Integrity360
your security in mind

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

Developing the early detection and prevention foundations for an effective security operations strategy

Kash Valji

Senior Director Consulting Systems Engineering - Fortinet

#SecurityFirstDublin

Building Unified SecOps Platforms

Early Threat Detection Prevention and Response

Why Are We Talking About SOCs

Why Are The SOC and SecOps Such Relevant Discussion Points Today

The Expansion of the Digital Attack Surface means your exposure to advanced adversaries in greater than ever

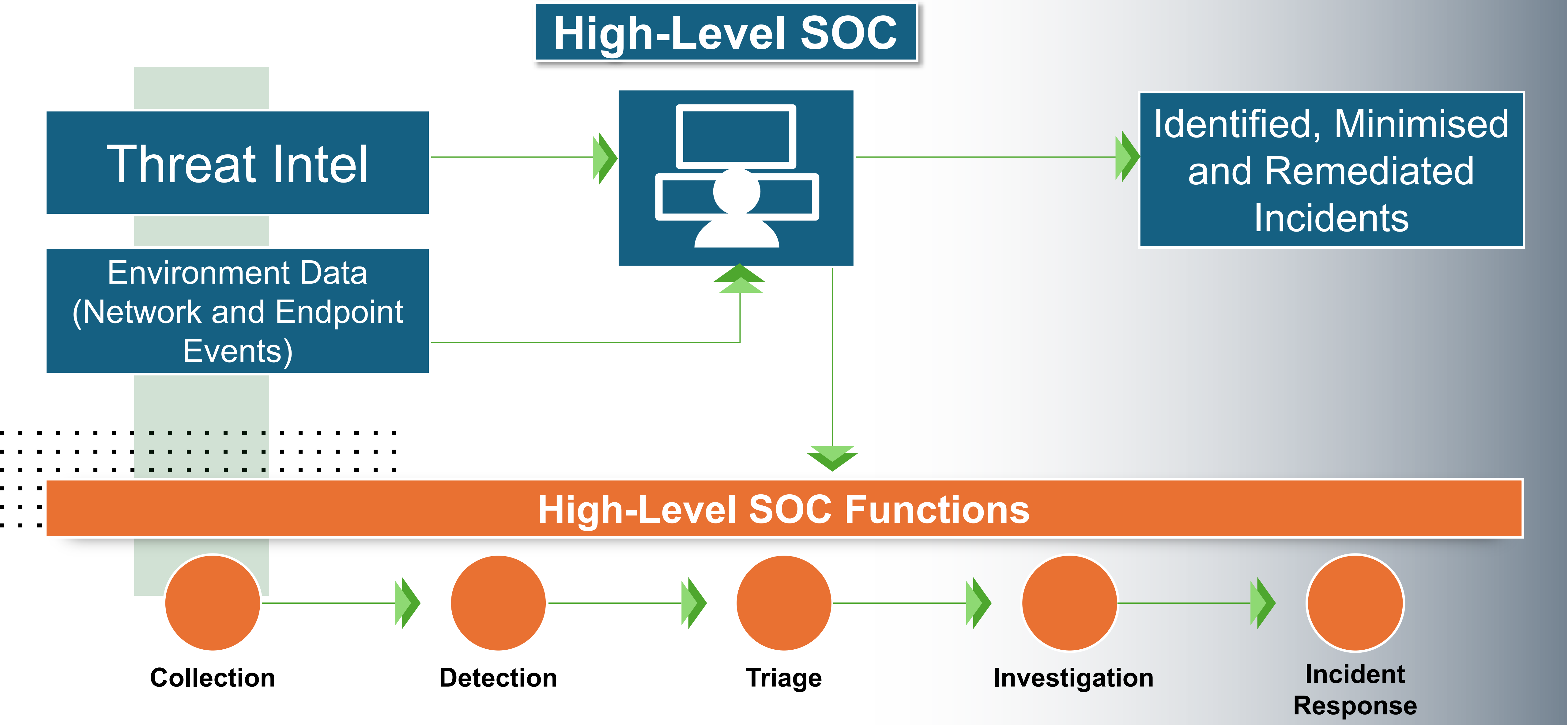
Top Reasons Security Operations Are More Difficult Than They Were 2 Years Ago

(Enterprise Strategy Group Report, ‘SOC Modernization and the Role of XDR’)

41%	The Threat Landscape is evolving and changing rapidly
40%	The attack surface has grown
39%	The attack surface is continuously changing and evolving
37%	The volume and complexity of security alerts have increased
34%	My organizations increased use of public cloud services

The traditional cyber-security toolkit used by organisations need to be more than just a collection of technologies that are loosely connected together

SOC Functions



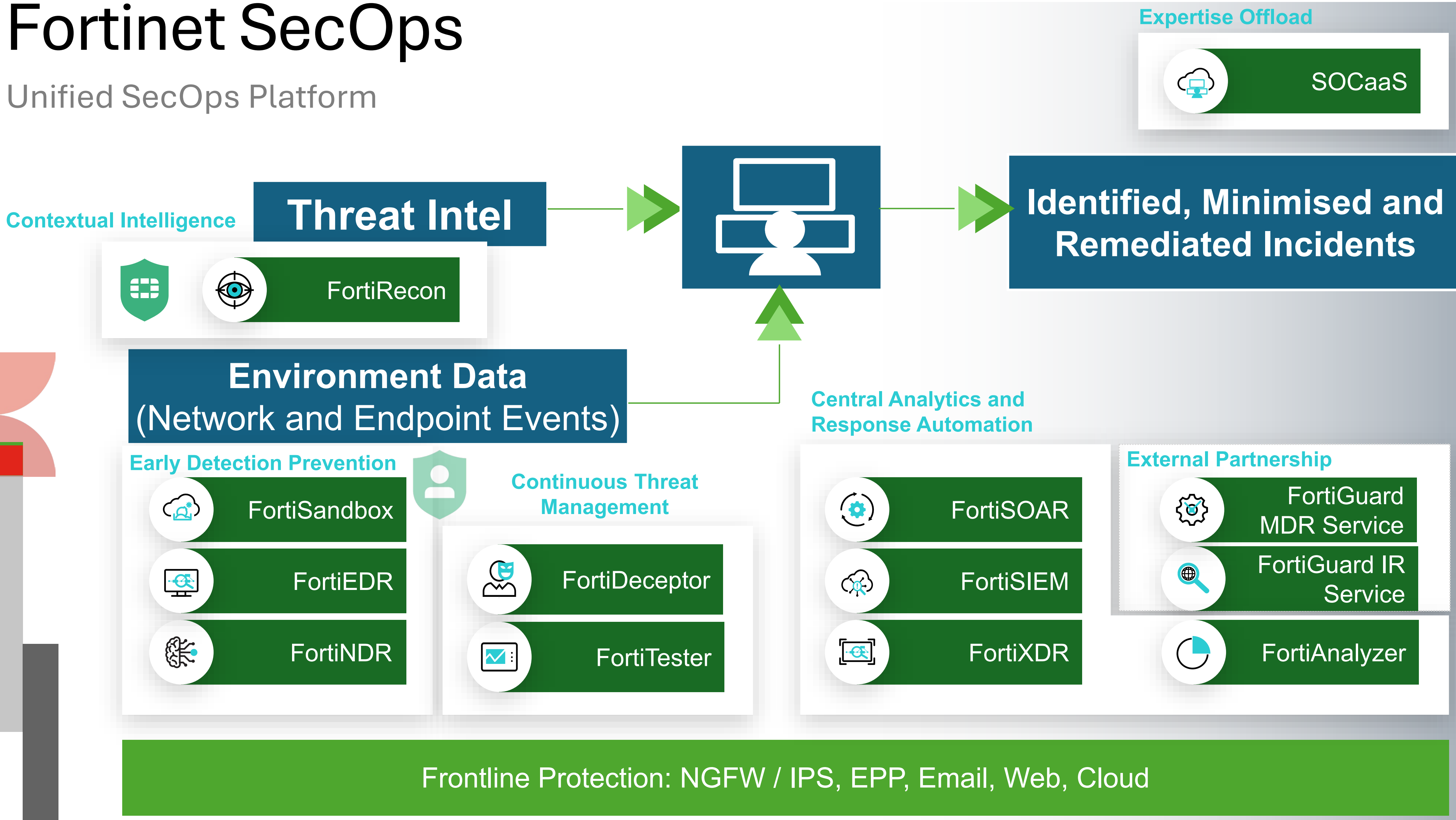
SOC Planning

Ok, I’ve decided I need a Command Centre, or need to improve the one I have, now what?

- Define Mission and Goals
- Threat Modelling: Know your Adversaries
- Requirements: Standards, Regulations and Policies
- Capabilities
- Choice of a Technology (Fabric)
- Audit from External Cyber Security consultancy
- Continuous Improvement

Fortinet SecOps

Unified SecOps Platform



Expertise Offload

SOCaaS

Contextual Intelligence

Threat Intel

FortiRecon

Identified, Minimised and Remediated Incidents

Environment Data (Network and Endpoint Events)

