Industrial Security Assessment Report

System Information

Facility: ACME Manufacturing Plant
Operator: Industrial Security Operator
System ID: 5af7e93d
Generated: 2025-07-23 14:18:03

Asset Summary

ID	Type	IP	Protocol	Criticality
ASSET-004	IED	192.168.60.194	S7Comm (Siemens)	Medium
ASSET-008	Engineering Workstation	192.168.177.131	MELSEC (Mitsubishi)	Medium
ASSET-013	Engineering Workstation	192.168.211.59	IEC 61850	Medium
ASSET-014	Router	192.168.94.203	OPC UA	Medium
ASSET-017	Router	192.168.216.77	IEC 61850	Medium
ASSET-002	IED	192.168.63.243	EtherNet/IP	Low
ASSET-005	Engineering Workstation	192.168.38.141	S7Comm (Siemens)	Low
ASSET-011	RTU	192.168.21.52	BACnet	Low
ASSET-016	IED	192.168.36.110	MELSEC (Mitsubishi)	Low
ASSET-018	Engineering Workstation	192.168.103.119	OPC UA	Low
ASSET-019	Safety Instrumented System	192.168.93.105	IEC 60870-5-104	Low
ASSET-020	IED	192.168.204.127	BACnet	Low
ASSET-021	Engineering Workstation	192.168.148.196	OPC UA	Low
ASSET-003	Protection Relay	192.168.24.130	OPC UA	High
ASSET-006	SCADA Server	192.168.167.192	PROFINET	High
ASSET-007	HMI	192.168.214.48	S7Comm (Siemens)	High
ASSET-009	Switch	192.168.229.181	FINS (Omron)	High
ASSET-012	Protection Relay	192.168.154.199	MELSEC (Mitsubishi)	High
RTU-01	RTU	192.168.2.50	DNP3	High
HMI-01	HMI	192.168.1.20	EtherNet/IP	High
ASSET-001	Protection Relay	192.168.106.184	BACnet	Critical
ASSET-010	SCADA Server	192.168.131.151	FINS (Omron)	Critical
ASSET-015	Switch	192.168.14.99	Common Industrial Protocol	Critical
ASSET-022	Safety Instrumented System	192.168.150.117	DNP3	Critical
ASSET-023	Switch	192.168.40.98	OPC UA	Critical
ASSET-024	IED	192.168.80.122	Modbus/TCP	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-024	CVE-2022-31814	High	5.0	Unpatched
ASSET-024	CVE-2021-44228	Critical	4.3	Unpatched
PLC-001	CVE-2021-44228	Critical	7.8	Unpatched
SCADA-01	CVE-2023-1234	High	9.8	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