Cybersecurity For OT with Microsoft solutions

February 2025

Capgemini

OT excellence is composed of key topics that all have different levels of maturity

Build resiliency

Design and deploy at large scale protections for network, machines and accesses
Protection framework should be modular/adaptive depending on site business criticality

Visibility

Get a clear vision of the assets to protect based on inventory/cartography (physical and functional) and risks analysis to define a progressive roadmap

Detect & react

Capability to detect attacks on all machines connected to the industrial networks, but also the abnormal behaviors

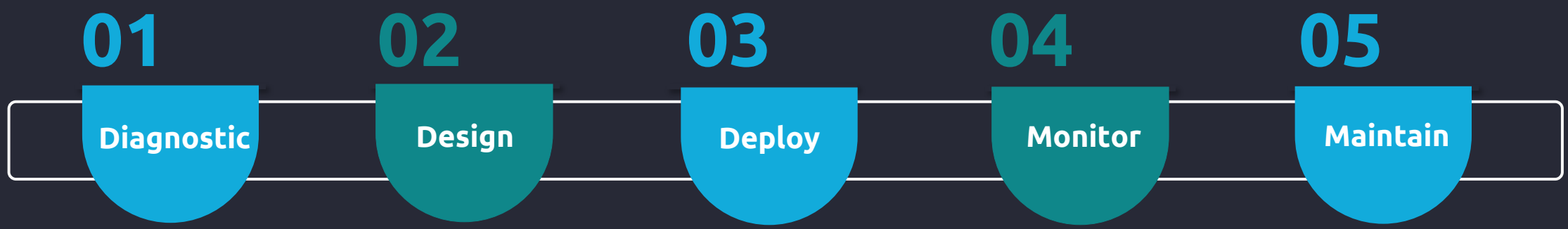
Maintain the level of resilience

Anticipate new offers to improve production efficiency which paradoxically increases the cyber risks (i.e., greater IT connections) and supports the transition to industry 4.0

All this must be adapted to OT context :
Security & **Safety** consistency,
taking into account **Operations Constraints** (eg machine availability for patching, machine allocated to function and not individual)
respecting **Performance** & Technology Constraints (eg latency, network band with, machine CPU/memory, OS obsolescence)
and being compliant with **local/business regulations**

Securing an industrial system is a long journey to go step by step based on a compromise with risks, compliance, costs and timeline

To reach the “OT excellence”, we propose 5 service components to support the client increasing his maturity along the journey



With MICROSOFT Solutions we are covering the Diagnostic and Monitor service components.

OT/IIOT High-Level Architecture and Value

- **OT Asset Discovery and Management**

  Agentless discovery showcasing what devices are doing and how they are communicating.

- **Risk and Vulnerability Analysis**

  What are the risk associated and mitigation impacting OT environment. Periodic updates and vulnerability detection.

