Industrial Security Assessment Report

System Information

Facility: ACME Manufacturing Plant
Operator: Industrial Security Operator
System ID: c27aaf0b
Generated: 2025-07-23 13:38:03

Asset Summary

ID	Type	IP	Protocol	Criticality
ASSET-004	Historian	192.168.164.77	S7Comm (Siemens)	Low
ASSET-007	Switch	192.168.102.55	BACnet	Low
ASSET-011	Switch	192.168.114.127	S7Comm (Siemens)	Low
ASSET-013	Switch	192.168.192.201	BACnet	Low
ASSET-015	Historian	192.168.61.16	PROFINET	Low
ASSET-021	RTU	192.168.217.86	S7Comm (Siemens)	Low
ASSET-005	PLC	192.168.204.96	S7Comm (Siemens)	High
ASSET-006	VFD	192.168.214.110	MELSEC (Mitsubishi)	High
ASSET-010	IED	192.168.112.131	Modbus/TCP	High
ASSET-012	DCS Controller	192.168.98.189	IEC 61850	High
ASSET-014	HMI	192.168.220.245	IEC 60870-5-104	High
ASSET-017	Safety Instrumented System	192.168.10.230	Modbus/TCP	High
ASSET-018	Switch	192.168.78.157	Modbus/TCP	High
ASSET-019	SCADA Server	192.168.239.49	FINS (Omron)	High
ASSET-020	Protection Relay	192.168.101.250	EtherNet/IP	High
RTU-01	RTU	192.168.2.50	DNP3	High
HMI-01	HMI	192.168.1.20	EtherNet/IP	High
ASSET-001	RTU	192.168.3.35	EtherNet/IP	Critical
ASSET-002	PLC	192.168.89.30	S7Comm (Siemens)	Critical
ASSET-003	IED	192.168.153.116	S7Comm (Siemens)	Critical
ASSET-008	VFD	192.168.161.199	Common Industrial Protocol	Critical
ASSET-009	RTU	192.168.93.146	IEC 61850	Critical
ASSET-016	VFD	192.168.103.3	Modbus/TCP	Critical
ASSET-022	Engineering Workstation	192.168.8.133	OPC UA	Critical
ASSET-023	Firewall	192.168.27.91	Common Industrial Protocol	Critical
ASSET-024	SCADA Server	192.168.30.175	IEC 61850	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-017	CVE-2021-44228	Critical	8.1	Unpatched
ASSET-018	CVE-2022-31814	High	8.3	Unpatched
PLC-001	CVE-2021-44228	Critical	5.7	Unpatched
HMI-01	CVE-2022-6789	Medium	9.3	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