations)

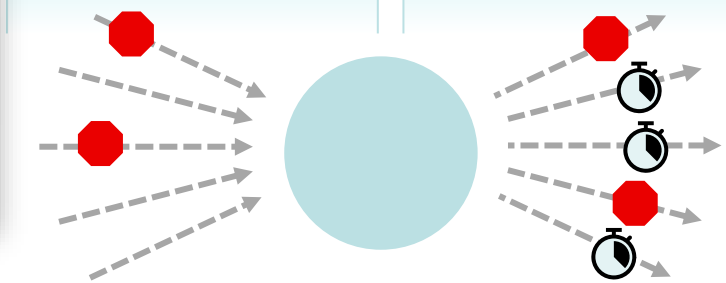
Zero Trust Principles

Assume Breach (Assume Compromise)
Assume attackers can and will successfully attack anything (identity, network, device, app, infrastructure, etc.) and plan accordingly

→ *Transforms overall thinking, strategy, and architectures from "safe network" to "open network"*

Reduce threat space & attack surface
The less to protect, or the less spent on protection, the easier it is to support Zero Trust drivers

→ *Reduce "attack surface" of each asset*



Reduce blast radius
Limit access of a potentially compromised asset, typically with just-in-time and just-enough-access (JIT/JEA) and risk-based polices like adaptive access control.

→ *Enforces least privilege principle*

Zero Trust Foundational Concepts

- **System Asset-Centricity**

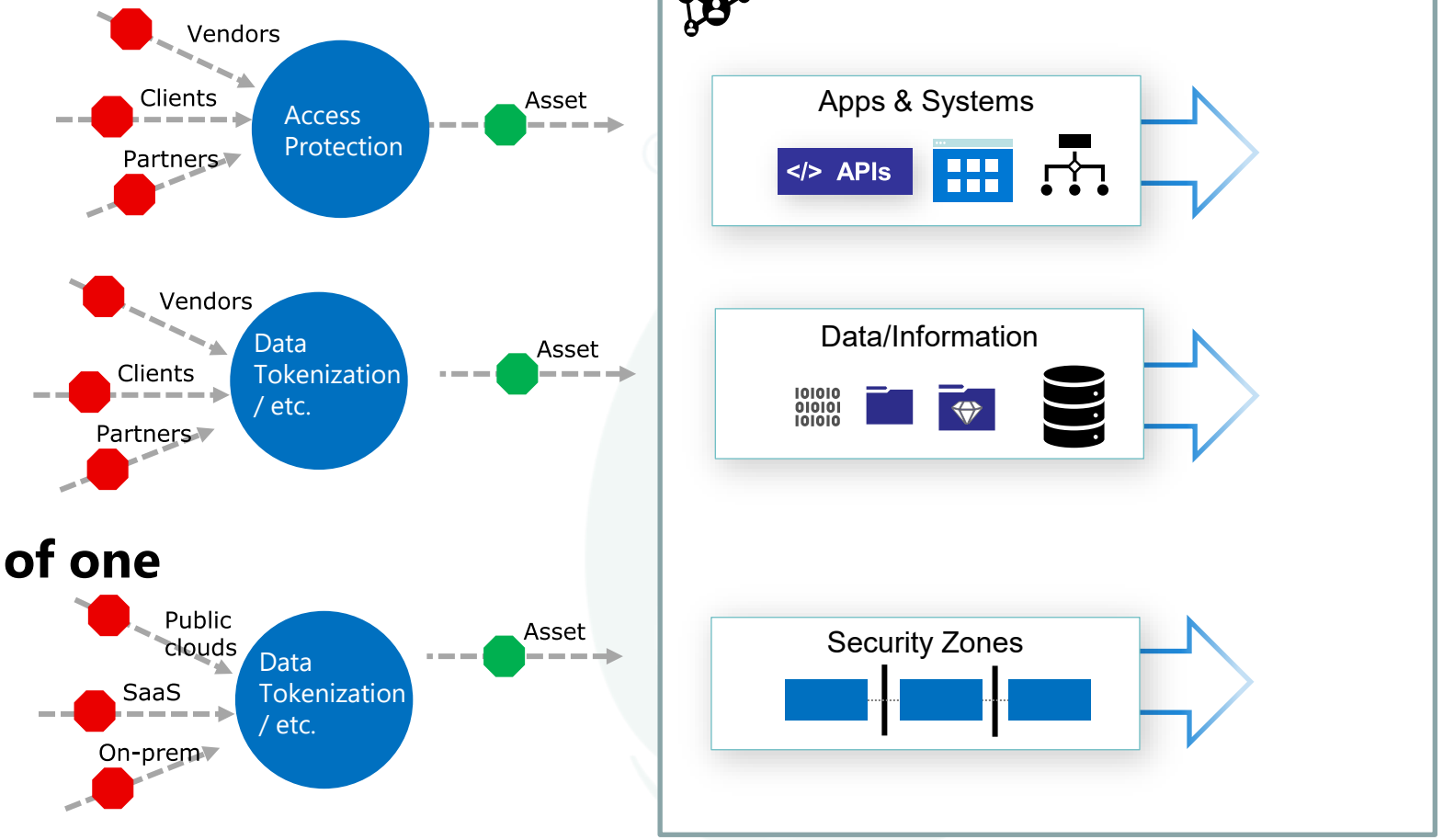
  Granular protection of assets enables agility and reduces the blast radius

