

CHAPTER 10

Security Architecture and Cyber Resilience

Building the Digital Fortress

“Resilience is not the absence of attacks, but the ability to continue delivering value despite them. Security must be designed in; resilience must be proven.”

The network now connects the enterprise. This final chapter of Part III ensures that connection can survive contact with an adversary.

EXECUTIVE SUMMARY

For Nordic Ventures Group, cybersecurity is no longer an isolated IT concern. It is a condition for operational continuity, regulatory compliance, customer trust, and long-term competitiveness.

The organisation operates across fourteen countries, supports 6,000 users and five factories, and carries significant technical debt across twelve distributed datacentres and 140 legacy applications. This creates a broad and uneven attack surface.

A modern security architecture must therefore do more than prevent intrusion. It must help the organisation:

- understand and govern cyber risk;
- protect identities, applications, data, and infrastructure;
- detect suspicious activity early;
- contain incidents before they spread;
- restore critical operations safely;
- and learn continuously from failures and near misses.

NIST Cybersecurity Framework 2.0 organises cybersecurity outcomes into six functions: Govern,

Identify, Protect, Detect, Respond, and Recover. The addition of Govern reinforces that cybersecurity is an enterprise-risk and leadership responsibility, not merely a technical function.

For Nordic Ventures Group, cyber resilience protects more than systems. It protects factory production, revenue, regulatory standing, business relationships and the economic value promised by the wider Azure transformation.

The Security Strategy at a Glance

Security objective	Architectural response	Business outcome
Enterprise-wide risk governance	NIST CSF 2.0, security policies and accountable ownership	Consistent executive oversight
Identity protection	Zero Trust, MFA, Conditional Access and PIM	Reduced identity-based risk
Workload protection	Segmentation, private connectivity and hardened baselines	Smaller attack surface
Data protection	Classification, encryption and controlled access	Protection of sensitive information
Continuous detection	Microsoft Defender capabilities and Microsoft Sentinel	Faster threat identification
Automated response	SOC procedures, automation rules and playbooks	Reduced incident impact
Cyber recovery	Immutable backups, tested restoration and DR plans	Continued business operations

Security objective	Architectural response	Business outcome
OT resilience	Factory segmentation and Defender for IoT monitoring	Reduced production risk
Continuous compliance	Azure Policy, evidence collection and control monitoring	Better audit readiness

Microsoft's Cybersecurity Reference Architecture presents an end-to-end model spanning legacy IT, cloud, multicloud, AI, IoT, and operational technology, making it a useful target-state reference for Nordic Ventures Group's mixed environment.

1. Govern

Cybersecurity as Enterprise Risk

Security begins with governance.

The board, executive leadership, technology teams and business owners must agree on:

- risk appetite;
- critical business services;
- security ownership;
- acceptable exceptions;
- reporting thresholds;
- investment priorities;
- and escalation procedures.

Without this alignment, security becomes fragmented across countries and technology teams.

Governance at Nordic Ventures Group should establish a common security model while recognizing that risks may differ between:

- factories;
- corporate applications;
- SAP and ERP;
- AI platforms;
- development environments;

- and acquired companies.

Security Governance Structure

Governance body	Primary responsibility
Board and executive leadership	Risk appetite and strategic oversight
CISO	Enterprise security strategy and control model
CIO	Technology accountability and operational integration
Architecture Review Board	Security architecture and exception decisions
Security Operations Centre	Detection, investigation and response
Platform team	Secure-by-default cloud capabilities
Application owners	Workload risk and remediation
Factory and OT leadership	Production safety and OT resilience
Data Protection Officer	Privacy and GDPR oversight
Internal audit	Independent assurance

Business Value

Effective governance provides:

- faster security decisions;
- clearer accountability;
- improved regulatory evidence;
- stronger investment prioritization;
- and reduced inconsistency between countries.

NIS2 requires applicable entities to adopt proportionate cybersecurity risk-management measures that address areas including incident handling, business continuity,

supply-chain security, vulnerability management, encryption, access control, and asset management.

2. Identify

Understanding What Must Be Protected

An organisation cannot protect assets it does not understand.

