Security Operations : In-house vs Outsourced

Anna Webb

Head of Security Operations

11th October 2022

Kocho

BECOME GREATER

Agenda

- Business Considerations
- Business Drivers
- Stakeholders
- Target Operating Model
- Current Infrastructure
- Who do you need?
- Typical SOC
- In-House Delivery
- Fully Managed Delivery
- “Hybrid” Blended Delivery

Business Considerations

- Type of business
- Number of locations
- Number of staff
- Hours of business
- Hours of operation
- On-site
- Remote
- Hybrid
- Regulation / Legislation

Business Drivers for Security Operations

- → Security
- → Insurance
- → Regulatory Compliance
- → Reputation
- → Competitiveness
- → Previous breach

Who are your stakeholders?

- CTO / CISO
- Head of Security
- Finance
- Business Operations
- Head of IT
- Compliance
- ICO

Target Operating Model

People

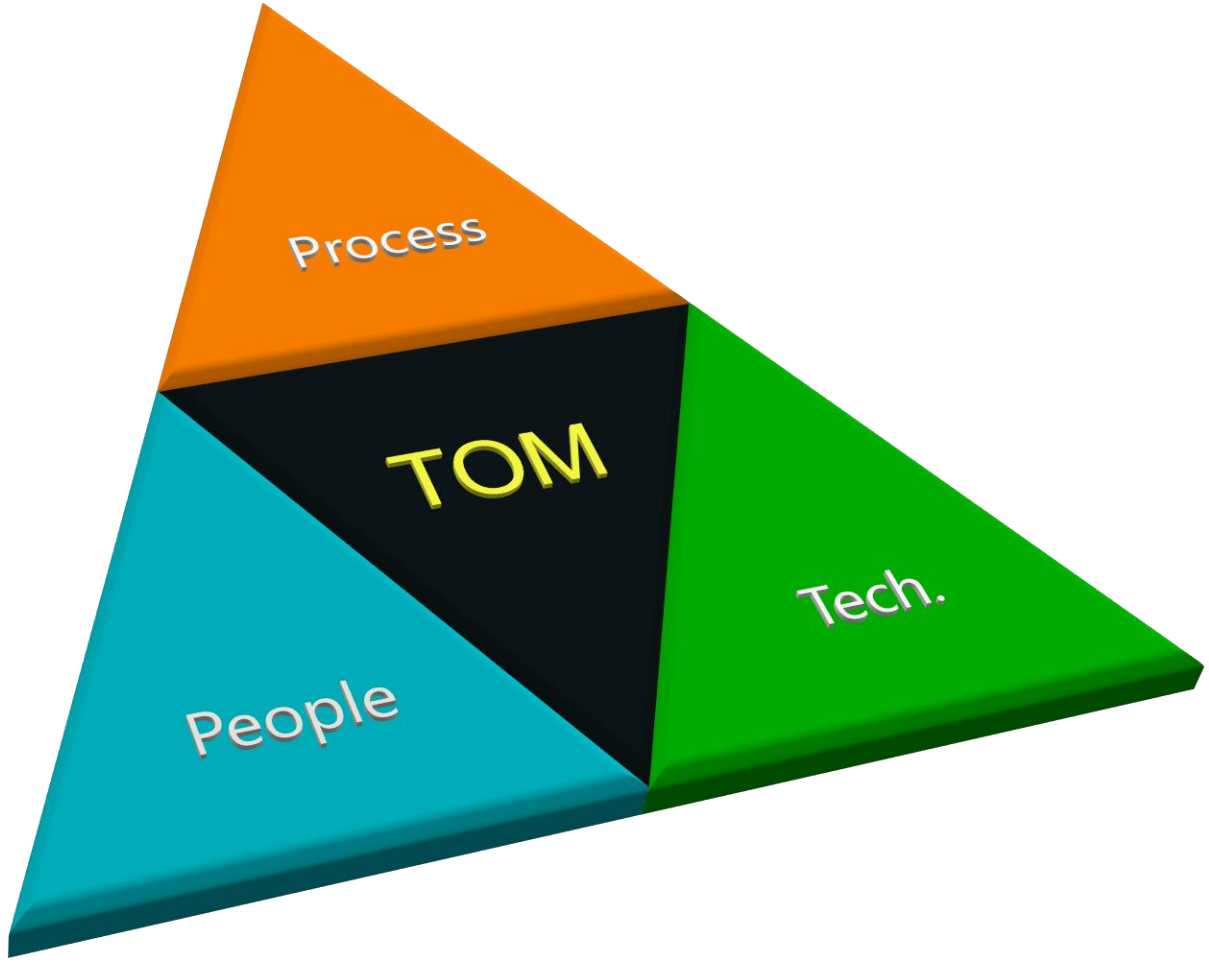
- Who do you need?
- What Roles?
- How many?

Process

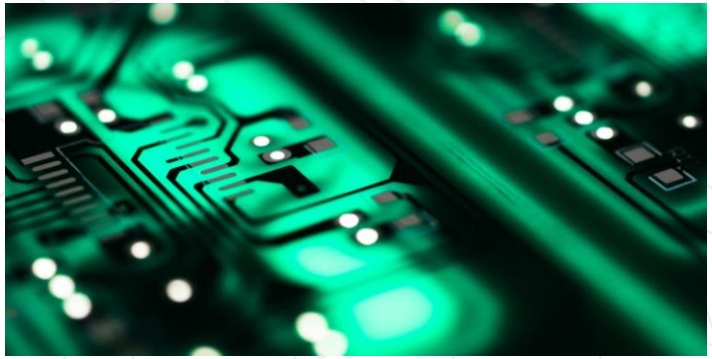
- Repeatable
- Easy to follow
- Company wide

