Vulnerability Management

Governance Meeting –22/03/2025

Bruno Suric

Agenda

- Overview of last scan results
- Remediation requirements
- Key remediation actions
- Next Meeting

Scan results & remediation requirements

Overview of Scan Results

Severity	Finding Summary	Source Systems	Remediation Team
Critical	OpenSSL	Greenbone Security Assistant	IT Service Teams
High	Wireshark, Oracle JRE, Microsoft IE	Greenbone Security Assistant	IT Service Teams
Medium	CVE related configuration issues	Greenbone Security Assistant	IT Service Team
Low	Minor CVE's relating vulnerabilities	Greenbone Security Assistant	IT Service Team

Remediation Requirements

Remediation Requirements

Severity	Requirement
Critical	Remediation within 5 working days
High	Remediation within 20 working days
Medium	Remediation within 60 working days
Low	Remediation within 120 working days

References to Standards

- ✓ **ISO/IEC 27001:2013** - Information Security Management Systems (ISMS)
- ✓ **NIST SP 800-53** - Security and Privacy Controls for Information Systems and Organizations
- ✓ **OWASP Top Ten** - Security Risks
- ✓ **CVE and CVSS Standards**
- ✓ **ITIL (Information Technology Infrastructure Library) Framework**
- ✓ **ISO/IEC 27002:2022** - Information Security Controls

Key remediation actions & next meeting

Remediation Action:

Identify Critical Vulnerabilities	Security Operations Management Team
Classify and Prioritize Vulnerabilities	Security Operations Management Team
Communicate Findings	Workplace Management
Remediate Critical and High Vulnerabilities	IT Service Teams
Monitor and Verify	Security Operations Management Team

Next Meeting:
22/09/2025

Agenda:
<AGENDA TO GO HERE>