CompTIA SecOT+ Certification Exam Objectives

EXAM NUMBER: SOT-001 V1

CompTIA SecOT+ SOT-001 V1 Certification Exam
Exam Objectives Document Version 1.2

CompTIA

About the Exam

The CompTIA SecOT+ SOT-001 V1 certification exam will certify that the successful candidate has the knowledge and skills required to:

- Understand the physical impact of operational technology (OT) cybersecurity threats.
- Assess the security posture of OT environments as a part of a risk management program.
- Differentiate the design, operational, and security aspects of OT and IT environments in support of safety or business operations.
- Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance, in the OT environment.
- Identify, analyze, and respond to OT security events and incidents.
- Define and apply OT incident management principles.

The target audience consists of control engineers and OT cybersecurity engineers with at least three years of hands-on experience working in OT environments and two years of hands-on experience implementing cybersecurity technologies and solutions in an OT environment.

These content examples are meant to clarify the exam objectives and should not be construed as a comprehensive listing of all the content of this examination.

EXAM ACCREDITATION

TBD

EXAM DEVELOPMENT

CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an IT professional.

CompTIA AUTHORIZED MATERIALS USE POLICY

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse, or condone utilizing any content provided by unauthorized third-party training sites (aka "brain dumps"). Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA's exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the CompTIA Certification Exam Policies. Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the CompTIA Candidate Agreement. If a candidate has a question as to whether study materials are considered unauthorized (aka "brain dumps"), they should contact CompTIA at examsecurity@comptia.org to confirm.

PLEASE NOTE

The lists of examples provided in bulleted format are not exhaustive lists. Other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam, although not listed or covered in this objectives document. CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current, and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.

TEST DETAILS

Required exam	SecOT+ SOT-001 V1
Number of questions	TBD
Types of questions	Multiple-choice and performance-based
Length of test	TBD
Recommended experience	At least three years of hands-on experience working in OT environments and two years of hands-on experience implementing cybersecurity technologies and solutions in an OT environment
Passing score	TBD

EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination and the extent to which they are represented.

DOMAIN		PERCENTAGE OF EXAMINATION
1.0	OT Systems and Safety Foundations	14%
2.0	OT Risk Management	17%
3.0	OT Threat Intelligence	14%
4.0	OT Cybersecurity Architecture, Design, and Engineering	18%
5.0	OT Security Operations	22%
6.0	OT Incident Management	15%
Total		**100%**

1.0 OT Systems and Safety Foundations

1.1 Given a scenario, apply safety techniques to the job environment.

- Safety considerations
  - Environment
  - Loss of life
  - Property
  - Injury
- Industrial ratings
- Hazards
  - Electrical
  - Pressure
  - Heights
  - Temperature
  - Fire
  - Chemical
  - Water
- Lockout/tagout procedures
- Job safety analysis (JSA)
- Personal protective equipment (PPE)
- Safety meeting
  - Briefing
  - Outbrief

1.2 Explain the unique elements in OT environments.

- Convergence of IT and OT
- Role of IT vs. role of OT
- Device types and roles
  - Sensors
  - Actuators
  - Controllers
  - Programmable logic controllers (PLCs)
  - Human-machine interfaces (HMIs)
  - Variable frequency drives (VFDs)
  - Relays
  - Intelligent electronic devices (IEDs)
  - Remote terminal units (RTUs)
  - Engineering workstations
  - Operator workstations
  - Historians
  - Transient/portable devices
- Industrial control system
  - Distributed control system (DCS)
  - Localized control network
  - Safety instrumented system (SIS)
  - Supervisory control and data acquisition (SCADA)
  - Manufacturing execution system (MES)
- Stand-alone systems and networks
- Critical infrastructure sectors

1.3 Explain control theory concepts.

- Control logic
  - Ladder logic
  - Functional block diagram
  - Structured text list
  - Sequential function blocks
- Process variable
- Set points
- Inputs and outputs (I/Os)
- Watchdogs
- Timers
- Current value
- Tags