Early Detection Prevention

FortiSandbox

FortiEDR

FortiNDR

Continuous Threat Management

FortiDeceptor

FortiTester

Central Analytics and Response Automation

FortiSOAR

FortiSIEM

FortiXDR

External Partnership

FortiGuard MDR Service

FortiGuard IR Service

FortiAnalyzer

Frontline Protection: NGFW / IPS, EPP, Email, Web, Cloud

Deeper Defences Through Common Frameworks

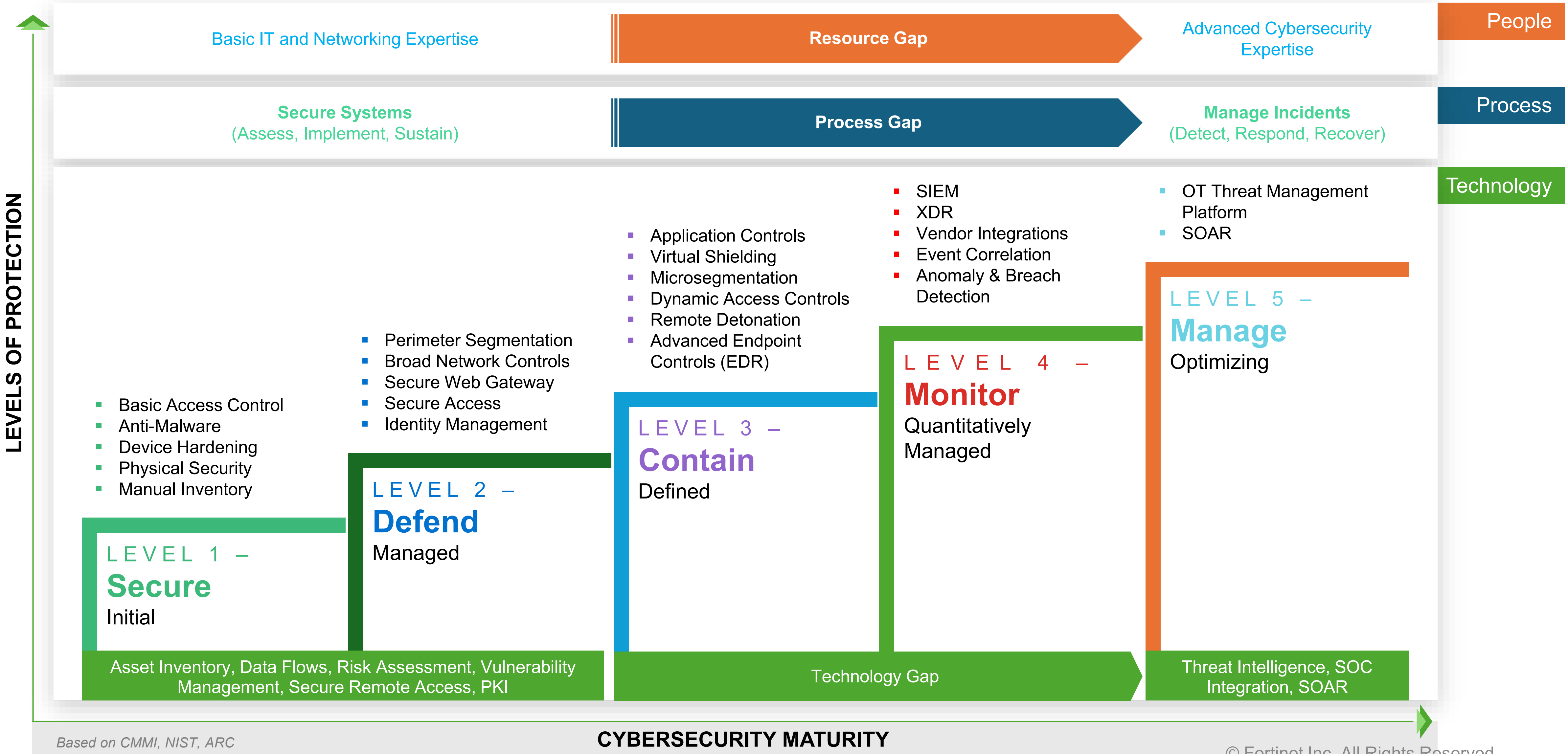
Empowering The Blue Team with Open Standards

Open Standards Industry Framework Integration

- Cyber Kill Chain
- MITRE ATT&CK
- MITRE Engage
- MITRE Attack Flow
- STIX / TAXII
- Open API’s

SOC / Cyber Maturity Levels

Start, Build, or Offload Your SOC with 24x7 Coverage



People

Basic IT and Networking Expertise

Resource Gap

Advanced Cybersecurity Expertise

Process

Secure Systems
(Assess, Implement, Sustain)

Process Gap

Manage Incidents
(Detect, Respond, Recover)

Technology

LEVELS OF PROTECTION

- Basic Access Control
- Anti-Malware
- Device Hardening
- Physical Security
- Manual Inventory

LEVEL 1 –
Secure
Initial

- Perimeter Segmentation
- Broad Network Controls
- Secure Web Gateway
- Secure Access
- Identity Management

LEVEL 2 –
Defend
Managed

- Application Controls
- Virtual Shielding
- Microsegmentation
- Dynamic Access Controls
- Remote Detonation
- Advanced Endpoint Controls (EDR)

LEVEL 3 –
Contain
Defined

- SIEM
- XDR
- Vendor Integrations
- Event Correlation
- Anomaly & Breach Detection

LEVEL 4 –
Monitor
Quantitatively Managed

- OT Threat Management Platform
- SOAR

LEVEL 5 –
Manage
Optimizing

Asset Inventory, Data Flows, Risk Assessment, Vulnerability Management, Secure Remote Access, PKI

Technology Gap

Threat Intelligence, SOC Integration, SOAR

CYBERSECURITY MATURITY

Based on CMMI, NIST, ARC