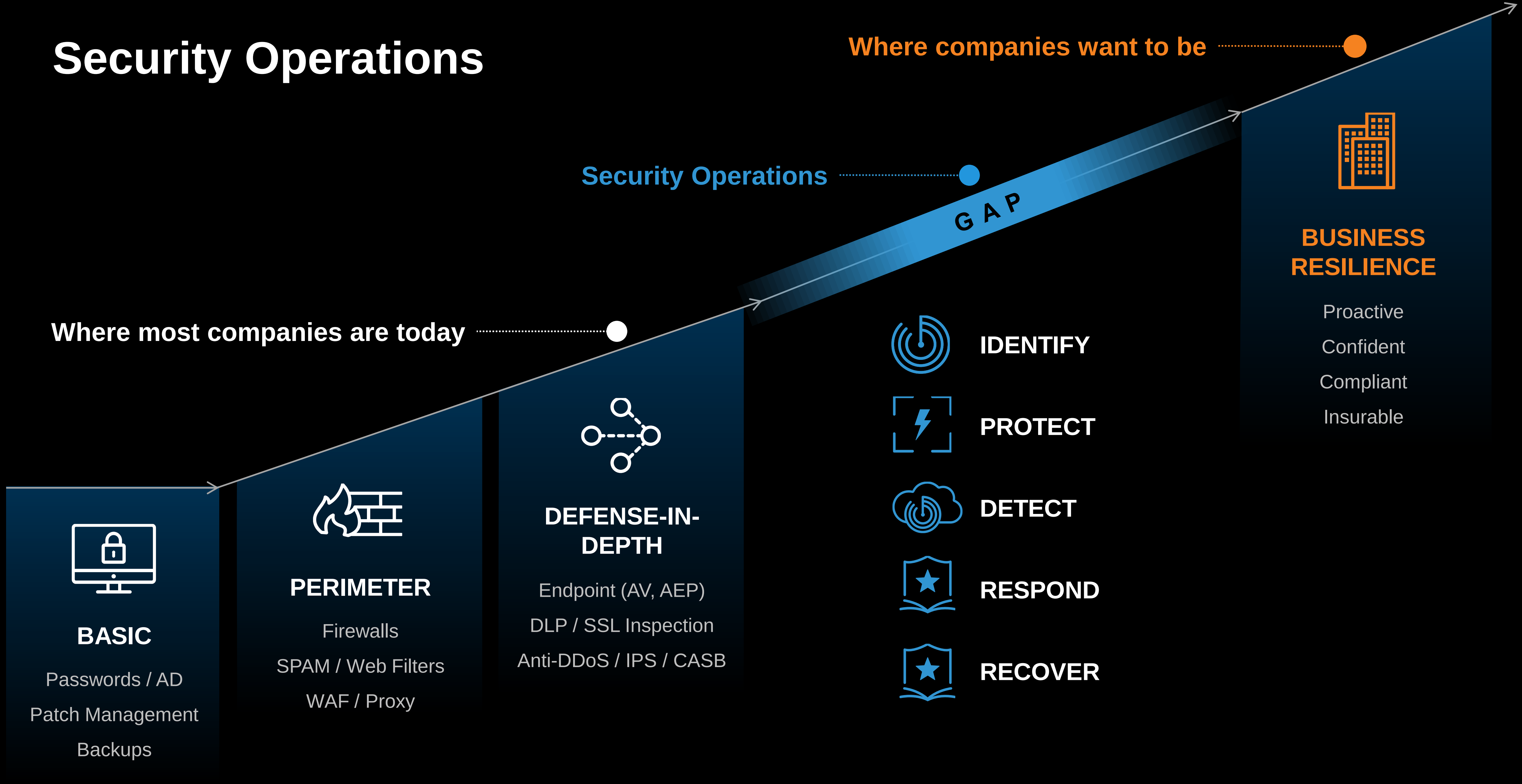
ARCTIC WOLF

THE LEADER IN SECURITY OPERATIONS

# Security + Compliance in the Nordics

Petter Glenstrup – SE Director Nordics

# Security Operations



Where companies want to be

Security Operations

Where most companies are today

GAP

**BASIC**

Passwords / AD

Patch Management

Backups

**PERIMETER**

Firewalls

SPAM / Web Filters

WAF / Proxy

**DEFENSE-IN-DEPTH**

Endpoint (AV, AEP)

DLP / SSL Inspection

Anti-DDoS / IPS / CASB

**IDENTIFY**

**PROTECT**

**DETECT**

**RESPOND**

**RECOVER**

**BUSINESS RESILIENCE**

Proactive

Confident

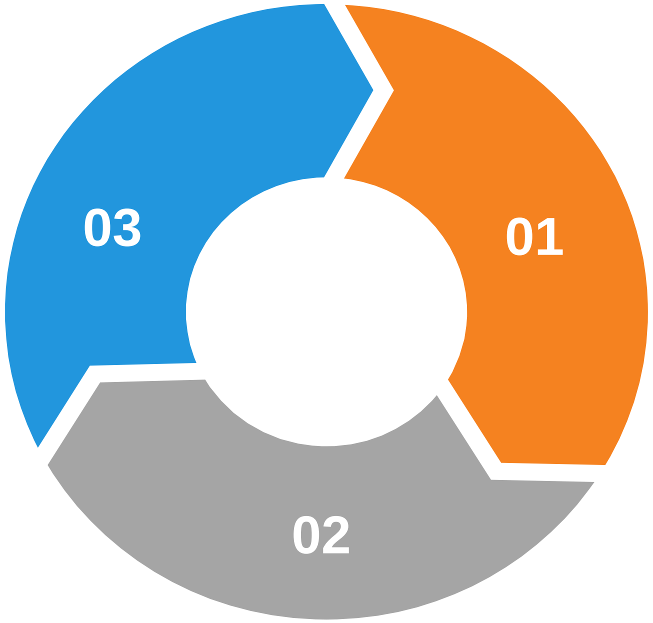
Compliant

Insurable

# Maintaining compliance in security requires people, processes and technology

*People – Hard to find / Hard to keep*

- L1-L3 Security Analysts
- Security System Specialists
- Security Manager
- SOC Manager
- CISO
- …



*Technology – Easy to buy / Hard to manage*

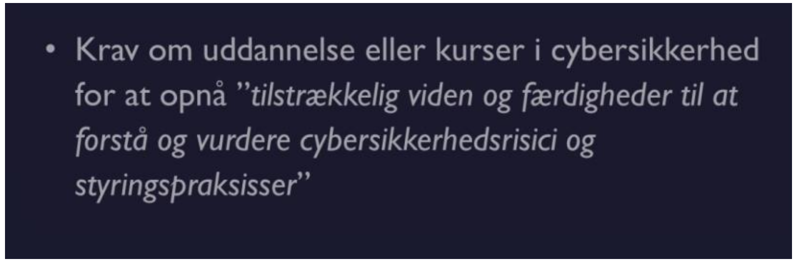
- NGFW
- EDR
- SWG
- SIEM
- SOAR
- Threat Intelligence
- NDR
- …

*Processes – Easy to forget / Easy to left halfway*

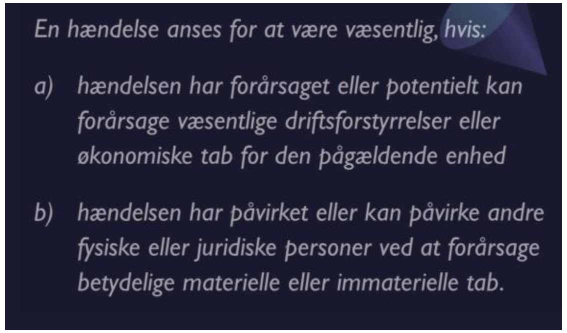
- Security Incident Management
- Incident Response Policy & Plan & Process
- Threat Hunting
- Continuous Development
- …

”The Security Triad – Technology & Processes & People (TPP)”