Technology

- What kind?
- Underlying Infrastructure
- On-Prem / Cloud / Hybrid



Current Infrastructure



On-Prem

- Physical Servers / Equipment
- Workstations - Desktops / Laptops
- Operating systems / Software
- Active Directory
- Legacy Systems

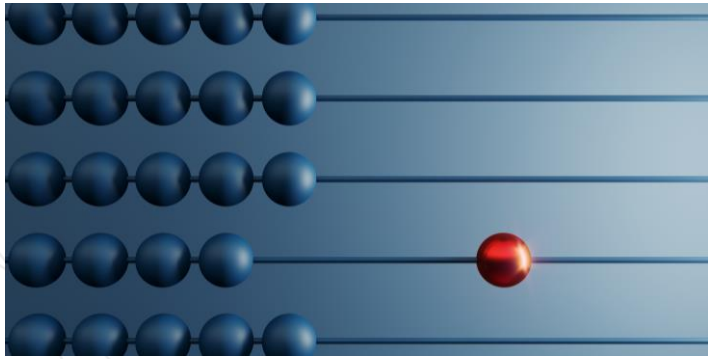
Hybrid

- Endpoints – Mobiles etc
- IoT
- AD – Password Hash sync
- APIs

The Cloud

- Azure / AWS etc
- AAD
- O365
- SaaS / IaaS / PaaS
- Containerisation

People - Who do you need?



Who?

- SOC Manager
- Architect
- Tier 1 Analyst
- Tier 2 Analyst
- Tier 3 Analyst

How Many?

- SOC Manager x 1
- Architect x 1
- Tier 1 - circa 2 – 5
- Tier 2 - circa 2 – 3
- Tier 3 - 1 or 2

How Much?

- £80k - £120k
- £65k - £80k
- £25k - £35k
- £35k - £45k
- £40k - £55k

Typical SOC

SOC Capability

- Threat Intelligence
  - Analytics & Alert Config
  - Trend Analysis
  - Vulnerability Management
- Event Management
- Incident Management
- Risk Management
- Reporting
- Security Strategy
- Capability Model

People

- Recruitment
  - Security Vetting
  - Career Framework
  - Retention
- Skills & Experience
  - Training & Development
- Segregation of Duties

Process

- Documentation
  - Governance
  - Compliance

Technology

- Support & Management
- Tuning & Optimisation
- Risk/Scope Analysis
- Log Sources
  - Queries
  - Retention
  - Destruction

In-House Delivery

People

- SOC Manager
- Analyst – Tier 1,2,3
- Associated Costs
  - Base Salary
  - Pension
  - Benefits
  - Bonus
  - Holiday
- On-Call / Shift
- Training
- Recruitment

Process

- Incident Management
- Problem Management
- Change Management
- Security Incident Mgt
- Emerging Threats
- JML – Security specific
- Staff Onboarding
- Process review
- Reporting
- DR/ BCP
- ISO27001?

Technology

- Hardware, Software
- On-Prem or Cloud
- Licensing
- Applications
- Storage
- Virtual Appliances
- Password Management
- Development of the technology
- Improvements
- Maintenance / Downtime

Typical Costs - £240k - £680k+/year Approx.

Small
£240k+/year
Approx.

Medium
£460k+/year
Approx.

Large
£680k+/year
Approx.

Fully Managed Delivery

People

- ✓ SOC Manager
- ✓ Analyst – Tier 1,2,3
- ✓ Associated Costs
  - ✓ Base Salary
  - ✓ Pension
  - ✓ Benefits
  - ✓ Bonus
  - ✓ Holiday
- ✓ On-Call / Shift
- ✓ Recruitment / Training
- ✓ Clearances

Process

- ✓ Incident Management
- ✓ Problem Management
- ✓ Change Management
- ✓ Security Incident Mgt
- ✓ Emerging Threats
- ✓ JML – Security specific
- ✓ Staff Onboarding
- ✓ Process review
- ✓ Reporting
- ✓ DR/ BCP
- ✓ Accreditation / ISO27001?

Technology

- ✓ Hardware, Software
- ✓ SIEM / SOAR
- ✓ Licensing
- ✓ Storage
- ✓ Virtual Appliances
- ✓ Password Management
- ✓ Development
- ✓ Improvements
- ✓ Maintenance / Downtime
- ✓ Leverage Technology partner

Typical Costs - £50k - £550k+/year Approx

Small
£50k+/year
Approx.

Medium
£250k+/year
Approx.

Large
£550k+/year
Approx.

"Hybrid" (Blended) Delivery

People

- IT / Security Manager
- Smaller In-House team
- ✓ Reduced costs around staff
- ✓ 24 x 7 Provided by Managed Service
- ✓ Training can be provided by Managed Service provider
- ✓ Reduced recruitment burden
- ✓ Support from the Managed Service Provider

Process

- ✓ Incident Management
- ✓ Problem Management
- ✓ Change Management
- ✓ Security Incident Mgt
- ✓ Emerging Threats
- ✓ Reporting
- ✓ Support for DR/ BCP
- ✓ Support for Accreditation / ISO27001?
- Typically will feed into any client's base processes

Technology

- ✓ Overall responsibility for installation, maintenance and improvement of the SIEM / SOAR can lie with Managed Service provider
- ✓ Tech for analysts etc
- ✓ Leverage Technology partner
- Log Ingestion /Retention
- Licensing

Typical Costs - £30k - £350k+/year

Small
£30k+/year
Approx.

Medium
£120k+/year
Approx.

Large
£350k+/year
Approx.

Kocho

BECOME GREATER

Thank you

→ Any questions?