SOC POLICY DOCUMENT

Policy ID: SOC-NET-001
Policy Name: Port Scanning Detection and Response
Category: Network Security

Description

This policy defines detection and response procedures for unauthorized port scanning activity against internal and external-facing network assets.

MITRE ATT&CK; Mapping

Tactic: Discovery
Technique: T1046 – Network Service Scanning

Detection Criteria

- Scan Types: SYN Scan, FIN Scan, Full TCP Connect Scan
- Time Window: 3 minutes
- Slow Scan Threshold: Activity observed across 3 or more windows
- Sensitive Ports: 22, 3306, 6379, 3389, 5432

Severity Levels and Response Actions

Low Severity

- Log the activity for auditing
- No immediate action required

Medium Severity

- Monitor the source IP
- Increase logging on target systems

High Severity

- Block the source IP at the firewall
- Notify SOC analysts
- Capture packet-level evidence

Critical Severity

- Immediately block the source IP
- Isolate affected systems if required
- Create an incident ticket

- Escalate to Incident Response Team

Recommended Mitigations

- Apply network segmentation to limit attack surface
- Restrict exposure of sensitive services
- Implement rate limiting on firewalls
- Deploy IDS/IPS signatures for port scanning detection

Compliance References

- ISO/IEC 27001 – A.12.6.1
- NIST SP 800-53 – SI-4
- PCI-DSS – Requirement 11