1.4 Explain OT communication mediums and protocols.

- Serial (RS-232, RS-485)
  - Modbus RTU
  - Profibus
  - Data Highway Plus
  - Distributed Network Protocol 3 (DNP3)
- Ethernet
  - Ethernet for Control Automation Technology (EtherCAT)
  - Modbus Transmission Control Protocol (TCP)
  - Common Industrial Protocol (CIP)/EtherNet/Industrial Protocol (EtherNet/IP)
  - Open Platform Communications (OPC) Data Access (DA)
  - OPC Unified Architecture (UA)
  - Building Automation and Control Networks (BACnet)/KNX
  - Profinet
- Wireless
  - Very high frequency (VHF)
  - Automated information system (AIS)
  - Very small aperture terminal (VSAT)
  - M-Bus
  - 802.15.4
  - 802.11

1.5 Compare and contrast infrastructure considerations for OT.

- Legacy/unsupported
  - Operating systems (OSs)
    - Embedded
    - Custom/proprietary
    - Real-time operating system (RTOS)
    - Commodity/general purpose
  - Hardware
  - Protocols
  - Physical ports
  - Applications
- Modern
  - Virtualization
    - Virtual machines
    - Hypervisor
    - Switching
    - Virtual PLCs
    - Containers
  - Software-defined network (SDN)
  - Middleware
  - Artificial intelligence (AI) capabilities
    - Machine learning (ML)
    - Generative AI
  - Cloud infrastructure
    - Public
    - Private
    - Hybrid
    - Edge devices
    - Vendor-provided services
  - Privatized backbone infrastructure
  - Autonomous systems

2.0 OT Risk Management

2.1 Explain the importance of governance, risk, and compliance.

- Operational/business objectives
  - Risk appetite
  - Balancing security vs. operations
  - Governance structures
  - Business continuity
  - Disaster recovery
- Drivers
  - National security
  - Regulatory compliance
  - Non-compliance
  - Business impact
    - Financial
    - Reputational
    - Quality
    - Operational
  - Business safety
    - Loss of life
    - Environmental
  - Reliability
  - Legal requirements

2.2 Explain the elements of cybersecurity program management.

- Risk levels
- Risk registry
- Maturity assessments
- Benchmarks
- Road map development
- Responsible, Accountable, Consulted, Informed (RACI) model
- Stakeholder management
- Elements of master service agreements (MSAs)
  - Procurement requirements
  - Service-level agreements (SLAs)
    - Internal
    - External
  - Memorandum of understanding (MOU)
  - Statement of work (SOW)
- Metrics and measures
- Training and awareness
- Understanding criticality
- Cybersecurity documentation
  - Policies
  - Processes
  - Standards
  - Standard operating procedures

2.3 Explain risk assessment concepts.

- Frameworks and methodologies
  - National Institute of Standards and Technology (NIST)
  - International Society of Automation (ISA)/International Electrotechnical Commission (IEC)
  - North American Electric Reliability Corporation (NERC)
  - Network Segment 2 (NS2)
  - Cybersecurity Risk Assessment (CRA)
- Risk variables
  - Likelihood
  - Impact/consequence
- Scoping
  - Assets
  - Network
- Threat surface identification
  - Attack vector
  - Exposure
  - Threat actor
- Risk assessment methods
  - Scenario-based
  - Supply chain
    - Hardware and software
  - Third-party risk
  - Failure mode and criticality
  - Qualitative vs. quantitative
  - Architecture review
  - Penetration test
  - Adversarial emulation
- Controlling risks
  - Risk register
  - Risk treatment
  - Controls catalogs
  - Control acceptance criteria
  - Control documentation
  - Inherited risk
  - Control maturity indicators
  - Controls calendar

2.4 Explain risk monitoring and disposition.

- Residual risk
- Auditing
  - Internal
  - External
- Reporting
- Escalations
- Disposition
  - Accept
  - Transfer
  - Avoid
  - Mitigate

2.5 Explain the importance of the change management process.

- Change identification
- Change determination
  - Applicability
  - Availability
- Change testing
  - Rollback
- Communication
  - Stakeholders
  - Department heads
  - System owners
  - Process owners
  - Asset owners
- Change approval

3.0 OT Threat Intelligence

3.1 Summarize the foundations of threat intelligence.

- Intelligence types
  - Human
  - Signals
  - Measurement and signature
  - Open-source intelligence (OSINT)
  - Imagery
- Threat intelligence frameworks
  - Diamond Model of Intrusion Analysis
  - Intelligence life cycle
  - MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Matrix for industrial control systems
  - Industrial control systems Cyber Kill Chain