- **Data Asset-Centricity**

  Replace high-value data assets with low-value "tokens" to reduce breach impact and enable agility

- **Secure anywhere/ network of one**

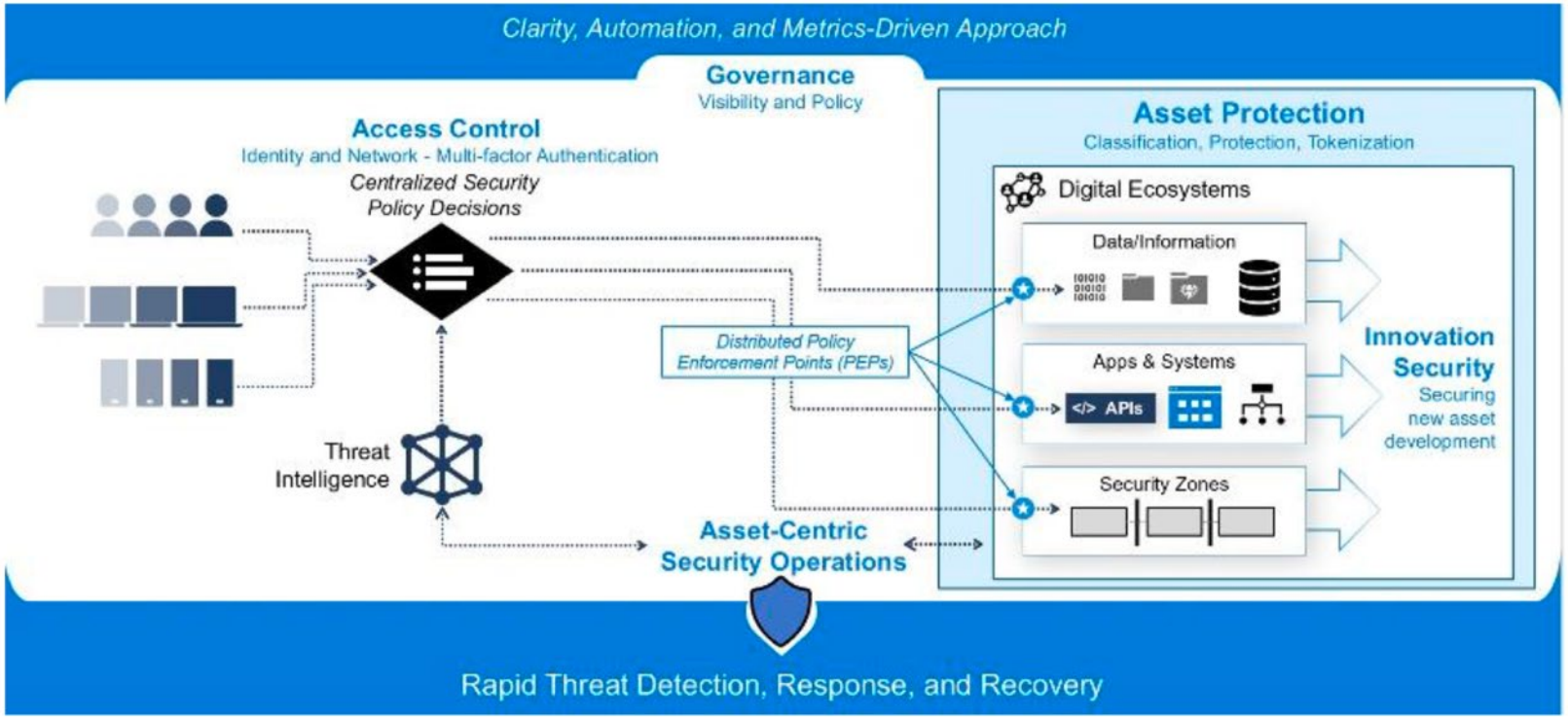
  Reduce granularity to increase agility/ support Zones to focus on business value/ Secure anywhere as an underlying principle



These concepts lay the foundation for Velocity (Agility), Adaptability, Disruption and Complexity….

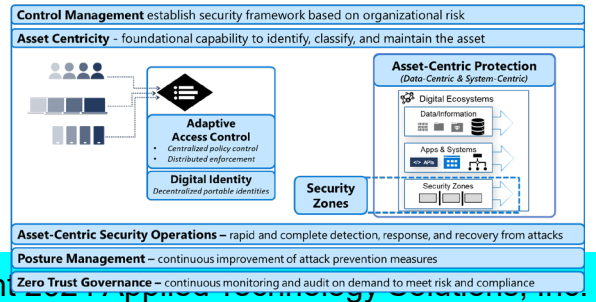
… They are often used together and not alone in a comprehensive Zero Trust Strategy

What is a Zero Trust Architecture*



Zero Trust is an *asset-centric* information security approach that enables organizations to secure and manage data/information, applications, Application Program Interfaces (APIs), any data integrations *on any network*, including the cloud, internal networks, and public or untrusted (Zero Trust) networks

* From The Open Group's Zero Trust Reference Model Snapshot



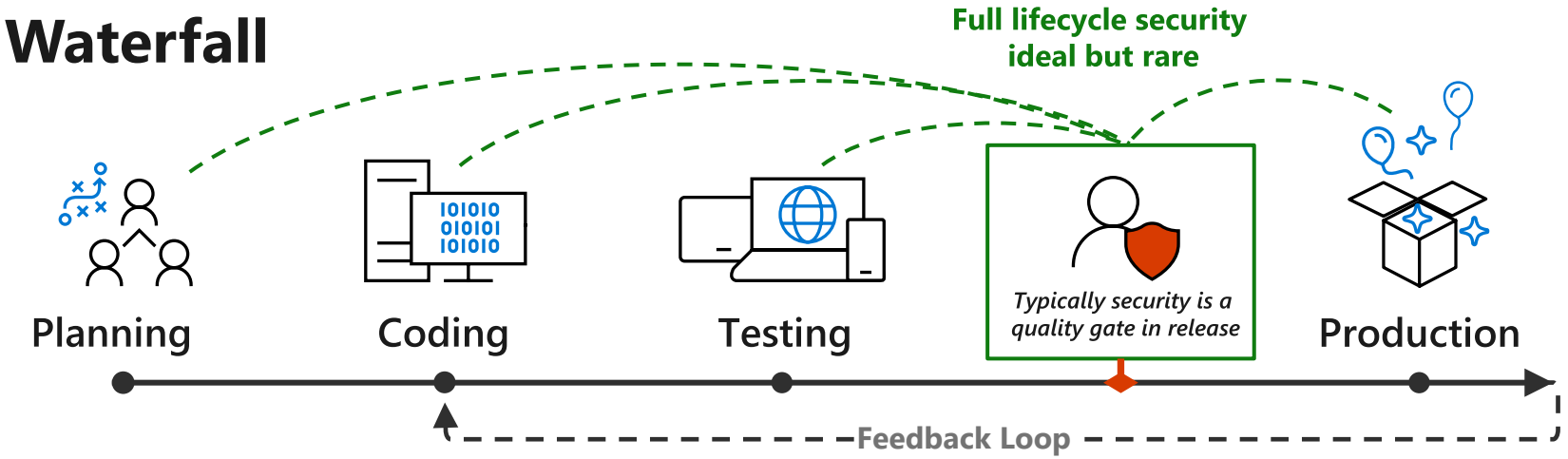
Zero Trust Capabilities

Modern Digital Organizations and Operational Model

Organization and Product Strategy and Operating Model

New & enhanced Products and Capabilities

Waterfall



Bias to Plan & Quality *(Weeks/Months)*

Existing Products and Capabilities

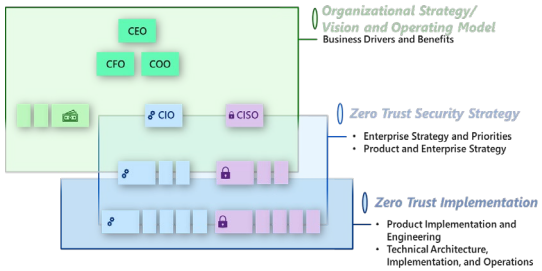
DevOps

Quality and Security risk mitigated by rapidly release of fixes

Bias to Speed & Agility *(Hours/Days)*

Enterprise DevSecOps

A key Zero Trust capability



Security must be integrated with all layers of business

Establish Integrated Security Strategy

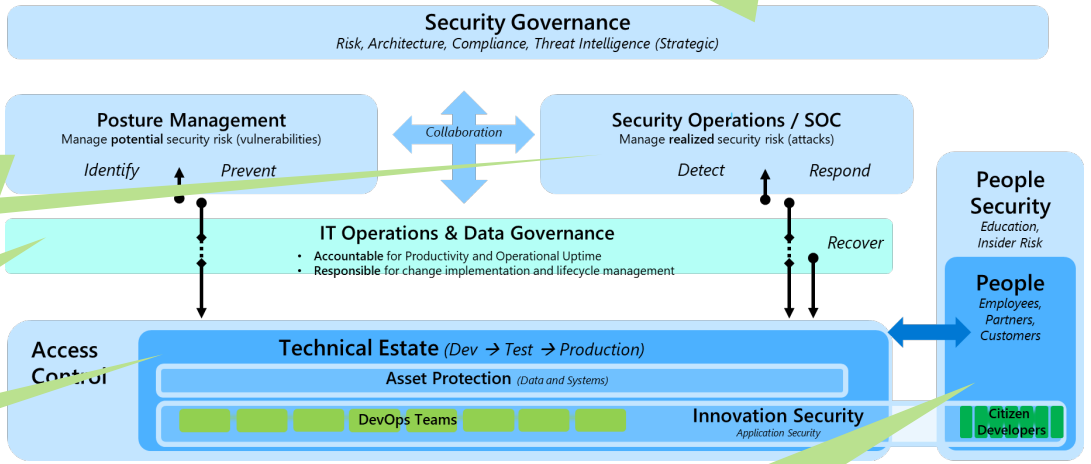
1. Secure by intent Product/ Technology Strategy
2. Compliance/ Common controls
3. Empower growth and operations

Secure in Operation

1. RASP, Binary exploit generation and fuzzing
2. ITSM/ SOC/ X-SOAR integrated
3. Integrated posture mgmt.

Security Critical Analysis

1. Threat Modeling & Vulnerabilities
2. Asset Centricity
3. Posture Mgmt.



Build and Ship Secure Products

1. Traditional DevSecOps: SAST, IAST, DAST, RASP
2. Binary exploit generation and fuzzing
3. Statistical Dependency Analysis
4. Secure by design
5. Secure architectures
6. Cyber-Resilient by design
7. Reuse of cybersecurity patterns
8. Reusable and reliable secrets mgmt. and certs

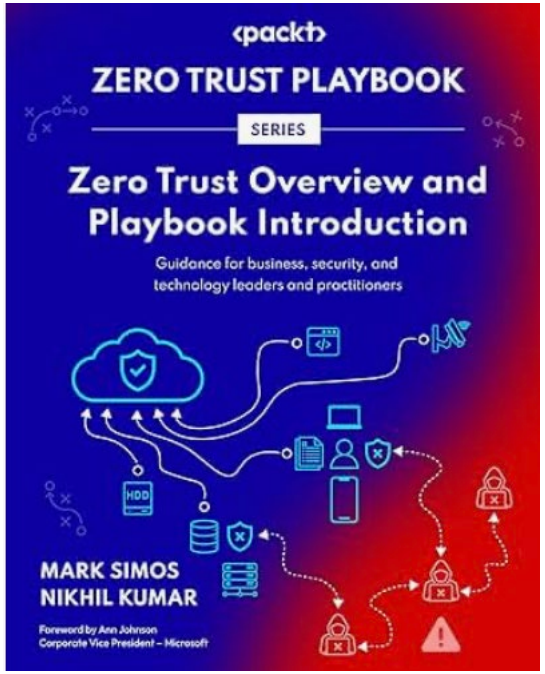
Establish Security Operating Model

1. People Security
2. Secure Processes – technology, security/ product
3. Gamified training, X-SOAR, etc.
4. Mapped to operating model

Strategy Model
Operational Model
Operating Model

Where to learn more

- The Open Group's Security Forum Zero Trust page
  - And information in The Open Group library
- Multiple groups on LinkedIn
  - Including one for The Open Group's ZTA work
- Several vendors, including member companies of The Open Group



Nikhil & Mark wrote a book!

http://zerotrustplaybook.com

QUESTIONS!

THANK YOU!

- Leadership
- World Class Technology
- Experience
- Execution

- Zero Trust/Security/ Compliance
- AI/Cognitive Solutions
- Digital Transformation
- EA & Strategy
- SOA & Cloud
- Solutions Architecture/ Development
- Big Data/ Virtualization/ Data Lakes

Name **Title**

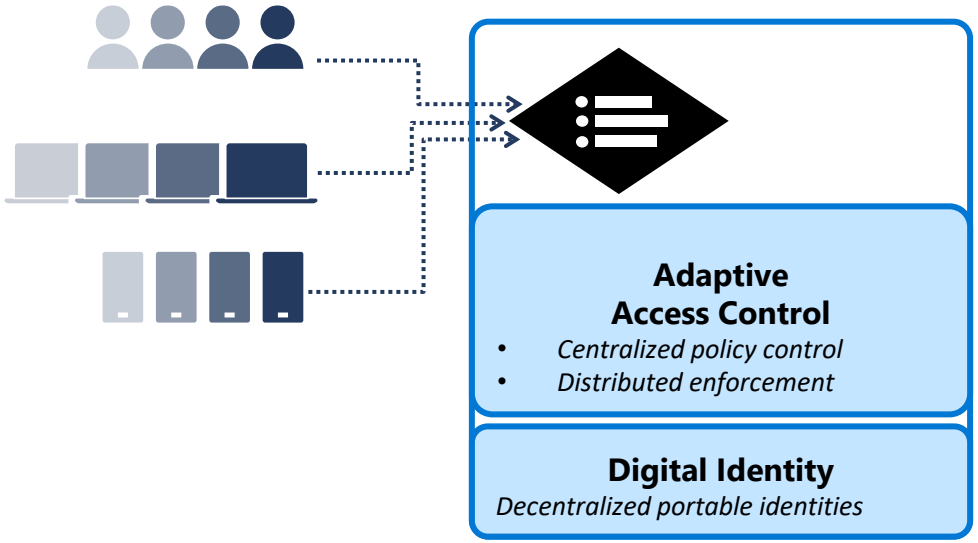
Nikhil Kumar President & Founder, ApTSi
Co-Chair Zero Trust Working Group, The Open Group
Member AI Working Group, The Open Group
Co-Chair SOA4BT Project, The Open Group
Member AI Working Group
Chair, AEA Boston Chapter
nikhil@ap-tech-solns.com
(248)-797-8143

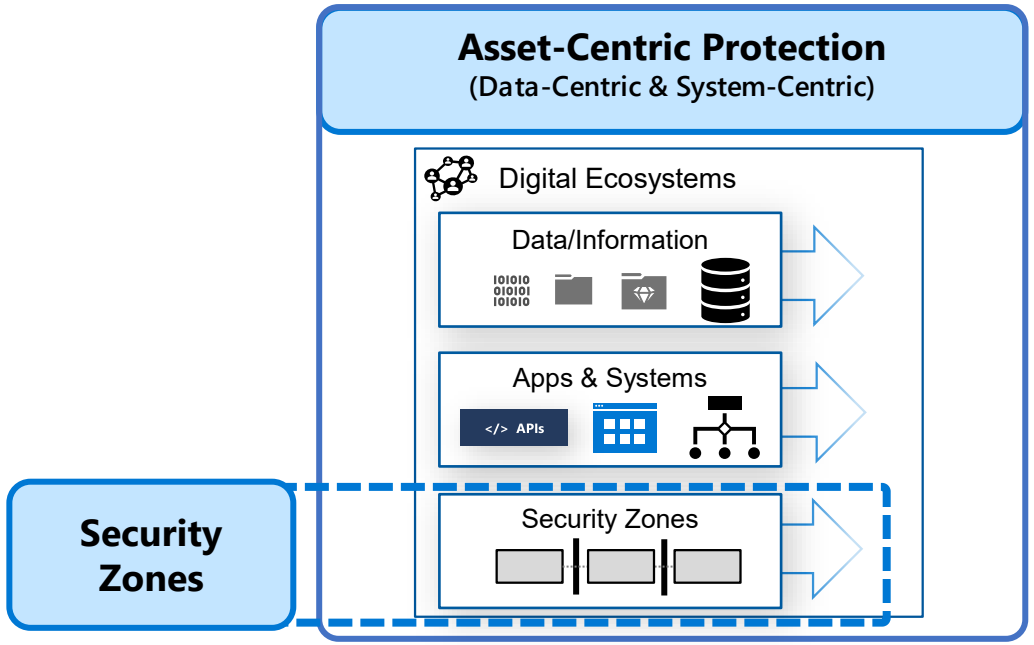
Key Zero Trust Capabilities

DevSecOps and SCRM

Risk Controls - establish overall security framework based on organizational risk

Asset Centricity - foundational capability to identify, classify, and maintain the asset



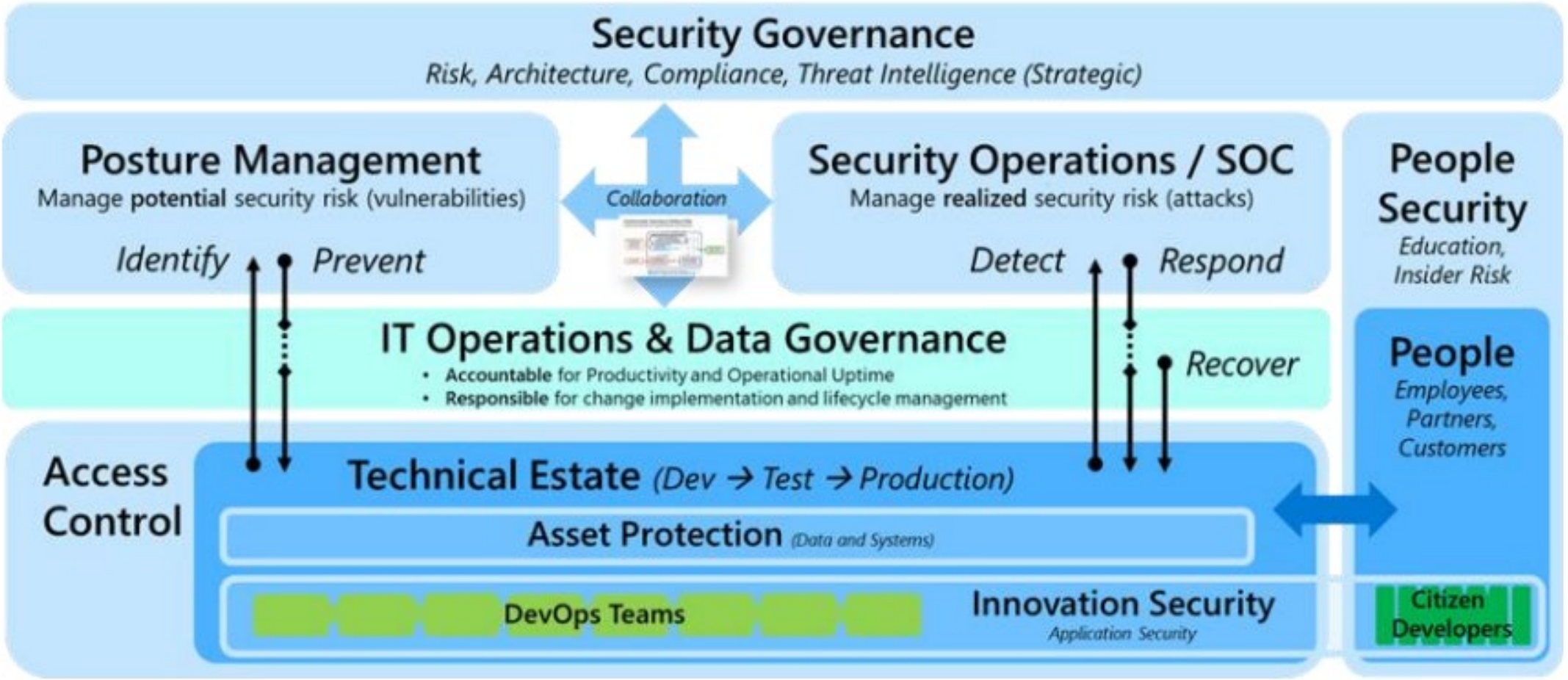


Asset-Centric Security Operations – rapid and complete detection, response, and recovery from attacks

Posture Management – continuous improvement of attack prevention measures

Zero Trust Governance – continuous monitoring and audit on demand to meet risk and compliance

Zero Trust Operating Environment



The Zero Trust Playbook – the 3 Pillars

Strategic
Set the Direction

Business Strategy
Mission/Vision/Goal

Business Capabilities

Zero Trust Capabilities
Informed by Reference Model

Technical Capabilities

Operational
Integrate into Organization

Business Operations
Product Lines + Value / Supply Chain

Business Constraints + **Business Processes**

Zero Trust Solution Architectures

Zero Trust Services and Components

Technical Constraints

Technology Estate
Services / APIs

Zero Trust Integration
Cross-cutting Concerns

Operating Model
Monitor and Adjust

Business Operating Model
Activities + Org Structure

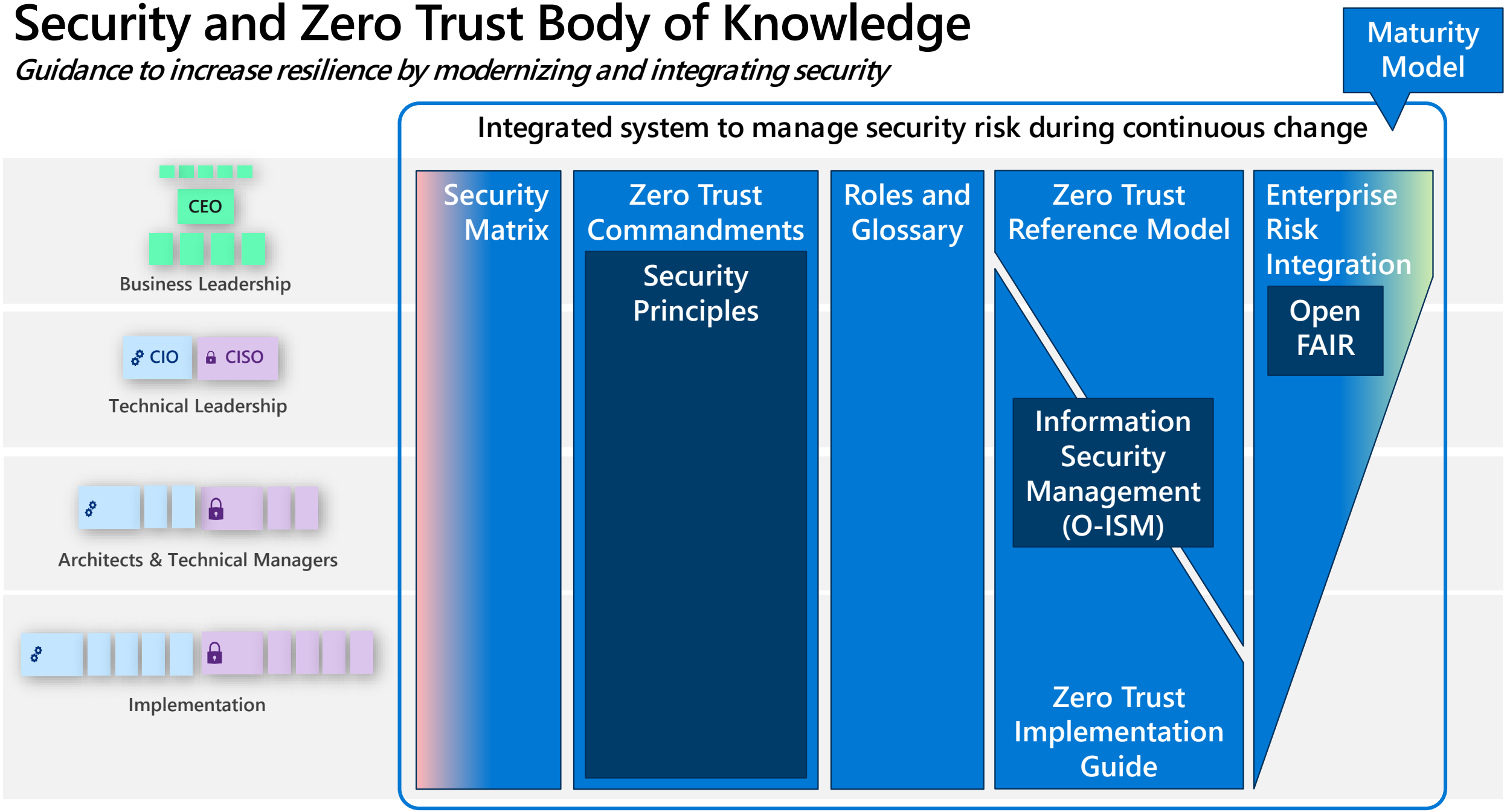
Governance & Guardrails

Decision Rights & Accountabilities

Training & Cultural Change *Enable Learning Organization*

Security and Zero Trust Body of Knowledge

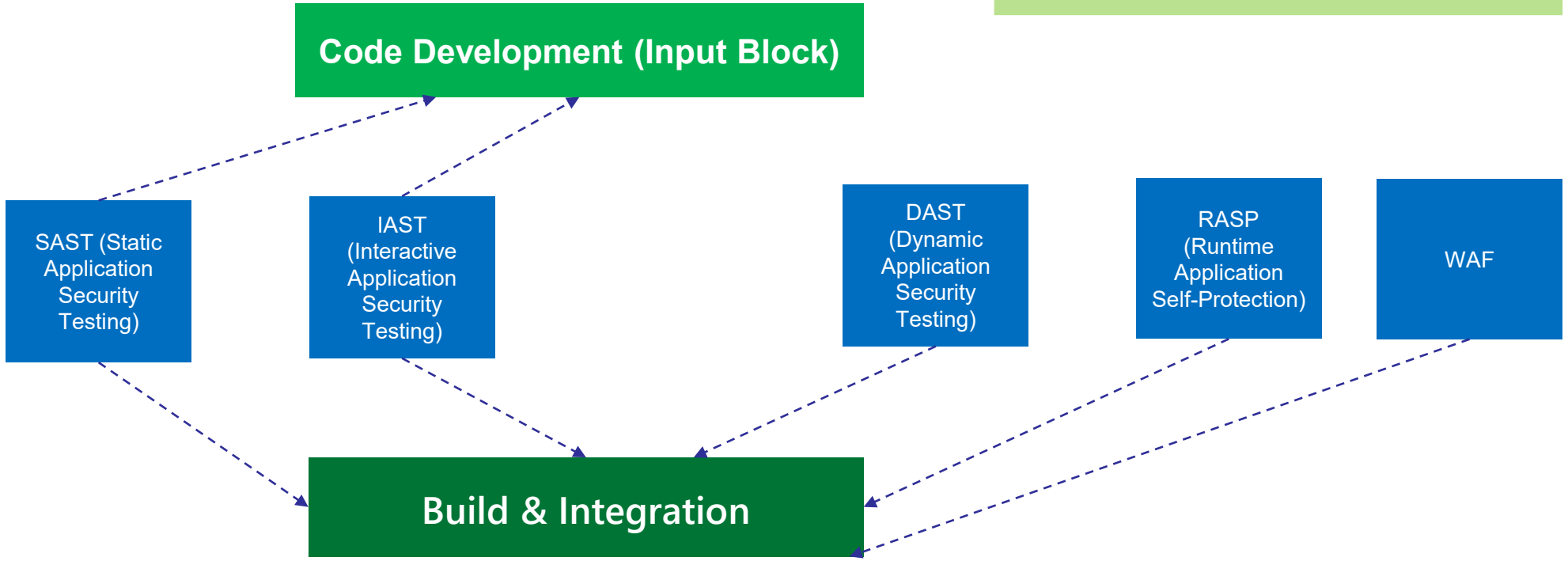
Guidance to increase resilience by modernizing and integrating security



Development and Security Automation – address security continuously

1. Development and automation – SAST, DAST, IAST, RASP

Modern CICD includes Dynamic Introspection



Development and Security Automation – managing, detecting and remediating vulnerabilities

Vulnerabilities and SCRM (Supply Chain Risk Management)

CVEs (Common Vulnerabilities and Exposures)

Dependencies (Third-party Libraries and Components)

Statistical Dependency Analysis

SBOMs (Software Bill of Materials)

Aggregate SBOMs

Open Source and Its Implications

Statistical Vulnerability Detection

AI for Continuous Feedback

Secure the Supply Chain

Development and Security Automation – managing and detecting vulnerabilities – AI and SCRM

AI for Vulnerability Detection and Risk Prediction