Nordic Ventures Group requires a continuously maintained view of:

- users and privileged identities;
- applications;
- cloud resources;
- factory and OT assets;
- data;
- external connections;
- vendors;
- vulnerabilities;
- and business dependencies.

The purpose is not inventory for its own sake.

It is to understand which assets support critical business services and what would happen if they became unavailable, corrupted or exposed.

Business-Critical Asset Classification

Tier	Examples	Required protection level
Tier 1 — Mission critical	SAP, ERP, factory control integrations	Highest availability, monitoring and recovery
Tier 2 — Business critical	HR, finance, supply-chain applications	Strong controls and defined recovery
Tier 3 — Standard	Internal portals and productivity services	Standard enterprise baseline

Tier	Examples	Required protection level
Tier 4 — Experimental	Sandbox and selected AI pilots	Isolated and cost-controlled

Risk Assessment Questions

A Trusted Advisor should ask:

- Which systems can stop factory production?
- Which data is personal, commercially sensitive or safety critical?
- Which applications rely on unsupported technology?
- Which suppliers can access critical environments?
- Which identities have excessive privileges?
- Which workloads lack tested recovery?
- Which dependencies cross national or organizational boundaries?

TRUSTED ADVISOR INSIGHT *No single control saves the enterprise. What saves it is the layer nobody remembered to remove after the project ended.*

3. Protect

Security by Design and by Default

Protection should be built into the Azure platform rather than added individually by every application team.

The platform should provide approved patterns for:

- identity;
- networking;
- encryption;
- secrets;
- endpoint protection;
- vulnerability management;
- backup;
- logging;
- and secure deployment.

The goal is to make the secure path the easiest path.

Defence in Depth

The organisation should protect multiple layers.

Layer Example controls

Identity MFA, Conditional Access, PIM and access reviews

Endpoint Endpoint detection, device compliance and patching

Network Segmentation, firewalling, NSGs and private endpoints

Application Secure development, testing and managed identities

Data Classification, encryption, retention and DLP

Platform Azure Policy, Defender for Cloud and hardened baselines

Operations Monitoring, privileged workflows and change control

No single security product can protect the entire enterprise.

Resilience comes from coordinated layers that continue to provide protection when another control fails.

4. Protecting the Factory Environment

OT Security Requires a Distinct Approach

Operational technology cannot be treated exactly like traditional IT.

Factories may contain:

- industrial control systems;
- programmable logic controllers;
- human-machine interfaces;
- engineering workstations;
- sensors;
- legacy operating systems;
- and equipment that cannot be patched frequently.

Availability and physical safety may be more important than rapid software change.

Segmentation, Not Assumed Air-Gapping

Microsegmentation and network isolation reduce exposure, but they should not automatically be described as air-gapping.

A true air gap implies no direct network connection. Many modern factories require controlled connectivity for monitoring, analytics, support or production integration.

The architecture should therefore use zones and conduits that strictly control communication between:

- enterprise IT;
- industrial DMZs;
- factory operations;
- control systems;
- safety systems;
- and external vendors.

Microsoft's Defender for IoT guidance references layered OT architectures and the Purdue model when planning segmentation and sensor placement.

Defender for IoT

Microsoft Defender for IoT can use OT network sensors to discover devices, maintain asset inventories, assess vulnerabilities and monitor traffic for suspicious or unauthorised behaviour. Sensors can be deployed as physical appliances or virtual machines and can operate as cloud-connected or locally managed systems.

The capability may support:

- passive asset discovery;
- visibility into unmanaged OT devices;
- behavioural anomaly detection;
- unauthorised-protocol detection;
- vulnerability prioritization;
- and integration with centralised security operations.

OT Security Principles

- Do not interrupt production unnecessarily.

- Prefer passive monitoring where active scanning may create risk.
- Separate IT, OT and safety environments.
- Control and record vendor remote access.
- Use jump hosts and privileged access workflows.
- Test changes with factory engineering teams.
- Maintain offline or protected recovery options.
- Align incident response with safety procedures.

5. Data Security

Protect the Information, Not Only the Infrastructure

Nordic Ventures Group processes:

- employee information;
- financial data;
- customer information;
- SAP and ERP records;
- manufacturing data;
- intellectual property;
- and AI training or analytical datasets.

The security architecture should classify information according to sensitivity and business importance.

Data Protection Model

Data class	Example	Typical controls
Public	Published marketing content	Integrity and availability
Internal	Operating procedures	Authenticated access
Confidential	Commercial and ERP data	Encryption and restricted access
Highly confidential	HR, identity and strategic data	Strong access governance and monitoring

Data class	Example	Typical controls
Safety or production critical	Factory control data	Segmentation, integrity and resilient recovery

Core Controls

- Encryption in transit and at rest.
- Key management and rotation.
- Managed identities instead of embedded secrets.
- Data-loss prevention where appropriate.
- Access logging and review.
- Retention and deletion policies.
- Backup protection.
- Data-residency analysis.
- Privacy-by-design practices.

GDPR Article 32 uses a risk-based approach to security of processing; compliance cannot be reduced to selecting a single technical product or policy. Controls must be appropriate to the risk and organizational context.

6. Compliance as Code

Automating Controls Without Oversimplifying Compliance

Azure Policy can help enforce and assess technical requirements such as:

- permitted regions;
- mandatory diagnostic settings;
- encryption settings;
- approved resource types;
- private-network configuration;
- required tags;
- and security-agent deployment.

However, Azure Policy does not by itself guarantee GDPR or NIS2 compliance.

Microsoft notes that policy mappings can assist with assessing controls, but there is often no complete one-

to-one correspondence between a policy definition and a regulatory requirement.

Compliance also depends on:

- governance;
- contracts;
- people;
- documented procedures;
- lawful processing;
- incident management;
- supplier oversight;
- and evidence that controls operate effectively.

Continuous Compliance Model

Policy definition
Automated deployment
Continuous assessment
Evidence collection
Exception management
Remediation
Independent assurance

Business Value

- reduced manual control effort;
- faster identification of drift;
- consistent technical baselines;
- improved audit evidence;
- and faster onboarding of new workloads and countries.

TRUSTED ADVISOR INSIGHT *The fastest incident responses are never improvised. They are rehearsed until the room stops arguing about who is in charge.*

7. Detect

From Fragmented Monitoring to Unified Visibility

Nordic Ventures Group cannot defend fourteen countries through isolated monitoring tools.

A modern detection model centralizes relevant signals from:

- Entra ID;
- endpoints;
- Azure resources;
- Microsoft 365;
- applications;
- networks;
- factory and OT systems;
- cloud platforms;
- and selected third parties.

Microsoft Sentinel is a cloud-native SIEM that combines security analytics, threat intelligence, automation and investigation across multicloud and multiplatform environments.

Detection Architecture

Capability	Purpose
Microsoft Sentinel	SIEM, investigation, hunting and orchestration
Defender XDR capabilities	Correlate endpoint, identity, email and application signals
Defender for Cloud	Cloud posture and workload protection
Defender for IoT	OT and IoT visibility
Entra risk signals	Detect risky users and sign-ins
Azure Monitor and Log Analytics	Platform and operational telemetry

Capability	Purpose
Threat intelligence	Enrich alerts with known indicators

Detection Engineering

The SOC should not depend only on default alerts.

It should continuously develop and test detections based on:

- threat models;
- business-critical scenarios;
- MITRE ATT&CK techniques;
- red-team findings;
- incident lessons;
- and threat intelligence.

Priority scenarios for Nordic Ventures Group may include:

- privileged account compromise;
- ransomware propagation;
- suspicious factory access;
- data exfiltration;
- malicious administrative changes;
- unexpected cross-country access;
- and compromise of a critical supplier.

8. Respond

Contain Quickly and Decide Clearly

Incident response must combine technology, process and executive decision-making.

A response plan should define:

- who declares an incident;
- who may isolate systems;
- who communicates with factories;
- who informs customers and authorities;
- who approves recovery;
- and how evidence is preserved.

Microsoft Sentinel supports SOAR through automation rules and playbooks that can assist with incident assignment, enrichment and automated response actions.

