TechCorp SME Network Architecture & SOC Scenario

Company Profile: TechCorp Manufacturing A/S

Business: Industrial manufacturing and automation solutions
Size: 150 employees
Locations:

- **Corporate HQ** (Copenhagen) - Administration, IT, Engineering
- **Factory 1** (Aarhus) - Primary manufacturing facility
- **Factory 2** (Odense) - Secondary production & packaging facility **Industry:** Manufacturing (automotive parts & industrial components)
  Security Maturity: Growing (recently invested in SOC capabilities due to increased cyber threats against manufacturing)

Network Architecture Overview

Multi-Site Infrastructure

```
┌──────────────────────────────────────────────────────────────────────────────────┐
│                          TECHCORP MANUFACTURING NETWORK                          │
│                                                                                  │
│  Internet ◄──────────────────────► Corporate WAN ◄───────────────────────┐       │
│     │                                    │                               │       │
│     ▼                                    ▼                               ▼       │
│ ┌───────────────────────────────┐ ┌────────────────────────┐ ┌─────────────────┐ │
│ │        CORPORATE HQ           │ │      FACTORY 1         │ │   FACTORY 2     │ │
│ │       (Copenhagen)            │ │      (Aarhus)          │ │   (Odense)      │ │
│ │                               │ │                        │ │                 │ │
│ │ ┌─────┐  ┌─────┐  ┌─────────┐ │ │ ┌─────┐  ┌───────────┐ │ │ ┌─────┐  ┌────┐ │ │
│ │ │ FW  │◄►│ DMZ │◄►│IT/Admin │ │ │ │ FW  │◄►│Production │ │ │ │ FW  │◄►│Prod│ │ │
│ │ └─────┘  └─────┘  └─────────┘ │ │ └─────┘  └───────────┘ │ │ └─────┘  └────┘ │ │
│ │                               │ │                        │ │                 │ │
│ │ • Domain Controller           │ │ • SCADA Systems        │ │ • PLC Network   │ │
│ │ • File/Mail Servers           │ │ • HMI Workstations     │ │ • Quality Ctrl  │ │
│ │ • Admin Workstations          │ │ • Production Line PCs  │ │ • Packaging     │ │
│ │ • Engineering Workstations    │ │ • Manufactur. Systems  │ │ • Shipping      │ │
│ └───────────────────────────────┘ └────────────────────────┘ └─────────────────┘ │
│                                                                                  │
└──────────────────────────────────────────────────────────────────────────────────┘
```

Technical Infrastructure

Network Segments:

Corporate HQ (Copenhagen):

- **External:** `0.0.0.0/0` (Internet)
- **DMZ:** `172.16.100.0/24` (Public-facing services)
- **IT LAN:** `192.168.10.0/24` (Admin & office workstations)
- **Server VLAN:** `192.168.20.0/24` (Corporate servers)

- **Engineering:** `192.168.30.0/24` (CAD/Engineering workstations)
- **Management:** `192.168.99.0/24` (Network equipment)

Factory 1 (Aarhus) - Primary Manufacturing:

- **Production IT:** `10.1.10.0/24` (Manufacturing IT systems)
- **SCADA Network:** `10.1.20.0/24` (Supervisory control systems)
- **PLC Network:** `10.1.30.0/24` (Programmable Logic Controllers)
- **HMI Network:** `10.1.40.0/24` (Human Machine Interfaces)
- **Safety Systems:** `10.1.50.0/24` (Emergency shutdown systems)

Factory 2 (Odense) - Secondary Production:

- **Production IT:** `10.2.10.0/24` (Manufacturing IT systems)
- **PLC Network:** `10.2.30.0/24` (Packaging & quality control)
- **HMI Network:** `10.2.40.0/24` (Operator interfaces)

Key Systems:

Corporate HQ Systems:

System	IP Address	Role	OS	Critical
Domain Controller	192.168.20.10	DC01-TCORP	Windows Server 2019	3
File Server	192.168.20.15	FS01-TCORP	Windows Server 2019	3
Web Server	172.16.100.10	WEB01-TCORP	Linux Ubuntu	2
Mail Server	172.16.100.20	MAIL01-TCORP	Linux Ubuntu	3
ERP Database	192.168.20.25	ERP01-TCORP	Windows Server 2019	3
Engineering Server	192.168.30.10	CAD01-TCORP	Windows Server 2019	2
Backup Server	192.168.20.35	BACKUP01-TCORP	Linux Ubuntu	2
HQ Firewall	172.16.100.1	FW-HQ-TCORP	Cisco ASA 5516	3

Factory 1 (Aarhus) OT Systems:

System	IP Address	Role	OS/Platform	Critical
SCADA Server	10.1.20.10	SCADA01-F1	Windows Server 2016	4
Historian Database	10.1.20.15	HIST01-F1	Windows Server 2016	3
HMI Station 1	10.1.40.20	HMI01-F1	Windows 10 IoT	3
HMI Station 2	10.1.40.21	HMI02-F1	Windows 10 IoT	3
Production Line PLC	10.1.30.50	PLC-LINE1	Siemens S7-1500	4
Packaging PLC	10.1.30.55	PLC-PACK1	Allen-Bradley	3
Safety PLC	10.1.50.10	PLC-SAFE1	Pilz Safety	4
Factory 1 Firewall	10.1.10.1	FW-F1-TCORP	Fortinet FortiGate	3

