Microsoft Certified

Security, Compliance & Identity Fundamentals

SC-900 · Cybersecurity Act 2024 (Act 854)

Webinar

Brought to you by
Microsoft Organizational Skilling

Discover more learning opportunities here at

https://esi.microsoft.com/

Microsoft

Presenter

Mohammed Arif, PhD

GenAI Architect & Lead Data Scientist

What You Will Learn — Session Agenda

01 **Security & Compliance Concepts**

Shared Responsibility · Zero Trust · CIA Triad · Encryption · GRC

02 **Identity & Access Management**

Microsoft Entra ID · MFA · Conditional Access · PIM · Identity Protection

03 **Microsoft Security Solutions**

Security Copilot · Defender XDR · Microsoft Sentinel · Defender for Cloud · Azure Security

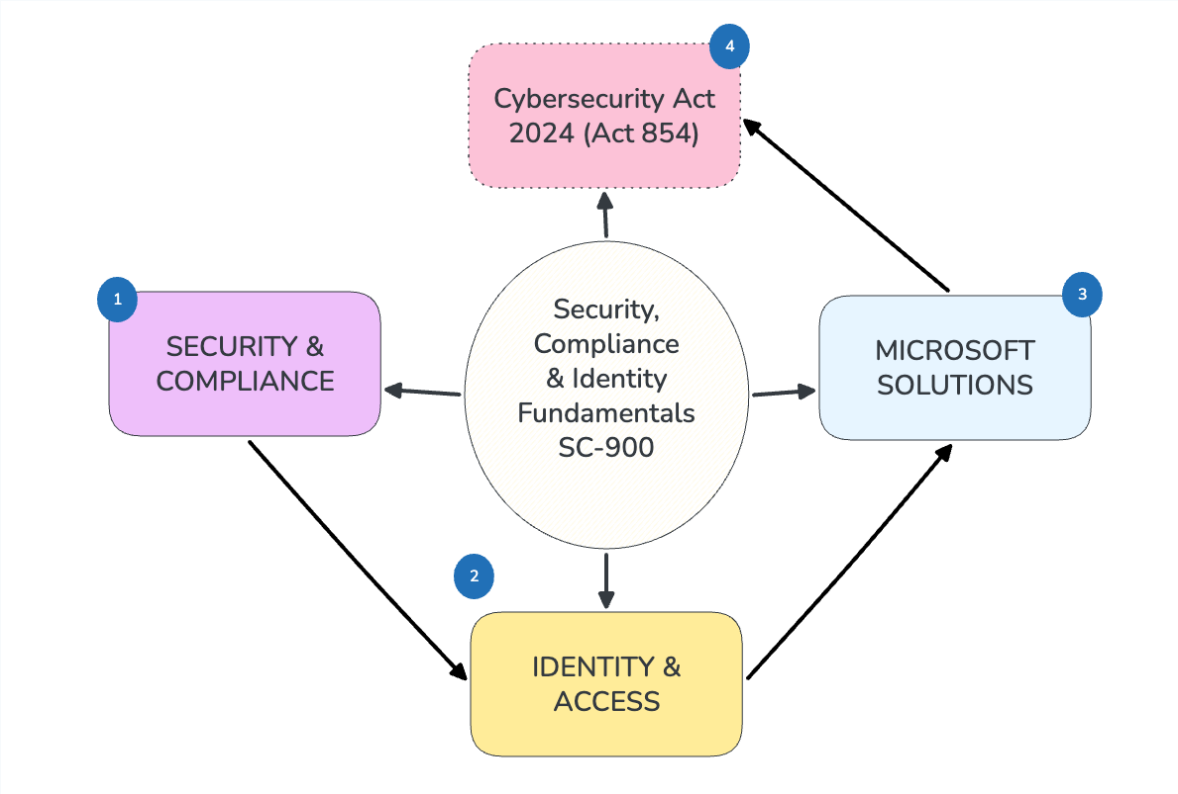
04 **Cybersecurity Act 2024 (Act 854)**

NCII Framework · Obligations · Incident Reporting · Licensing · Penalties

05 **Interactive Quiz**

Test your knowledge across all topics

What You Will Learn — Session Agenda



01

Security & Compliance Concepts

Shared Responsibility · Zero Trust · CIA Triad · Encryption · GRC

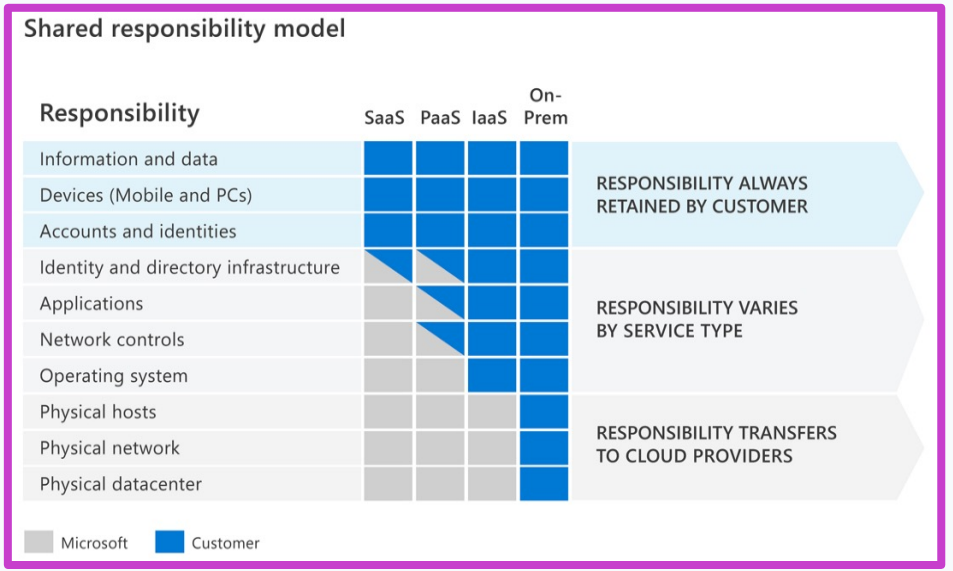
The Shared Responsibility Model

Customer Always Owns

- Information & Data
- Devices — Mobile & PCs
- Accounts & Identities

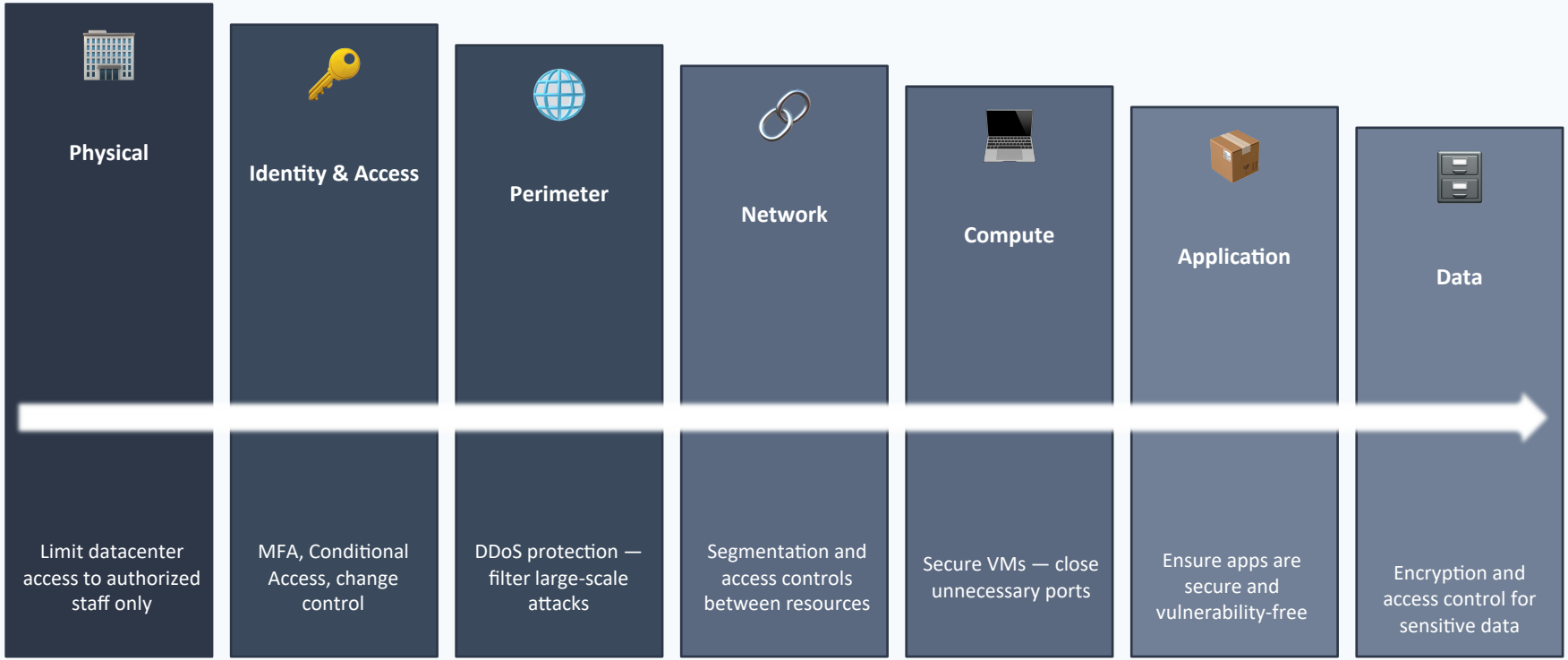
Responsibility Shifts by Model

On-Prem	You own everything
IaaS	You own: OS, apps, data
PaaS	You own: apps & data
SaaS	You own: data & identities



Defense in Depth — Layered Security Strategy

A series of security mechanisms that slow the advance of an attack. Each layer provides protection so that if one is breached, the next prevents unauthorized access.



CIA Triad — The Goals of a Cybersecurity Strategy

C

Confidentiality

- Ensure sensitive data stays private — customer info, passwords, financial records
- Encryption protects data; encryption keys must also stay confidential
- Most visible part of security — everyone understands the need for secrecy

I

Integrity

- Ensure data or messages have not been tampered with or altered
- The email you receive must be identical to the one sent
- Encrypted data must decrypt back to exactly the original — unchanged

A

Availability

- Data must be accessible to authorized users when they need it
- Security cannot sacrifice access — employees need decrypted data to work
- Balance protection with usability — overly restricted data creates bottlenecks

The Zero Trust Model — Trust No One, Verify Everything

01

Verify Explicitly

Always authenticate and authorize based on all available signals — identity, location, device, service, workload, data classification, and anomalies.

02

Least Privileged Access

Limit user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive policies, and data protection.

03

Assume Breach

Minimize blast radius. Segment access. Encrypt end-to-end. Use analytics to get visibility, drive threat detection, and improve defences.

Six Foundational Pillars

Identities

Verify with strong authentication

Devices

Monitor all devices accessing network

Applications

Discover shadow IT, control access

Data

Classify, label, and encrypt

Infrastructure

Real-time threat detection

Networks

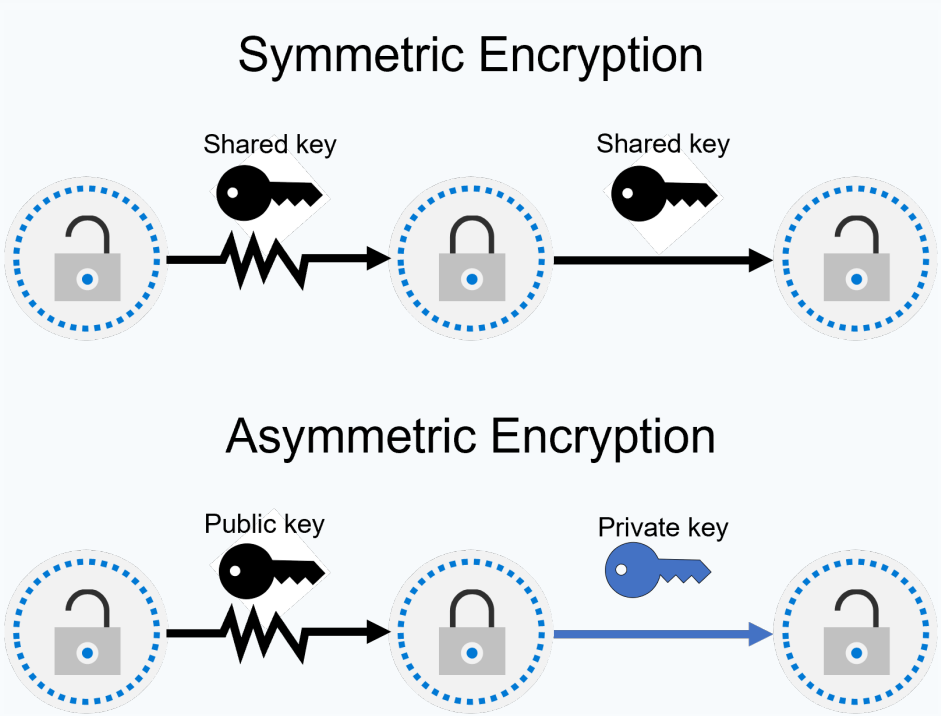
Segment and encrypt all comms

Encryption & Hashing — Protecting Data

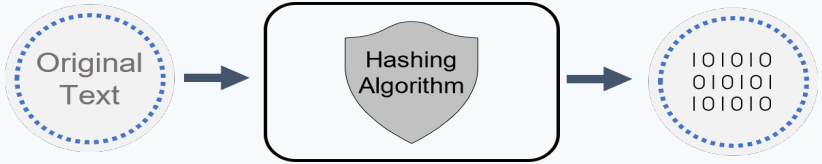
Encryption

Makes data unreadable to unauthorized viewers. Requires a secret key to decrypt.

Symmetric	Same key encrypts & decrypts (e.g. AES)
Asymmetric	Public/private key pair — used in TLS/HTTPS
At Rest	Data stored on disk — protected from physical theft
In Transit	Data moving across networks — protected by HTTPS
In Use	Data in RAM/CPU — protected by secure enclaves



Encryption & Hashing — Protecting Data



Hashing

Converts text into a unique, fixed-length value. Cannot be reversed back to the original.

- Deterministic — same input always produces same output
- Non-reversible — unlike encryption, there is no decryption
- Used to store passwords securely — never stored as plaintext
- Salting: adds a random value to the input before hashing to defend against brute-force dictionary attacks
- Common algorithms: SHA-256, bcrypt

Governance, Risk & Compliance (GRC)

Governance

Rules & Direction

The system of rules, practices, and processes an organization uses to direct and control its activities. Examples: who has admin privileges, when credentials expire, access control policies.

Risk Management

Identify & Respond

The process of identifying, assessing, and responding to threats. External risks: cyberattacks, economic shifts, pandemics. Internal risks: data leaks, fraud, insider threats.

Compliance

Laws & Regulations

Country, state, or multinational laws and regulations the organization must follow. Compliance defines minimum standards — it is not the same as full security. In Malaysia: Act 854, PDPA 2010.

Additional concepts: Data Residency (where data is physically stored) — Data Sovereignty (data is subject to laws of the country where collected) — Data

02

Identity & Access Management

Microsoft Entra ID · MFA · Conditional Access · PIM · Identity Protection

Authentication vs Authorization — Two Distinct Steps

Authentication (AuthN)

"Who are you?"

- Proves a person is who they claim to be
- Grants initial access to the system
- Methods: Password + MFA, Biometrics, FIDO2, Smart Cards, Certificates
- Example: Entering username + password + Authenticator code

Authorization (AuthZ)

"What can you do?"

- Determines what an authenticated user is permitted to access or do
- Enforced through roles and policies after authentication
- Principle: Least Privilege — give minimum access necessary
- Example: A user can read reports but cannot delete records

Microsoft Entra ID — Cloud Identity & Access Management

Microsoft's cloud-based identity and access management service. Formerly Azure Active Directory (Azure AD). Subscribers to Azure, Microsoft 365, or Dynamics 365 automatically have access.