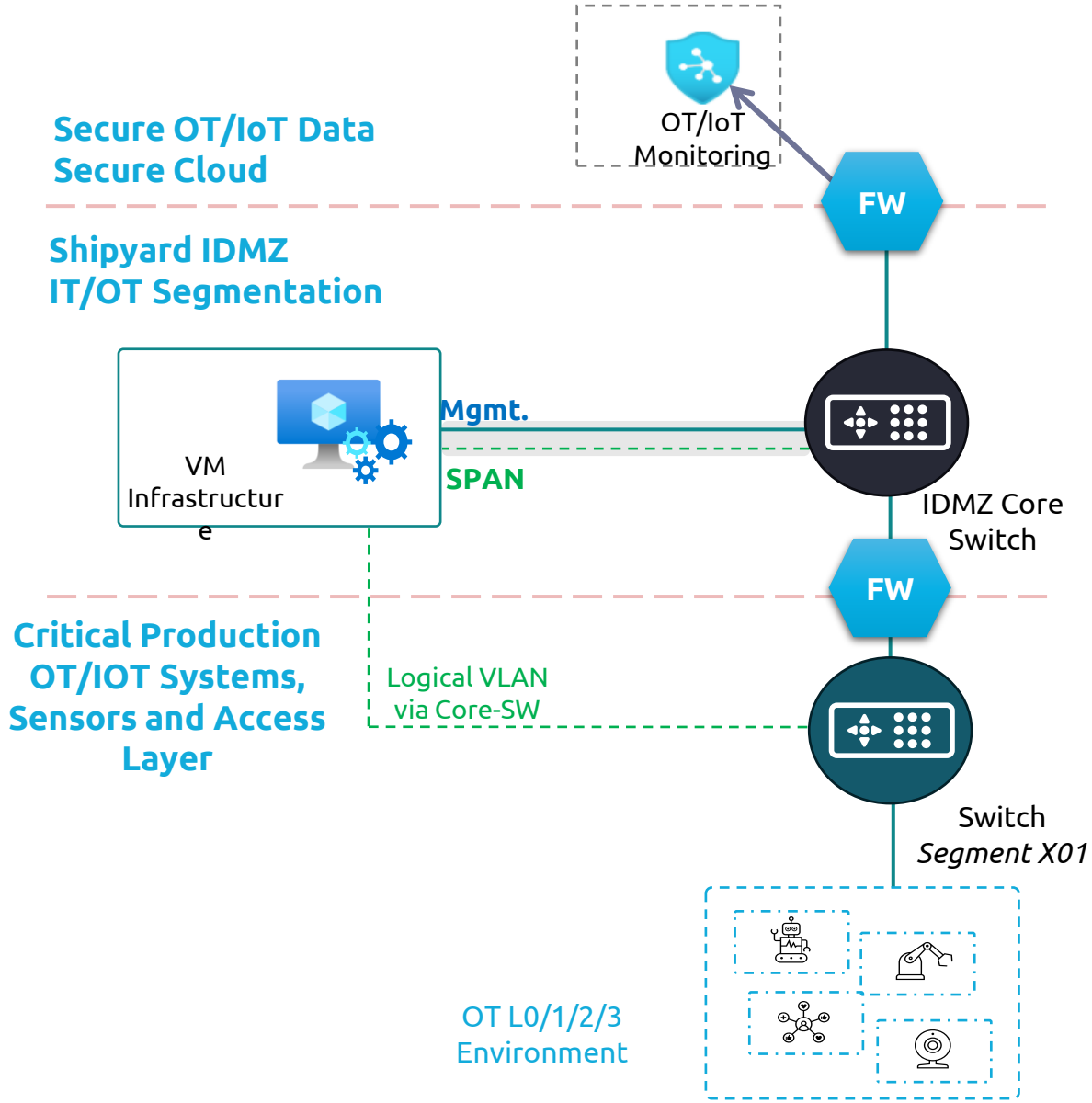
- **Continuous OT monitoring**

  Real time monitoring for traffic and vulnerabilities.

  Detects anomalous communication between plant devices.

- **Unified Security Monitoring and Governance**

  Single pane of glass for visibility with built-in reporting structure



Physical Connections

Logical Connections

Trunk Connection

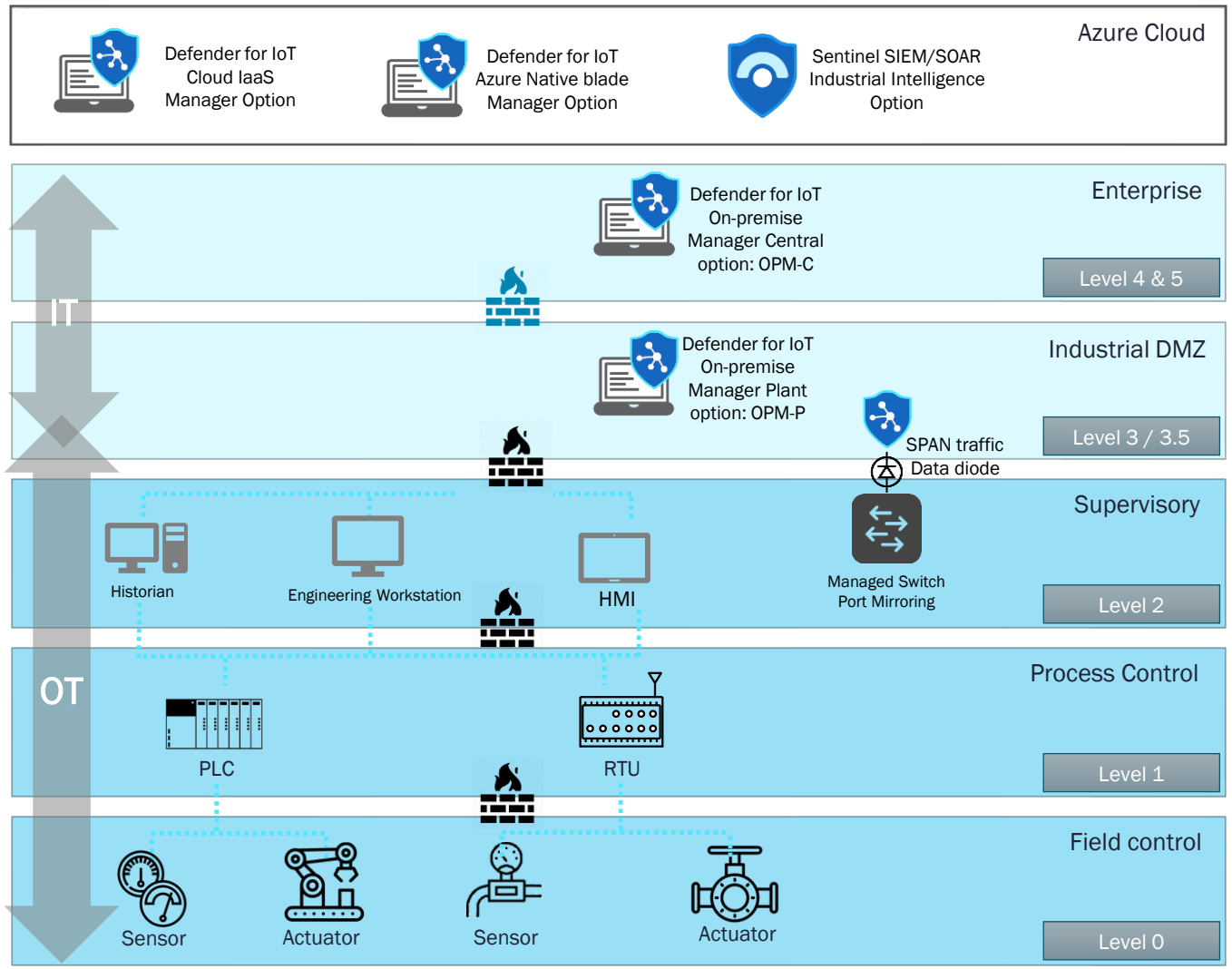
VM Instance Config

vCPU: 8

Memory: 32 GB

Storage: 500 GB (300 IOPS)

Secure Reference Architecture Design and Roadmap



5 SOC and SIEM integration - Tuning and Baselining

4 On Boarding Cloud-Connected Sensors

3 Passive D4IoT Sensor Placement in OT Traffic Configure Traffic mirroring

2 OT Traffic Flows and Topology evaluation / analysis for optimal sensor placement and sampling

1 Scan config and port validation Wireshark traffic analysis SPAN / TAPS identification (optional) PCAP file

IT Security Analysts / Responders

Capgemini

Managed Detection and Response
Using Microsoft Security (L1 & L2)
- Sentinel Design and Deployment Fastrack
- Log Optimization and Storage options
- Use Case Factory
- Custom Alerts
- Cyber Forensics
- Vulnerability Management
- Threat Hunting

6 OT Security Analysts / Responders

Respond to OT Security alerts from OT probes on the industrial network

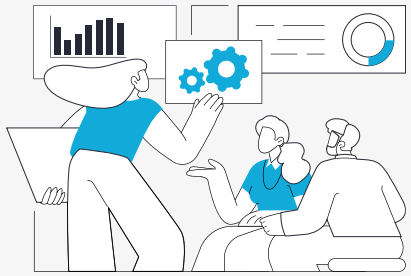
Respond to Abnormal OT behavior alerts from OT probes, including baseline management (Nozomi, Claroty etc.)