Automation should accelerate known actions, but high-impact decisions still require governance and human judgment.

Incident Response Lifecycle

Triage
Validate
Contain
Eradicate
Recover
Communicate
Learn

Example Ransomware Scenario

If ransomware affects a factory-related environment:

Validate the incident and affected scope.

Isolate compromised identities and network segments.

Protect unaffected factories and enterprise services.

Activate crisis and factory-continuity procedures.

Preserve forensic evidence.

Assess whether backups and recovery environments remain clean.

Restore critical services according to business priority.

Communicate with leadership, employees, partners, and authorities as required.

Complete lessons learned and control improvements.

NIS2 contains cybersecurity risk-management and incident-reporting obligations for entities within its scope, including an early-warning and staged-notification model for significant incidents. Exact national procedures must be confirmed in each applicable jurisdiction.

TRUSTED ADVISOR INSIGHT *A backup is a hope. A tested restoration is a plan. The Trusted Advisor never confuses the two in front of the board.*

9. Recover

Recovery Is a Security Capability

Backup alone is not cyber resilience.

Backups may be:

- deleted;
- encrypted;
- corrupted;
- incomplete;

- inaccessible;
- or compromised through administrative credentials.

A cyber-recovery design should include:

- immutable or protected backups;
- separation of backup administration;
- multifactor authentication;
- restricted deletion;
- offline or isolated copies where justified;
- clean-room restoration;
- documented recovery sequencing;
- malware validation;
- and regular restore testing.

Recovery Priorities

Recovery priority	Examples
Priority 1	Factory production, identity, SAP and ERP
Priority 2	Supply chain, finance and essential collaboration
Priority 3	HR, reporting and internal services
Priority 4	Development, testing and sandbox environments

Recovery Metrics

- Recovery Time Objective.
- Recovery Point Objective.
- Percentage of successful backups.
- Percentage of successful restore tests.
- Time to establish a clean recovery environment.
- Time to validate application integrity.
- Percentage of critical systems covered by recovery plans.

NIS2 explicitly includes business continuity, backup management, disaster recovery and crisis management among its cybersecurity risk-management measures.

10. Supply-Chain Security

Nordic Ventures Group depends on:

- software vendors;
- cloud providers;
- consultants;
- equipment manufacturers;
- managed service providers;
- logistics partners;
- and factory-maintenance suppliers.

A compromise of a trusted supplier can bypass internal controls.

The security program should include:

- supplier risk classification;
- security requirements in contracts;
- access restrictions;
- periodic reviews;
- breach-notification obligations;
- software and dependency governance;
- and controlled offboarding.

NIS2 includes supply-chain security and the security aspects of supplier and service-provider relationships within its minimum risk-management areas.

11. Security Operations Model

Technology Requires Clear Ownership

Capability Primary ownership

Security strategy CISO and executive leadership

Cloud security architecture Security architecture and platform teams

Identity security Identity platform team

Network security Network and security teams

OT security Factory engineering, OT security and SOC

Detection engineering SOC

Incident response CSIRT or incident-response team

Cyber recovery Operations, application owners and security

Compliance evidence Control owners, risk and compliance

Exception approval Architecture and risk governance

Centralised and Federated Operations

A fully centralised SOC may provide consistent visibility, but local teams remain essential for:

- factory context;
- national requirements;
- language;
- business impact;
- and physical response.

A federated model therefore makes more sense:

- central strategy and tooling;
- shared detection and response processes;
- local operational participation;
- and clear escalation paths.

12. Security Metrics That Matter

Security metrics should help leaders make decisions, not merely describe tool activity.

Executive Security Dashboard

KPI Business meaning

Critical exposure reduction Progress in reducing material risk

MFA and PIM coverage Strength of identity protection

Mean time to detect Speed of threat discovery

Mean time to contain Ability to limit business impact

Critical vulnerabilities past SLA Remediation discipline

Recovery-test success Ability to restore operations

Policy compliance Consistency of technical controls

Privileged access reviews completed Governance of administrative power

OT asset visibility Understanding of factory exposure

Security exceptions overdue Accumulated accepted risk

Supplier assessments completed Supply-chain assurance

High-severity incidents Current threat and control effectiveness

Metrics should be interpreted in context. A higher number of detected incidents may reflect better visibility rather than weaker security.