# Key areas



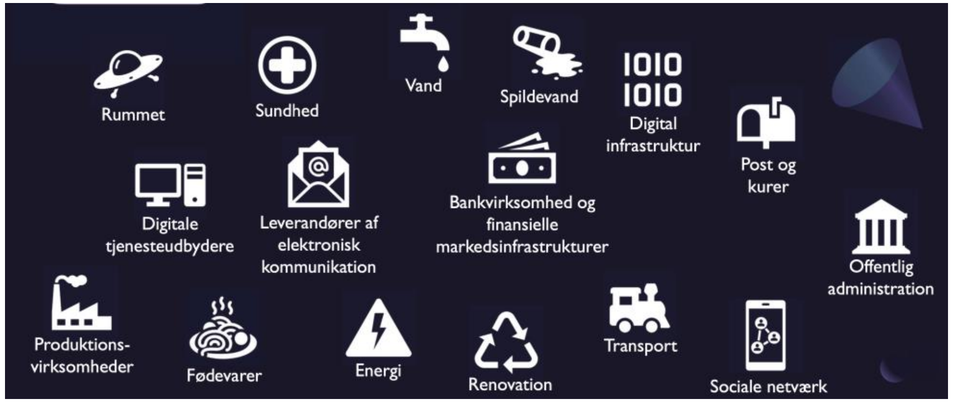
- Krav om uddannelse eller kurser i cybersikkerhed for at opnå "*tilstrækkelig viden og færdigheder til at forstå og vurdere cybersikkerhedsrisici og styringspraksisser*"

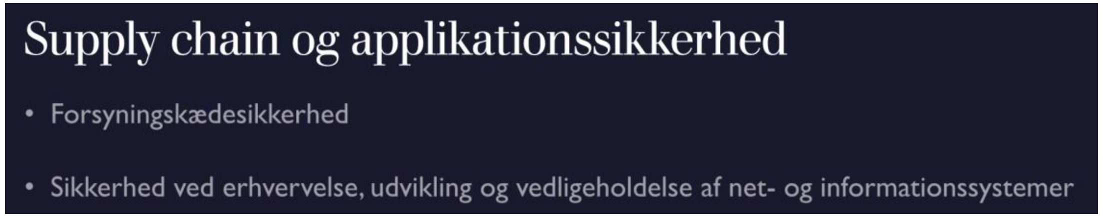


*En hændelse anses for at være væsentlig, hvis:*

*a) hændelsen har forårsaget eller potentielt kan forårsage væsentlige driftsforstyrrelser eller økonomiske tab for den pågældende enhed*

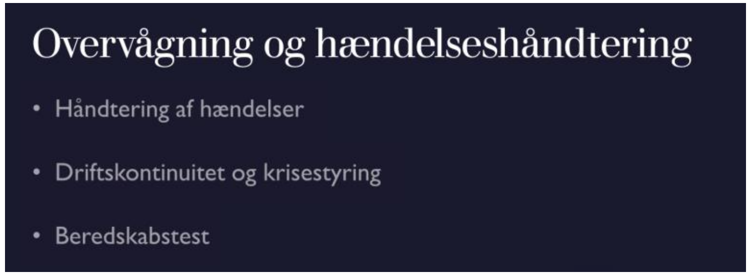
*b) hændelsen har påvirket eller kan påvirke andre fysiske eller juridiske personer ved at forårsage betydelige materielle eller immaterielle tab.*





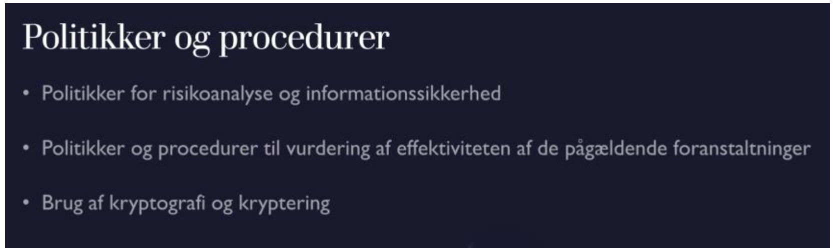
## Supply chain og applikationssikkerhed

- Forsyningskædesikkerhed
- Sikkerhed ved erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer



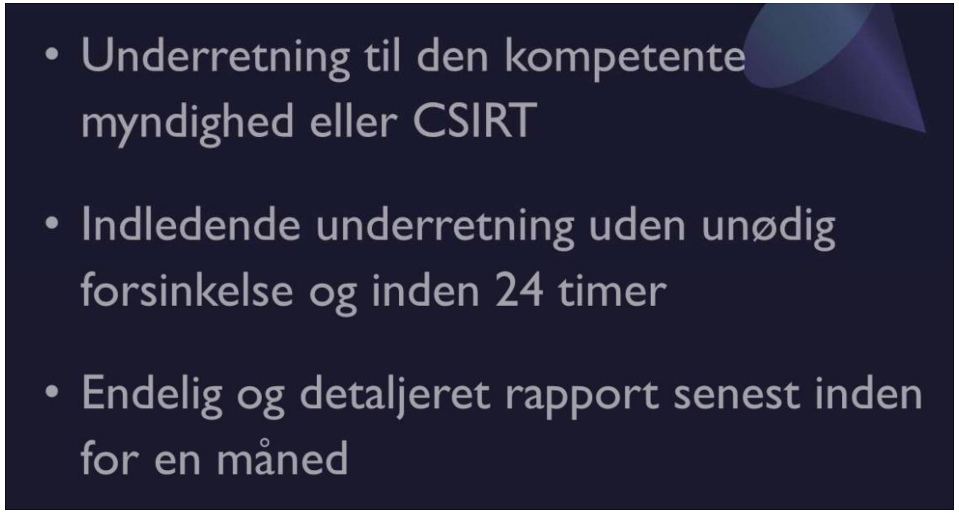
## Overvågning og hændelseshåndtering

- Håndtering af hændelser
- Driftskontinuitet og krisestyring
- Beredskabstest



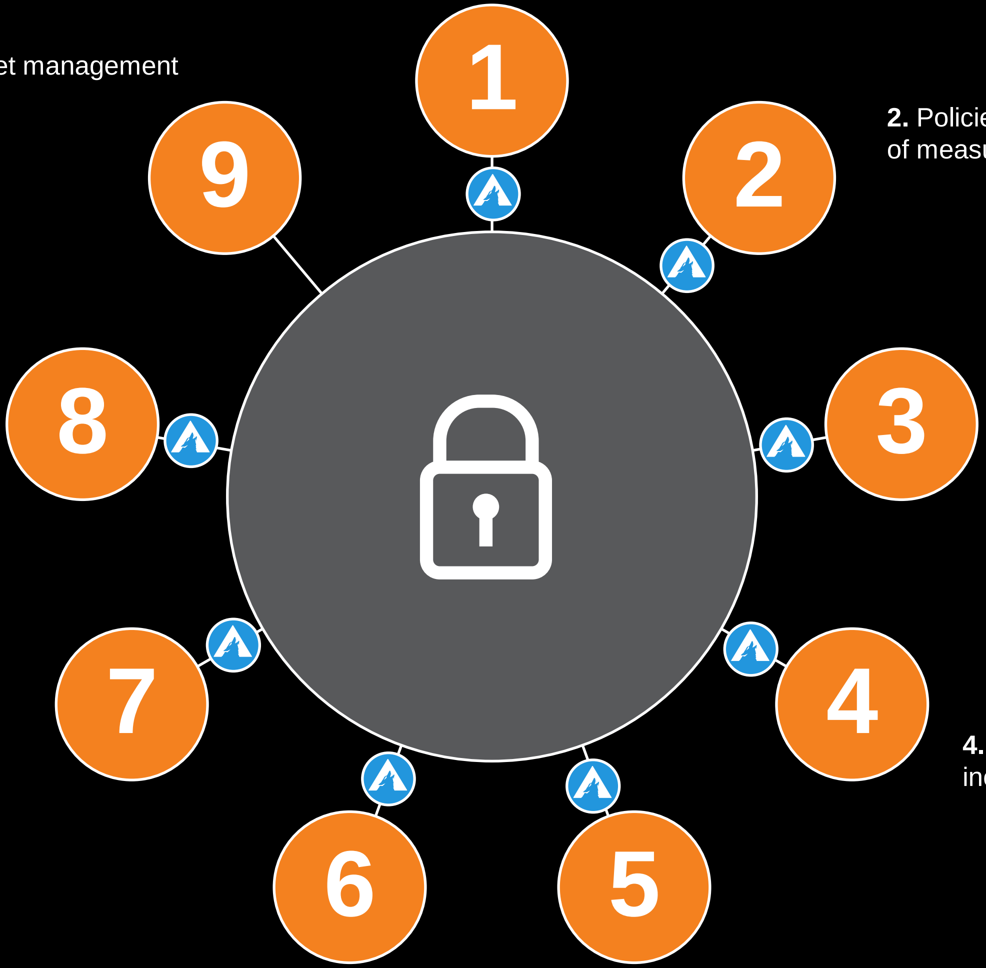
## Politikker og procedurer

- Politikker for risikoanalyse og informationssikkerhed
- Politikker og procedurer til vurdering af effektiviteten af de pågældende foranstaltninger
- Brug af kryptografi og kryptering



- Underretning til den kompetente myndighed eller CSIRT
- Indledende underretning uden unødig forsinkelse og inden 24 timer
- Endelig og detaljeret rapport senest inden for en måned

# NIS 2



**1.** Policies on risk analysis and information system security

**2.** Policies and procedures for assessing the effectiveness of measures to manage cyber security risks

**3.** Policies and procedures regarding the use of cryptography and, where applicable, encryption

**4.** incident handling (prevention, detection, and response to incidents)

**5.** Business continuity, such as backup management and disaster recovery, and crisis management

**6.** Supply chain security, including security-related aspects relating to the relationship between the individual entity and its direct suppliers or service providers

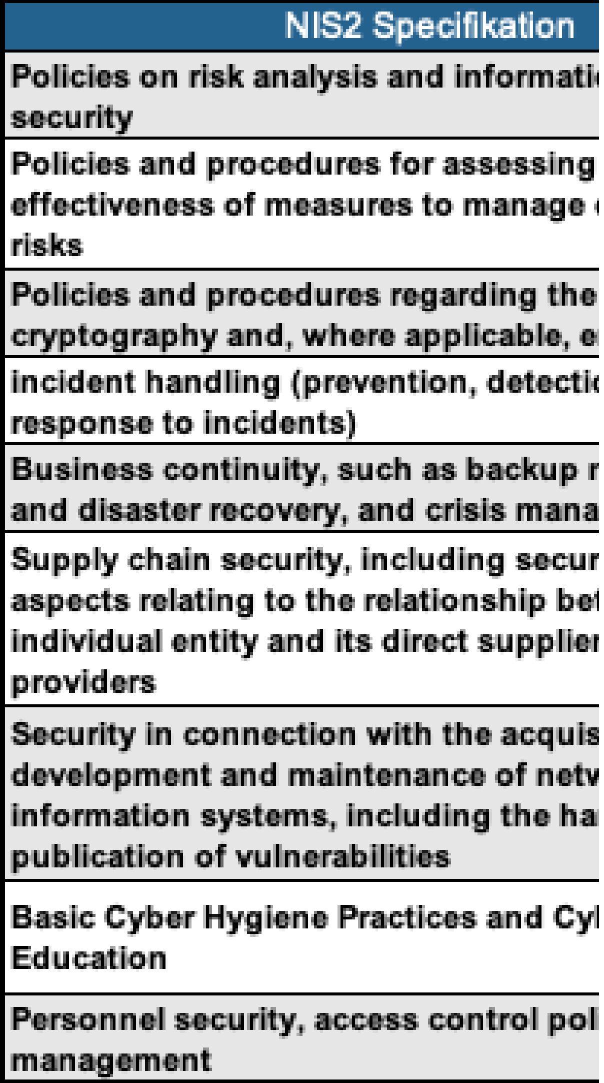
**7.** Security in connection with the acquisition, development and maintenance of networks and information systems, including the handling and publication of vulnerabilities

**8.** Basic Cyber Hygiene Practices and Cyber Security Education

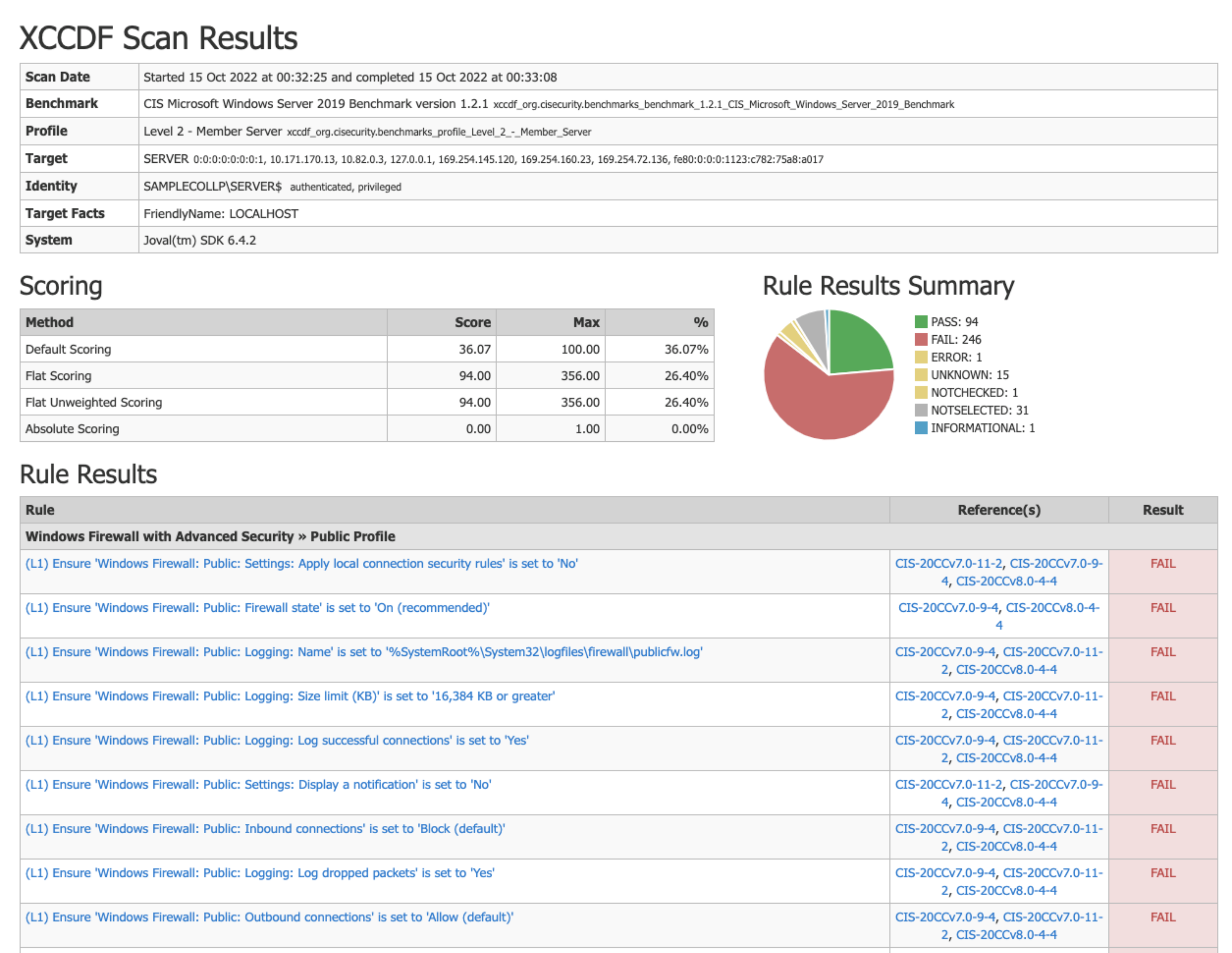
**9.** Personnel security, access control policies and asset management

**Arctic Wolf MDR, Managed Risk, Managed Security Awareness, and Incident Response**

# NIS2 Comparison Security Operation Services



| NIS2 Specifikation |
|---|
| Policies on risk analysis and informati security |
| Policies and procedures for assessing effectiveness of measures to manage risks |
| Policies and procedures regarding the cryptography and, where applicable, e |
| incident handling (prevention, detecti response to incidents) |
| Business continuity, such as backup r and disaster recovery, and crisis mana |
| Supply chain security, including secur aspects relating to the relationship bet individual entity and its direct supplier providers |
| Security in connection with the acquis development and maintenance of netv information systems, including the ha publication of vulnerabilities |
| Basic Cyber Hygiene Practices and Cyl Education |
| Personnel security, access control pol management |