Dependency Analysis (Dynamic and Static)

SBOM and Aggregate SBOM Analysis

Object Code Analysis

SCRM

AI Continuous Improvement

Vulnerability Management & Prediction

Integration with DevSecOps Pipelines

Statistical Vulnerability Detection

AI for Continuous Feedback

Secure the Supply Chain

Secure Products – involve being secure by design and a secure architecture

Zero Trust Principles

- Peer Reviews (Code Reviews)
- Reusable Objects
- Design Patterns
- Best Practices (Software Engineering)
- Automation Tools for Code Review
- Code Quality Checks
- Integration into CI/CD Pipeline
- Continuous Improvement and Feedback

Operations, DevSecOps and Zero Trust – creating continuous improvement in security

Key factors of Modern SOC

- Threat Detection
- Incident Response & Remediation
- Monitoring and Alerts
- Automation & Orchestration (SOAR)
- AI-Driven Analytics
- **Zero Trust Integration**

Role of Dev Sec Ops

- Continuous Integration with SOC
- Security in Development Lifecycle
- Vulnerability Management
- Collaboration between DevSecOps and SOC
- Security Incident Response Integration
- AI Ops and Threat Analysis

The Operations in DevSecOps and Zero Trust – creating continuous improvement in Products

Modern SOC Driving Zero Trust Security

Zero Trust Principles in Operations

AI Operations

- The Modern SOC (Security Operations Center)
- Operations and Zero Trust
- Determination of Patterns (Lateral Attacks, Intrusions)

Intentional Security (Architecture and Development)

Zero Trust Principles

- Secure by Design
- Code Security (Continuous Improvement)
- Architect Securely

Intentional Secure Operations

Zero Trust Principles

- Incident Response and Threat Mitigation
- AI Ops in a feedback loop