13. Security Architecture Decision Record

ADR-010: Adopt an Integrated Cyber-Resilience Architecture

Context

Nordic Ventures Group must protect a hybrid environment covering legacy IT, Azure, Microsoft 365, enterprise applications, factory OT, and future AI platforms.

Decision

Adopt an integrated cyber-resilience architecture aligned with:

- NIST Cybersecurity Framework 2.0;
- Zero Trust;
- Microsoft Cybersecurity Reference Architecture;
- NIS2 risk-management principles;
- and risk-based privacy controls.

Centralize core governance, identity, detection and response capabilities while maintaining workload and factory-specific controls.

Alternatives Considered

- Continue with separate security tools per country.
- Focus primarily on perimeter protection.
- Outsource all security operations without internal ownership.
- Implement security controls only after migration.
- Treat backup as the complete recovery strategy.

Positive Consequences

- unified risk governance;
- stronger detection;
- reduced fragmentation;
- improved audit evidence;
- faster incident response;
- and greater operational resilience.

Negative Consequences

- increased implementation complexity;
- significant skills requirements;
- telemetry and licensing costs;
- organizational change;
- and the need for continuous tuning.

Mitigation

- phased adoption;
- risk-based prioritization;
- training and operating-model development;
- FinOps for security telemetry;
- automation;
- and regular architecture reviews.

The Nordic Ventures Group Lesson

Cybersecurity is not successful because no attack ever occurs.

It is successful when the organisation can:

- prevent avoidable incidents;
- identify attacks early;
- limit their spread;
- make clear decisions;
- restore critical operations;
- meet its obligations;
- and retain the trust of customers, employees and partners.

The strongest security architecture protects both sides of the transformation:

- the value already created;
- and the future opportunities the platform is designed to unlock.

Key Takeaways

Principle	What It Means
Cybersecurity Is Enterprise Risk Management	Security decisions belong in business and executive conversations.
Govern Before You Deploy	Clear ownership and risk appetite must guide technical controls.
Protect the Whole System	Identity, data, applications, cloud, legacy IT and OT must work as one security architecture.
Segmentation Is Not Automatically Air-Gapping	Factory security requires carefully controlled connectivity and operational context.
Compliance Cannot Be Guaranteed by a Tool	Policy as code supports compliance, but governance, people, and evidence remain essential.
Detection Must Be Engineered	Collecting logs is not the same as detecting material threats.

Principle	What It Means
Response Must Be Practised	Automation helps, but roles, authority and communication determine whether containment succeeds.
Recovery Is Part of Security	A backup has no value until restoration has been tested.
Security Enables Innovation	Teams move faster when safe patterns and trusted controls are built into the platform.

Reflection Questions

Which business service would create the greatest financial or safety impact if it became unavailable?

Does your board have a clearly defined cyber-risk appetite?

Can your organisation identify every privileged identity and critical asset?

Are factory and OT environments segmented according to operational risk?

Which compliance controls are automated, and which still depend on manual evidence?

Can your SOC detect and contain a compromised administrator account?

Are critical backups protected from the same identities that administer production?

When was the last successful end-to-end recovery test?

Could a supplier compromise reach critical systems?

Which security metric would be most meaningful to your CEO?

References

- NIST. Cybersecurity Framework 2.0. The framework organises outcomes across Govern, Identify, Protect, Detect, Respond, and Recover.
- Microsoft. Microsoft Cybersecurity Reference Architecture.
- Microsoft. Microsoft Defender for IoT Architecture and Components.
- Microsoft. Defender for IoT and OT Network Architecture.
- Microsoft. Microsoft Sentinel Overview.
- Microsoft. Automation in Microsoft Sentinel.
- Microsoft. Microsoft Cloud Security Benchmark and MCRA Design Guidance.
- European Union. Directive (EU) 2022/2555 — NIS2.
- European Union. General Data Protection Regulation — Article 32.
- Center for Internet Security. CIS Critical Security Controls v8.