OT-IT Perimeter Firewall — FORTINET paloalto NETWORKS

Industrial Protocol Firewall — FORTINET

Progressive OT Detection regarding client risks

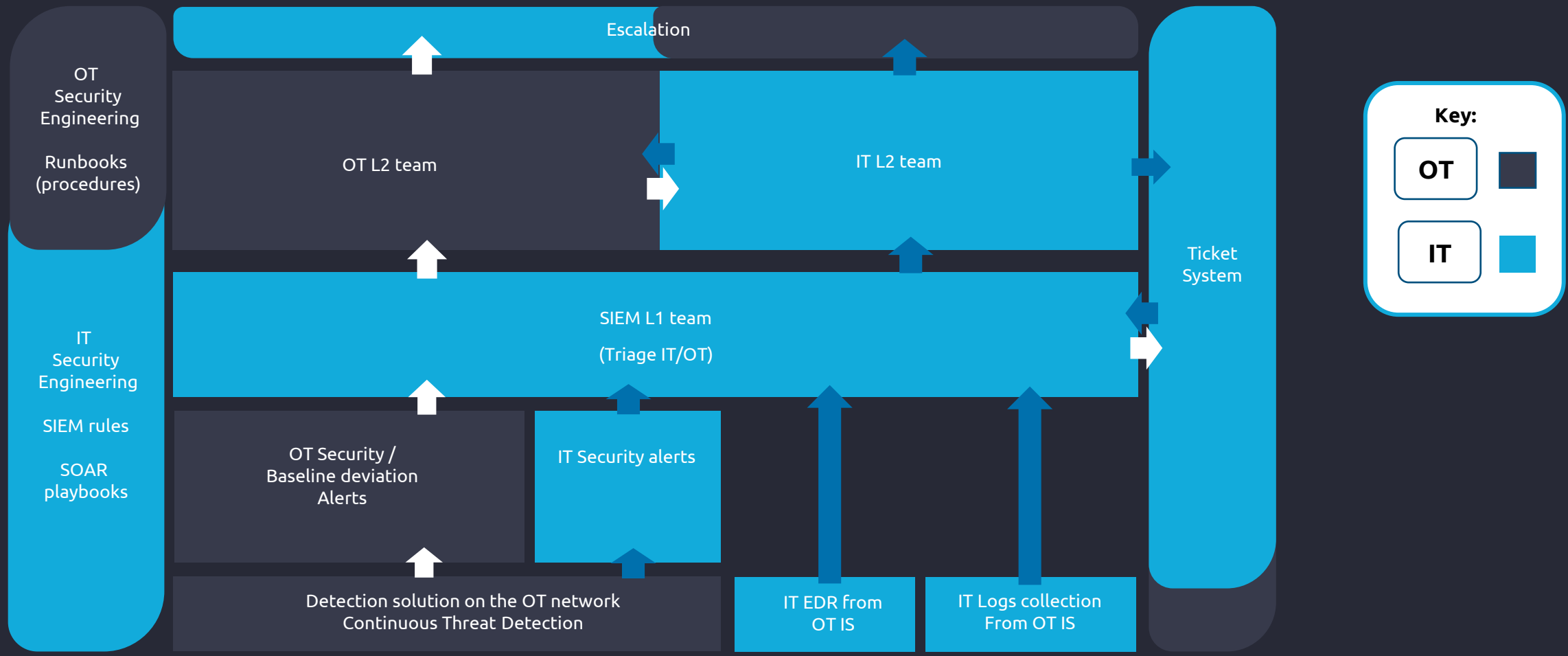
IT Security Alerts	OT Security Alerts	OT Abnormal behavior Alerts
▪ Known threat on the IT devices of the OT Network	▪ Known threat detection on OT devices ▪ Multiple scans on the OT Network ▪ Suspicious activity on the OT network (ie DDOS)	▪ Unauthorized PLC configuration modification e.g. deviation from known operating parameters ▪ PLC mode change e.g. Start/stop ▪ Unauthorized device on OT network ▪ Unauthorized Remote Access to OT Network ▪ Excessive login attempts ▪ …
Using log collection and the SIEM	Using OT probe on the Industrial network	Using OT probe on the Industrial network, including baseline management (Nozomi, Claroty …)



Preventative Actions

- Hygiene score follow up including OT Vulnerability Scanning
- Single problems / weaknesses / incidents will be checked across all factories
- Leverage feedback from other client engagements from Capgemini OT Knowledge base
- OT probe MRO, including detection use cases upgrade
- Support to cybersecurity representative at the factory

Integrated solution to existing IT SOC



A dedicated cybersecurity leader per factory

This person with the perfect knowledge of the shopfloor and the industrial process will be the decision maker for any remediation plan.