## XCCDF Scan Results

| | |
|---|---|
| **Scan Date** | Started 15 Oct 2022 at 00:32:25 and completed 15 Oct 2022 at 00:33:08 |
| **Benchmark** | CIS Microsoft Windows Server 2019 Benchmark version 1.2.1 xccdf_org.cisecurity.benchmarks_benchmark_1.2.1_CIS_Microsoft_Windows_Server_2019_Benchmark |
| **Profile** | Level 2 - Member Server xccdf_org.cisecurity.benchmarks_profile_Level_2_-_Member_Server |
| **Target** | SERVER 0:0:0:0:0:0:0:1, 10.171.170.13, 10.82.0.3, 127.0.0.1, 169.254.145.120, 169.254.160.23, 169.254.72.136, fe80:0:0:0:1123:c782:75a8:a017 |
| **Identity** | SAMPLECOLLP\SERVER$ authenticated, privileged |
| **Target Facts** | FriendlyName: LOCALHOST |
| **System** | Joval(tm) SDK 6.4.2 |

## Scoring

| Method | Score | Max | % |
|---|---|---|---|
| Default Scoring | 36.07 | 100.00 | 36.07% |
| Flat Scoring | 94.00 | 356.00 | 26.40% |
| Flat Unweighted Scoring | 94.00 | 356.00 | 26.40% |
| Absolute Scoring | 0.00 | 1.00 | 0.00% |

## Rule Results Summary

## Rule Results

| Rule | Reference(s) | Result |
|---|---|---|
| **Windows Firewall with Advanced Security » Public Profile** | | |
| (L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' | CIS-20CCv7.0-11-2, CIS-20CCv7.0-9-4, CIS-20CCv8.0-4-4 | FAIL |
| (L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' | CIS-20CCv7.0-9-4, CIS-20CCv8.0-4-4 | FAIL |
| (L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log' | CIS-20CCv7.0-9-4, CIS-20CCv7.0-11-2, CIS-20CCv8.0-4-4 | FAIL |
| (L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' | CIS-20CCv7.0-9-4, CIS-20CCv7.0-11-2, CIS-20CCv8.0-4-4 | FAIL |
| (L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' | CIS-20CCv7.0-9-4, CIS-20CCv7.0-11-2, CIS-20CCv8.0-4-4 | FAIL |
| (L1) Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No' | CIS-20CCv7.0-11-2, CIS-20CCv7.0-9-4, CIS-20CCv8.0-4-4 | FAIL |
| (L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' | CIS-20CCv7.0-9-4, CIS-20CCv7.0-11-2, CIS-20CCv8.0-4-4 | FAIL |
| (L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' | CIS-20CCv7.0-9-4, CIS-20CCv7.0-11-2, CIS-20CCv8.0-4-4 | FAIL |
| (L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' | CIS-20CCv7.0-9-4, CIS-20CCv7.0-11-2, CIS-20CCv8.0-4-4 | FAIL |

# Key Areas of NIS2

- **Full insight and visibility - you can't protect what you can't see**
    - Overview and insight into the entire infrastructure – Assets inventory and Assets Management
- **Monitoring 24/7/365**
    - Based on telemetry from the entire infrastructure including cloud, OT, IaaS, SaaS, Network, Firewall, Endpoints, Identity, AD, etc.
- **Incident handling**
    - 30 min response time, root cause, remediation plan and online incident response, incident response planning.
    - Documentation and rapporting
- **Proactive identifying, documenting and planning the remediation of vulnerabilities**
    - Continuous vulnerability scans, internal, external, host, identification of vulnerabilities, documentation, prioritization and planning of remediation

Contact: Ari Gudmannsson
Email: ari.gudmannsson@arcticwolf.com
Phone: +45 31 22 10 70

# Thank You