Incident Report – Brute Force Detection

Objective

To investigate suspicious login activity, identify brute force attacks, and demonstrate how SIEM capabilities support both incident response and compliance requirements.

Investigation Steps

Log Source Integration	Collected authentication logs from Microsoft 365 / Active Directory. Ingested into Microsoft Sentinel.

Detection Query (KQL)	`SecurityEvent WHERE EventID == 4625`
	`| summarize FailedLogins = count() by Account, IPAddress, bin(TimeGenerated, 5m)`
	`| WHERE FailedLogins > 10`

Incident Response Actions	Blocked suspicious IPs. Forced password resets and enforced MFA. Documented the incident in ticketing system.

Compliance Mapping

Framework	Control Reference	Relevance
SOC 2	CC6.1	Logical access monitoring (failed login attempts).
SOC 2	CC7.2	Incident response actions (blocking IPs, MFA reset).
ISO 27001	A.9.4.2	Secure log-on procedures.
ISO 27001	A.12.4.1	Event logging and monitoring.

Next Steps

- Automate detection using Sentinel Analytics Rules.
- Link alerts to Incident Response Playbook (see Project 2).
- Expand detection to include VPN and endpoint log sources.
- Maintain evidence for SOC 2 / ISO 27001 audits.