Advantages of a converged IT/OT supervision

Processes, tools and analysts mutualization to improve efficiency

Unique process
Consistency in the management of incidents whatever asset is connected on the IT network or the Industrial network (eg HMI)

Unique SIEM & ticketing tool
Standard operational procedure for L1
Deeper OT technical understanding for L2
Same SecEng team for detection improvement

Unique Team
Ease detection & mitigation if IT and OT compromission
Unique dashboards

With also an easier scalability

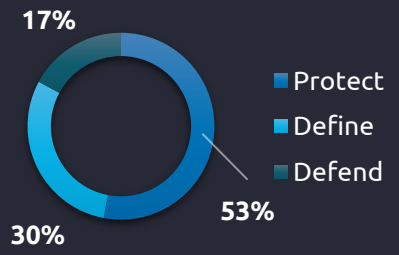
2 types of evolution:

- New perimeter (e.g. factories):
  - No impact on supervision coverage (same type of alerts)
  - Increased log telemetry and alerts (more assets)
- New events type (EDR, log collection,…):
  - Need to develop specific rules and SOP (but only for equipment not existing in the IT network)
  - Increased log telemetry and alerts

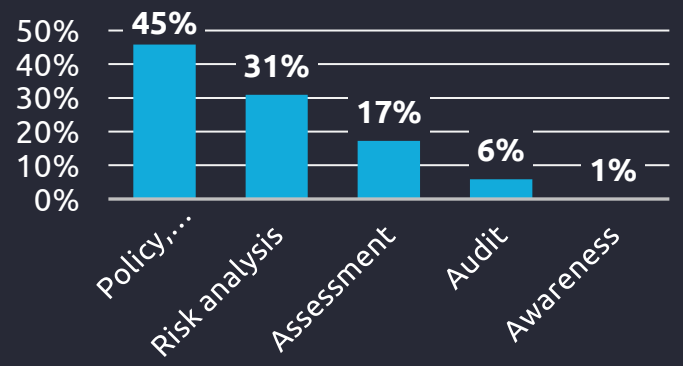
Why Capgemini ?

Because of our Cybersecurity OT experience based on close to 500+ projects for 100+ clients (multi sectors) delivered by 200 consultants world wide in the past 10 years. Also currently monitoring 300 factories

