Industrial Security Assessment Report

System Information

Facility: ACME Manufacturing Plant
Operator: Industrial Security Operator
System ID: b011c809
Generated: 2025-07-23 13:05:52

Asset Summary

ID	Type	IP	Protocol	Criticality
ASSET-002	HMI	192.168.120.43	FINS (Omron)	Medium
ASSET-003	RTU	192.168.15.28	S7Comm (Siemens)	Medium
ASSET-004	RTU	192.168.171.173	FINS (Omron)	Medium
ASSET-005	Router	192.168.104.10	EtherNet/IP	Medium
ASSET-013	HMI	192.168.123.240	IEC 61850	Medium
ASSET-007	RTU	192.168.117.194	BACnet	Low
ASSET-009	Firewall	192.168.174.74	OPC UA	Low
ASSET-015	RTU	192.168.28.57	EtherNet/IP	Low
ASSET-001	Firewall	192.168.44.140	IEC 61850	High
ASSET-006	Safety Instrumented System	192.168.163.212	OPC UA	High
ASSET-010	IED	192.168.177.170	DNP3	High
ASSET-011	Historian	192.168.191.141	IEC 61850	High
ASSET-014	SCADA Server	192.168.212.37	EtherNet/IP	High
ASSET-017	HMI	192.168.138.47	BACnet	High
ASSET-018	IED	192.168.41.232	IEC 61850	High
ASSET-019	Engineering Workstation	192.168.110.216	S7Comm (Siemens)	High
ASSET-020	IED	192.168.89.76	EtherNet/IP	High
ASSET-021	SCADA Server	192.168.136.175	DNP3	High
ASSET-023	Safety Instrumented System	192.168.77.245	S7Comm (Siemens)	High
RTU-01	RTU	192.168.2.50	DNP3	High
HMI-01	HMI	192.168.1.20	EtherNet/IP	High
ASSET-008	SCADA Server	192.168.114.12	OPC UA	Critical
ASSET-012	Safety Instrumented System	192.168.1.176	S7Comm (Siemens)	Critical
ASSET-016	SCADA Server	192.168.87.254	MELSEC (Mitsubishi)	Critical
ASSET-022	SCADA Server	192.168.29.192	Modbus/TCP	Critical
ASSET-024	VFD	192.168.94.183	Common Industrial Protocol	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-2023-2345	High	6.8	Unpatched
PLC-001	CVE-2021-44228	Critical	6.4	Unpatched
SCADA-01	CVE-2023-1234	High	7.6	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