Human Identities

Internal

Employees — authenticate via organization's Entra ID

External

Guests, partners, customers — authenticate via their own IdP

Workload Identities

Service Principal

Identity for an app — developers manage credentials

Managed Identity

Auto-managed by Azure — no credential management needed

Device Identities

Entra Registered

BYOD — personal device, no org account required to sign in

Entra Joined

Org-owned device — signed in with organizational account

Hybrid Joined

Joined to both on-premises AD and Entra ID

Hybrid Identity: Entra ID Connect cloud sync provisions and synchronizes on-premises AD users into Entra ID — giving users one identity for both environments.

Multifactor Authentication (MFA) — Stronger Identity Security

MFA dramatically improves identity security by requiring more than one verification factor during sign-in.

Something You Know

- Password or PIN
- Security questions (SSPR only)

Something You Have

- Microsoft Authenticator App
- OATH Hardware/Software Token
- SMS verification code
- FIDO2 security key

Something You Are

- Windows Hello (biometrics)
- Fingerprint scan
- Face recognition

Security Defaults: Free baseline that enforces MFA registration for all users, forces admin MFA, and requires MFA when needed — recommended for organizations starting their security journey.

Conditional Access — Intelligent Access Policy Engine

Conditional Access policies are if-then statements: If a signal is met, enforce a control. They analyse signals to automate access decisions.

SIGNALS (Assignments)

- User, group, or role
- Cloud application or action
- Sign-in risk & user risk
- Device platform / compliance state
- IP location (trusted or not)
- Client app being used

DECISION

- Policy conditions are evaluated
- If ALL assignments match, policy applies
- Access decision is made based on controls configured

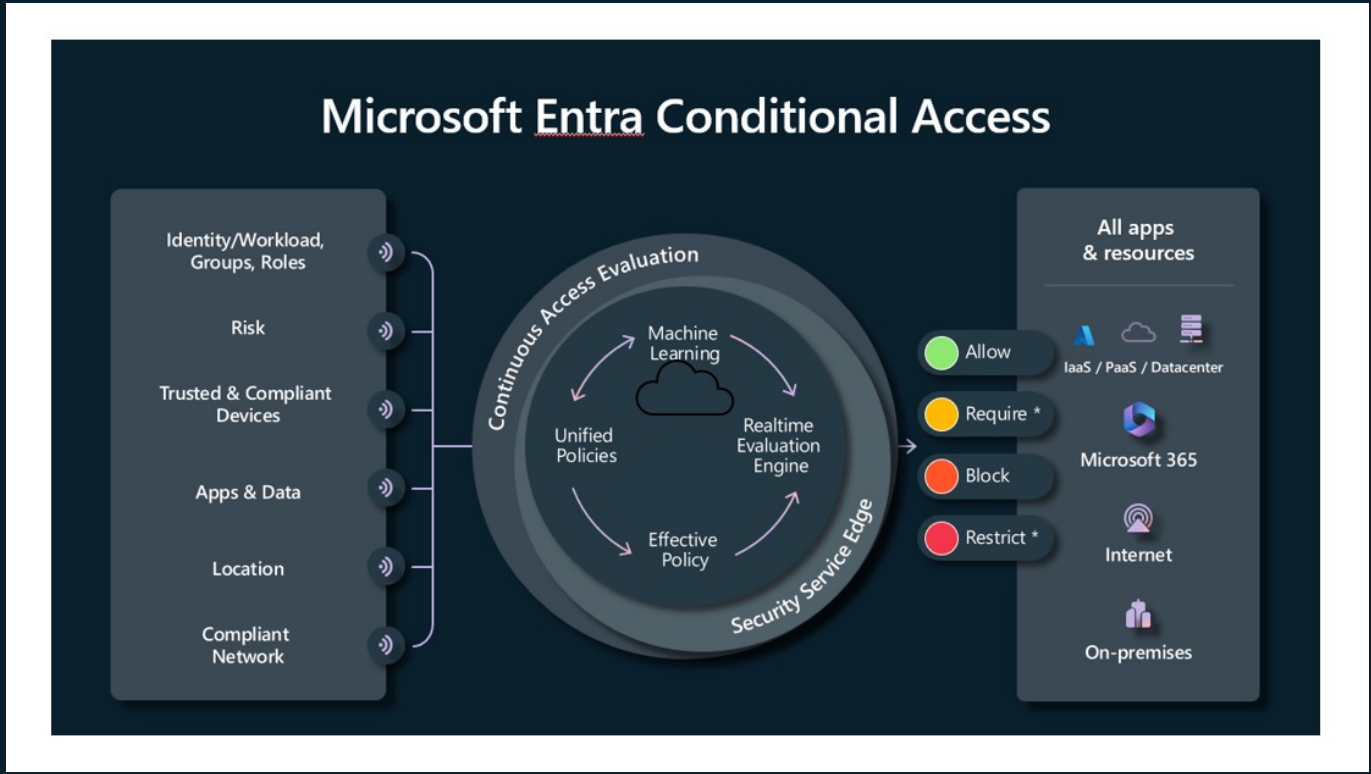
ACCESS CONTROLS

- Block Access — deny entry
- Grant with conditions: require MFA, compliant device, password change
- Session control: limit what users can do (e.g. block downloads)

Global Secure Access extends Conditional Access to network traffic — Microsoft Entra Internet Access (SaaS/Web) and Microsoft Entra Private Access (replacing legacy VPN for internal apps).

Conditional Access — Intelligent Access Policy Engine

Conditional Access policies are if-then statements: If a signal is met, enforce a control. They analyse signals to automate access decisions.



Privileged Identity Management (PIM) & Identity Protection

Privileged Identity Management

Manages, controls, and monitors access to critical resources. Reduces risk of excessive or misused admin privileges.

Just-In-Time

Access granted only when needed, not permanently

Time-Bound

Set start and end dates for elevated access

Approval-Based

Require approval before activating a privileged role

Visible & Auditable

Notifications sent; full access history downloadable

Microsoft Entra Identity Protection

Detects, investigates, and remediates identity-based risks using signals from trillions of daily events.

Sign-in Risk	Anonymous IP address, atypical travel, unfamiliar properties, impossible travel
User Risk	Leaked credentials, suspicious sending patterns, user-reported compromise
Investigate	Risk Detections report · Risky Sign-ins report · Risky Users report (with Security Copilot)
Remediate	Automated: risk-based Conditional Access policies. Manual: admin review via portal or API
Export	Send data to SIEM, Log Analytics, Event Hubs, or Storage for further correlation

03

Microsoft Security Solutions

Security Copilot · Defender XDR · Sentinel · Defender for Cloud · Azure Security

Microsoft Security Copilot — AI-Powered Security Analysis

An AI-powered, cloud-based security analysis tool that enables analysts to respond to threats quickly, process signals at machine speed, and assess risk faster than traditional methods.

Incident Summarization

Distil complex security alerts into concise, actionable summaries to enable quicker response and streamlined decision-making.

Impact Analysis

Assess the potential scope and impact of security incidents — identify affected systems and data to prioritize response.

Script Reverse Engineering

Analyze complex command line scripts and translate them into plain language with clear explanations of the attacker's actions.

Guided Response

Actionable step-by-step guidance for triage, investigation, containment, and remediation — with deep links to recommended actions.

Standalone	Dedicated Copilot portal — natural language prompts, text/image/document responses	**Embedded**	Built directly into Defender XDR, Sentinel, Entra, Defender for Cloud interfaces

Microsoft Defender for Cloud — Cloud Native Application Protection

A cloud-native application protection platform (CNAPP) with security measures designed to protect cloud-based applications from cyberthreats and vulnerabilities.

01

DevSecOps · Security from Code

Unifies security management at the code level across multi-pipeline environments (GitHub, Azure DevOps). Surfaces security posture insights from development through to cloud deployment. Helps teams prioritize critical code fixes with Pull Request annotations.

02

CSPM · Cloud Security Posture Management

Secure Score: aggregates findings into a single number — higher score = lower risk. Continually assesses resources against the Microsoft Cloud Security Benchmark (MCSB). Provides hardening recommendations. Integrates Security Copilot for recommendation context.

03

CWPP · Cloud Workload Protection Platform

Defender plans for specific workload types: Servers, App Service, Storage, SQL, Kubernetes, Container Registries, Key Vault, DNS, Resource Manager. Enhanced features: endpoint detection & response, vulnerability scanning, multi-cloud & hybrid security, JIT VM access.

Microsoft Sentinel — Cloud-Native SIEM & SOAR

SIEM — Collects data across the entire digital estate, identifies correlations and anomalies, generates alerts and incidents.

SOAR — Takes alerts from many sources, triggers automated workflows and processes to run security tasks that mitigate the issue.

COLLECT

Ingest data at cloud scale from all users, devices, applications, and infrastructure — on-premises and multi-cloud. Out-of-the-box data connectors + custom connectors + ASIM data normalization.

DETECT

Detect previously uncovered threats using analytics, MITRE ATT&CK mapping, threat intelligence integration, and watchlists. Minimize false positives with AI.

INVESTIGATE

Investigate threats with AI. Use Incidents (aggregated alerts), Hunting queries, and Jupyter Notebooks in Azure ML. Understand full attack scope and root cause.

RESPOND

Respond rapidly with Automation Rules and Playbooks (Azure Logic Apps). Automate common tasks — open tickets, block users, isolate endpoints, notify teams.

Microsoft Sentinel is now accessible through the Microsoft Defender portal — part of Microsoft's Unified Security Operations Platform (combining SIEM + XDR + posture management + threat intelligence).

Microsoft Defender XDR — Extended Detection & Response Suite

An enterprise defense suite that natively coordinates detection, prevention, investigation, and response across your environment to provide integrated protection against sophisticated attacks.

Defender for Endpoint

Unified endpoint platform — preventive protection, post-breach detection, automated investigation & response for devices.

Defender for Office 365

Protects against threats in email, links (URLs), and collaboration tools (Teams, SharePoint, OneDrive). Anti-phishing, Safe Attachments, ZAP.

Defender for Identity

Uses on-premises AD signals to detect privilege escalation, lateral movement, and compromised identities.

Defender for Cloud Apps

Full SaaS protection — discover shadow IT, SSPM, app-to-app protection, data protection, advanced threat detection.

Vulnerability Management

Continuous asset visibility, risk-based intelligent prioritization, and built-in remediation workflows.

Core Azure Security Infrastructure Services

Azure DDoS Protection

- Protects at Layer 3 & 4 against Volumetric, Protocol, and Application layer DDoS attacks
- Always-on traffic monitoring with automatic mitigation
- Adaptive real-time tuning based on your traffic profile
- Telemetry, monitoring, and alerting via Azure Monitor
- Two tiers: DDoS Network Protection and DDoS IP Protection

Azure Firewall & Web Application Firewall (WAF)

- Azure Firewall: managed, stateful cloud firewall protecting VNet resources. Integrates with Microsoft Threat Intelligence feed
- Supports allow/deny rules based on IP, ports, protocols, and FQDNs (application layer)
- WAF: centralized protection against SQL injection, XSS, and other web exploits. Protects against application-layer DDoS

Azure VNet, NSGs & Network Segmentation

- VNet: fundamental building block for private networks in Azure — no traffic allowed across VNets by default
- Network Security Groups (NSGs): filter inbound/outbound traffic using priority-ordered rules (source, destination, port, protocol)
- Segmentation supports Zero Trust — contain breach impact within a segment

Azure Bastion & Azure Key Vault

- Bastion: secure RDP/SSH directly in Azure portal — no public IP required on VM, protected from port scanning & zero-day exploits
- Key Vault: securely store API keys, passwords, certificates, and cryptographic keys
- Key Vault tiers: Standard (software-protected) & Premium (HSM-protected keys)

04

Cybersecurity Act 2024 (Act 854)

Malaysia's National Cybersecurity Law — NCII Framework, Obligations & Penalties

Cybersecurity Act 2024 (Act 854) — Overview

Purpose	Enacted specifically to enhance national cybersecurity and protect the National Critical Information Infrastructure (NCII) from cyber threats and incidents.
Parliament Passed	April 2024
Royal Assent	June 2024
In Force	26 August 2024
Governing Body	National Cyber Security Agency (NACSA) — the primary regulator and enforcer
Scope	Applies to all entities designated as NCII entities across 11 critical sectors, and to cybersecurity service providers

Act 854 is not a guideline — it is law. Non-compliance carries serious criminal and financial penalties.