3.2 Explain the relevance of historical cyber events impacting OT environments.

- Direct impact
  - Stuxnet
  - TRISIS
  - BlackEnergy 2 and BlackEnergy 3
  - FrostyGoop
  - Industroyer
- Indirect impact
  - Colonial Pipeline
  - SolarWinds
  - Maersk
  - AcidRain
  - 2024 CrowdStrike
  - Collins Aerospace/RTX

3.3 Explain key components of OT threat landscapes.

- Threat actors
  - Insider threats
    - Unintentional
    - Intentional
  - Hacktivists
  - Nation-states/advanced persistent threats (APTs)
  - Espionage
  - Cybercriminals
    - Extortion
- Threat vectors
  - Remote access
    - Third-party users
    - Internal users
  - Removable media
  - Social engineering
    - Phishing
    - Vishing
  - Account compromise
  - Supply chain
    - Firmware
  - Lateral movement
  - Pivot from IT to OT
  - Unauthorized devices
  - Misconfigurations
  - Vulnerability exploitation
  - On-path attacks
  - Quick response (QR) code security vulnerabilities
  - Cell-based
    - Subscriber Identity Module (SIM) swapping
    - Rogue base station

3.4 Given a scenario, analyze OT threat intelligence for cyberdefense.

- OT threat intelligence sources and feeds
  - Third-party services
    - Private
    - Original equipment manufacturer (OEM) vendor
    - Volunteer
    - Bug bounties
    - Social media platforms
  - Information Sharing and Analysis Centers (ISACs)
  - Government agencies
- Threat intelligence platforms
- File types
  - Yet Another Recursive Acronym (YARA)
  - Structured Threat Information Expression (STIX)
- Indicators of compromise (IOCs)
  - Hashes
  - Internet Protocol (IP) addresses
  - Malicious domains
  - Usernames
  - Email addresses
  - Registry modification
  - Abnormal processes
  - Unusual logs
  - Sessions
- Tactics, techniques, and procedures (TTP)

4.0 OT Cybersecurity Architecture, Design, and Engineering

4.1 Explain secure OT architectural principles.

- Least privilege and functionality
- Operational resilience
  - Endurance
  - Redundancy
  - High availability
  - Recoverability
- Compartmentalization
- Performance
- Criticality
- Auditability
- Observability
- Deterministic
- Interoperability/compatibility
- Simplicity
- Defense in depth

4.2 Summarize physical security concepts.

- Access control systems
  - Badges/fobs
  - Readers
  - Biometrics
  - Turnstiles
- Access control vestibule
- Room and cabinet security
  - Cable security
  - Intermediate distribution frames (IDFs)
  - Main distribution frames (MDFs)
- Surveillance
  - Physical walkdown/inspection
  - Video
  - Motion detection
  - Spectrum analyzer
- Fences
- Bollards

4.3 Given a scenario, determine the applicable hardware security controls and settings.

- Hardened physical interfaces
  - Port lockers
  - Port blockers
- PLC operating modes
- Designing backup strategy
- Updating firmware
- Implementing backups and settings
- Tamper detection and protection
- Drive encryption
- Secure Boot
- Root of trust/Trusted Platform Module (TPM)
- Hardware access control
- Port protocols and services management
- Secure removable media

4.4 Given a scenario, apply appropriate host and application security practices.

- Security applications
  - Host-based firewall
  - Host-based intrusion detection system (HIDS)
  - Endpoint protection platform (EPP)
  - Endpoint detection and response (EDR)
  - Endpoint privilege management (EPM)
- Applying patches and device updates
- Software access control
  - Role-based access control
  - Attribute-based access control (ABAC)
  - Mandatory access control
- Code signing and verification
- Configuring OS benchmarks
- Integrity verification and validation
- Deactivating debug interfaces
- Changing read/write protection settings

4.5 Given a scenario, recommend appropriate network security controls and designs.

- Assess rules and access control lists (ACLs)
  - Network
  - Explicit firewall policy
  - Allow list
  - Block list
- Port, protocol, and service management
  - Endpoint
  - Network
- Network access control
  - Media access control-based
  - Certificate-based
  - Token-based
- Segmentation and data flow enforcement
  - Physical
  - Logical
    - Subnetting
    - Virtual local area network (VLAN)
- