Industrial Security Assessment Report

System Information

Facility: ACME Manufacturing Plant
Operator: Industrial Security Operator
System ID: 103b59cb
Generated: 2025-07-23 12:36:35

Asset Summary

ID	Type	IP	Protocol	Criticality
ASSET-001	Protection Relay	192.168.21.227	BACnet	Medium
ASSET-003	Router	192.168.213.243	PROFINET	Medium
ASSET-004	Safety Instrumented System	192.168.110.194	DNP3	Medium
ASSET-008	Switch	192.168.220.11	MELSEC (Mitsubishi)	Medium
ASSET-016	DCS Controller	192.168.134.14	DNP3	Medium
ASSET-023	Engineering Workstation	192.168.216.241	Common Industrial Protocol	Medium
ASSET-005	VFD	192.168.111.144	S7Comm (Siemens)	Low
ASSET-007	HMI	192.168.188.226	BACnet	Low
ASSET-009	RTU	192.168.197.79	MELSEC (Mitsubishi)	Low
ASSET-010	Safety Instrumented System	192.168.24.171	Modbus/TCP	Low
ASSET-011	Engineering Workstation	192.168.203.61	IEC 60870-5-104	Low
ASSET-014	Switch	192.168.18.35	EtherNet/IP	Low
ASSET-015	IED	192.168.202.146	FINS (Omron)	Low
ASSET-020	Firewall	192.168.10.245	IEC 60870-5-104	Low
ASSET-021	Firewall	192.168.158.141	Modbus/TCP	Low
ASSET-022	IED	192.168.117.198	PROFINET	Low
ASSET-002	Historian	192.168.130.150	BACnet	High
ASSET-013	RTU	192.168.58.201	PROFINET	High
ASSET-018	PLC	192.168.195.235	Common Industrial Protocol	High
ASSET-019	Engineering Workstation	192.168.43.247	PROFINET	High
RTU-01	RTU	192.168.2.50	DNP3	High
HMI-01	HMI	192.168.1.20	EtherNet/IP	High
ASSET-006	Safety Instrumented System	192.168.234.217	DNP3	Critical
ASSET-012	Historian	192.168.243.172	FINS (Omron)	Critical
ASSET-017	Protection Relay	192.168.23.42	MELSEC (Mitsubishi)	Critical
ASSET-024	SCADA Server	192.168.136.101	S7Comm (Siemens)	Critical
PLC-001	PLC	192.168.1.10	Modbus/TCP	Critical
SCADA-01	SCADA Server	192.168.1.100	OPC UA	Critical

Vulnerability Summary

Asset	CVE ID	Severity	CVSS	Status
ASSET-007	CVE-2023-2345	High	6.3	Unpatched
ASSET-021	CVE-2022-31814	High	8.2	Unpatched
PLC-001	CVE-2022-31814	High	7.9	Unpatched
RTU-01	CVE-2021-7890	Critical	4.2	Unpatched

Alert Summary

Security Recommendations

1. Implement network segmentation for critical assets
2. Enable protocol-specific security features
3. Patch systems with known vulnerabilities
4. Review and update firewall rules
5. Conduct regular security awareness training