Cybersecurity Governance Structure — Three Tiers

01

National Level — National Cybersecurity Committee

Chaired by the Prime Minister

The highest-level body responsible for formulating national cybersecurity policy, approaches, and strategies. Sets the direction for the entire national cybersecurity framework and coordinates cross-government cybersecurity initiatives.

02

Regulatory Level — NACSA (National Cyber Security Agency)

Chief Executive with broad enforcement powers

NACSA's Chief Executive is empowered to: issue directives, gather information from NCII entities, manage the National Cyber Coordination and Control Centre (NC4), and take enforcement action against non-compliant entities.

03

Sector Level — NCII Sector Chiefs

11 Critical Sectors

Each sector has a designated Sector Chief responsible for identifying and designating NCII entities within their sector. The 11 sectors are: Government · Banking & Finance · Transport · Defence · Information & Communications · Health · Water & Waste · Energy · Agriculture · Trade · Science & Innovation

Key Obligations of NCII Entities — Three Mandatory Mandates

If your organization is designated as an NCII Entity under Act 854, the following are legally binding obligations:

01

Implement the Code of Practice

Ongoing

NCII entities must implement cybersecurity measures, standards, and processes in accordance with the Code of Practice endorsed by NACSA's Chief Executive. Example: the JDN Code of Practice for the Government Sector. This covers security controls, incident response procedures, and access management.

02

Annual Cybersecurity Risk Assessment

Annual · 30-day submission

Entities must conduct a formal Cybersecurity Risk Assessment at least once per year — or whenever material changes occur to their systems. The completed report must be submitted to NACSA within 30 days of completion.

03

Biennial Cybersecurity Audit

Every 2 Years · Registered Auditor

Entities must undergo a cybersecurity audit at least once every two years. The audit must be conducted by an independent auditor who has been approved and registered with NACSA's Chief Executive. Self-audits do not qualify.

Cyber Incident Management & Reporting — Act 854 Timeline

When an NCII entity becomes aware of a cyber incident (e.g. data breach, ransomware, system intrusion), the Authorized Person must follow this mandatory reporting timeline:

Immediately

Upon Awareness

The Authorized Person must notify NACSA immediately upon becoming aware of a cyber incident affecting NCII assets. Notification is made electronically via the NC4 portal.

Within 6 Hours

6-Hour Rule

A formal report containing brief details of the incident must be submitted through the NC4 portal within six (6) hours of first becoming aware of the incident. This is mandatory — no exceptions.

Within 14 Days

Follow-up Report

Additional information and investigation findings must be submitted to NACSA within 14 days of the initial notification. This includes full incident analysis, root cause, and remediation steps taken.

NC4 = National Cyber Coordination and Control Centre — the official NACSA reporting portal for all cybersecurity incidents.

Cybersecurity Service Licensing & Penalties — Act 854

📜 Cybersecurity Service Provider Licensing

Providers of certain cybersecurity services must obtain a licence from NACSA before offering or advertising those services. Unlicensed providers face criminal liability.

Services requiring a licence:

- **Managed SOC Monitoring**
- **Penetration Testing**

⚖️ Penalties for Non-Compliance

❌ **Failure to Implement Code of Practice**	**Fine up to RM 500,000 or Imprisonment up to 10 years or Both**
❌ **Failure to Report a Cyber Incident within the Required Timeframe**	**Fine up to RM 500,000 or Imprisonment up to 10 years or Both**
🔍 **NACSA Enforcement Powers (with or without warrant in urgent cases)**	Search premises · Seize electronic devices · Access computer data · Demand passwords

Thank You

SC-900 Exam & Study Resources

learn.microsoft.com/certifications/security-compliance-and-identity-fundamentals

Act 854 — NACSA Official Portal

www.nacsa.gov.my

Microsoft Security Documentation

learn.microsoft.com/security