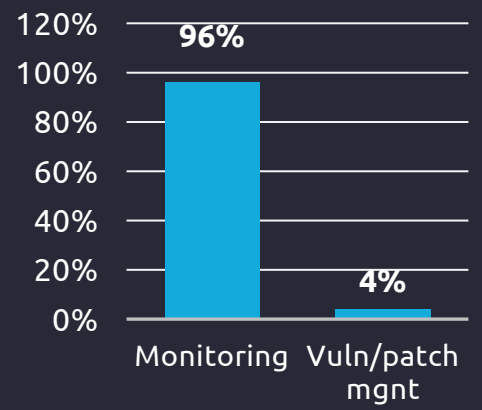
Portfolio Split



Define



Defend



10 % Junior
30 % Confirmed
40% Senior
20% Expert

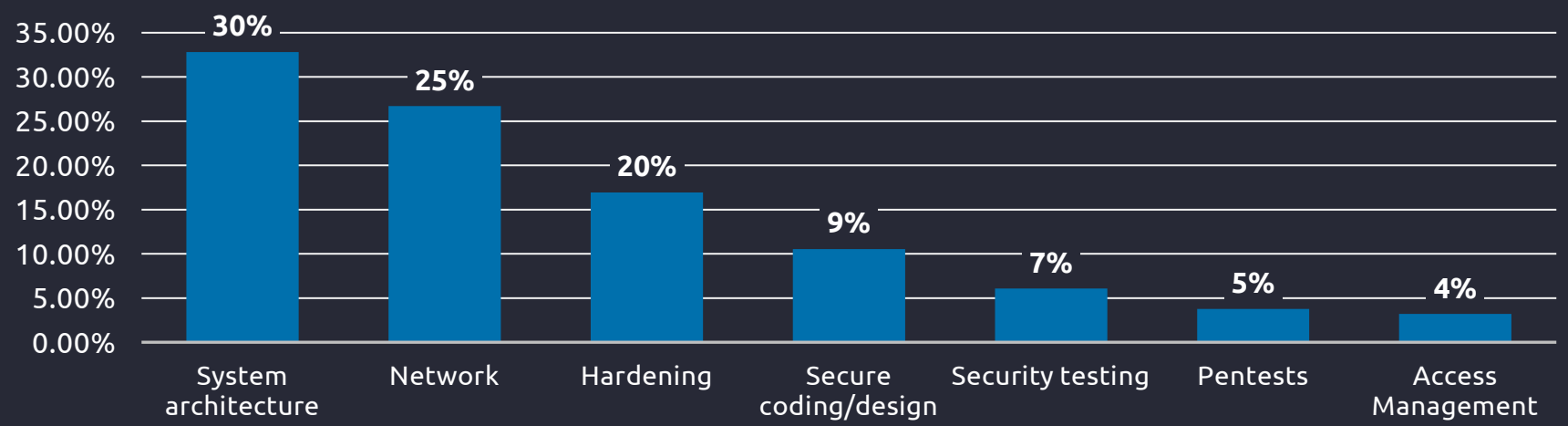
60%

20%

30%

20%

Protect



Large experience in monitoring Factories

- Global partner for **200 factories**
- Claroty, QRadar
- L1 – 3rd party SOC, OT L2 Capgemini India & France

- Scaling from **30 factories**
- Claroty
- L1 – Asahi SOC, OT L2 Capgemini India

- Scaling from **16 factories**
- Claroty, Splunk
- L1 – Capgemini UK SOC, OT L2 in India

- Scaling from **10+ factories**
- Nozomi and Industrial Defender
- Capgemini Spain dedicated SOC (L1/L2)

- Scaling from **3 factories**
- Azure Defender, Sentinel
- L1 – Capgemini UK SOC, OT L2 in India

- Scaling from **20 factories**
- Claroty
- L1 – Capgemini UK SOC, OT L2 in India

The client names in this slide are shared strictly under NDA and cannot be mentioned/quoted/published.

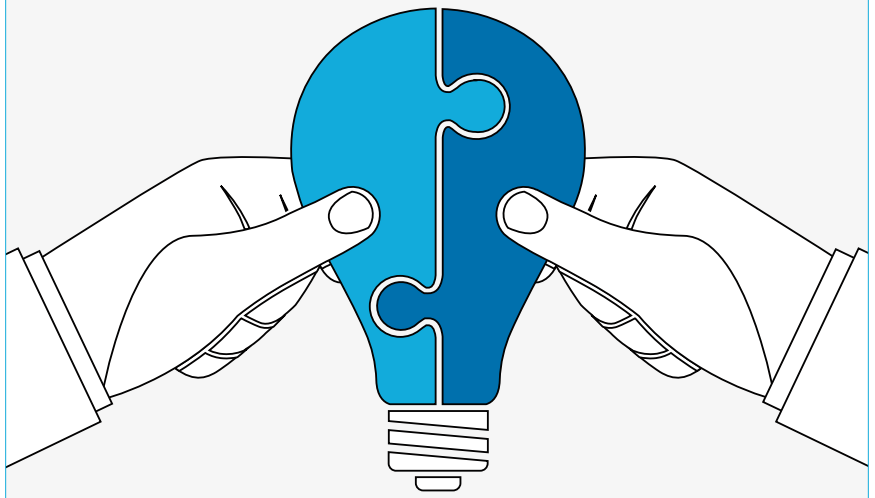
Better Together – Capgemini and Microsoft

Business-focused approach embracing continuous technology transformations

Proven partner for consulting and managed security services

Presence on **5** continents, **40** countries with **4500+** skilled professional experts.

Cybersecurity professionals operating from **14 CDCs** holding Industry leading Security Certifications.



Synergize together for security

Microsoft Azure expert and **Gold Certified Provider** running Azure Sentinel.

22+ years of bond with Microsoft driving cloud transformat-ions.

Cloud first way of working with Microsoft

Uses Accelerated Delivery Centers and **Rightshore® Delivery** method

Ensures **organisational security** with innovated technology and delivery.

Let’s qualify the client need to build a joint proposal

Thank you!

Capgemini