Factory 2 (Odense) OT Systems:

System	IP Address	Role	OS/Platform	Critical
HMI Station	10.2.40.20	HMI01-F2	Windows 10 IoT	3
Quality Control PLC	10.2.30.60	PLC-QC2	Siemens S7-1200	3
Packaging Line PLC	10.2.30.65	PLC-PACK2	Allen-Bradley	3
Factory 2 Firewall	10.2.10.1	FW-F2-TCORP	Fortinet FortiGate	3

Employee Workstations & Users:

Corporate HQ (Copenhagen):

- **Management:** `192.168.10.10-19` (CEO, Production Director, CFO)
- **Engineering:** `192.168.30.20-49` (Design engineers, process engineers)
- **IT/Admin:** `192.168.10.80-89` (IT administrators, system engineers)
- **Sales/Admin:** `192.168.10.60-79` (Sales, HR, accounting)

Factory 1 (Aarhus) - 65 employees:

- **Production IT:** `10.1.10.20-39` (Production supervisors, IT support)
- **HMI Operators:** `10.1.40.20-29` (Production line operators)
- **Maintenance:** `10.1.10.40-49` (Maintenance technicians)

Factory 2 (Odense) - 35 employees:

- **Production IT:** `10.2.10.20-29` (Supervisors, quality control)
- **HMI Operators:** `10.2.40.20-25` (Packaging operators)

Common Usernames:

Corporate:

- **Management:** `ceo.andersen` , `prod.director` , `cfo.hansen`
- **IT Admins:** `admin.jensen` , `it.support` , `sysadmin.nielsen`
- **Engineering:** `eng.larsen` , `design.petersen` , `process.olsen`

Factory Operations:

- **F1 Supervisors:** `f1.supervisor` , `prod.manager.f1` , `shift.lead.f1`
- **F1 Operators:** `operator.001` , `operator.002` , `maint.tech.f1`
- **F2 Supervisors:** `f2.supervisor` , `quality.mgr.f2`
- **F2 Operators:** `pack.operator.001` , `qc.tech.f2`

SOC Monitoring Scope

IT Infrastructure Log Sources:

1. **Windows Domain Controller (DC01-TCORP)**
    - Authentication events across all sites
    - Account management (creation, lockout, privilege changes)
    - Kerberos authentication

    - Group policy changes

2. **Web Server (WEB01-TCORP)**
    - Apache access logs (customer portal, supplier access)
    - Application errors
    - Failed login attempts to admin panels
    - Suspicious HTTP requests
3. **Corporate Firewalls (All Sites)**
    - Allow/deny decisions
    - Site-to-site VPN traffic
    - Internet access from factories
    - Port scan detection
4. **DNS Server (DC01-TCORP)**
    - DNS queries from all sites
    - Malicious domain detection
    - DNS tunneling attempts
    - Unusual query patterns

OT Infrastructure Log Sources:

5. **SCADA Systems (Factory 1)**
    - Operator login/logout events
    - System alarm events
    - Configuration changes
    - Production data access
6. **HMI Workstations (Both Factories)**
    - Windows authentication logs
    - Application access logs
    - USB device connections
    - File transfer activities
7. **Factory Firewalls (F1 & F2)**
    - IT/OT network boundary traffic
    - External connections from production networks
    - Inter-factory communications
    - Maintenance remote access
8. **Industrial Network Equipment**
    - Managed switch logs (VLAN changes, port security)
    - Wireless access point logs (maintenance devices)
    - VPN gateway logs (vendor remote access)

Typical Daily Activity Patterns

Corporate HQ (Copenhagen) - Business Hours: 08:00 - 17:00 CET

- High authentication activity (arrivals, breaks, departures)
- Engineering workstation activity (CAD, design work)
- ERP system access (orders, planning, accounting)
- Email and file server usage
- Management reporting and analysis

Factory 1 (Aarhus) - Production Schedule:

- **Day Shift:** 06:00 - 14:00 (Peak production)
  - HMI operator logins at shift start
  - High SCADA activity during production runs
  - Quality control data logging
- **Evening Shift:** 14:00 - 22:00 (Continued production)
  - Shift handover procedures
  - Production line changeovers
- **Night Shift:** 22:00 - 06:00 (Maintenance & cleaning)
  - ** Limited HMI activity expected**
  - Automated systems continue
  - Planned maintenance activities

Factory 2 (Odense) - Packaging Schedule:

- **Day Shift:** 07:00 - 15:00 (Primary packaging operations)
- **Afternoon:** 15:00 - 19:00 (Shipping preparation)
- **Night:** 19:00 - 07:00 (Minimal activity, cleaning)
  - **Very limited legitimate activity**

24/7 Automated Systems:

- SCADA data collection and historian logging
- Production line sensors and monitoring
- Environmental controls (HVAC, lighting)
- Security cameras and access control
- Network infrastructure monitoring
- Backup operations (typically 02:00 AM)

Suspicious Activity Indicators:

Time-Based Anomalies:

- **Corporate users** accessing systems outside 08:00-17:00
- **Production changes** during non-shift hours
- **Engineering access** to factory systems after hours
- **Weekend activity** on production systems without scheduled maintenance

Location-Based Anomalies:

- **Corporate users** authenticating from factory networks
- **Factory operators** accessing corporate systems
- **Cross-site access** without business justification
- **External VPN** access to OT networks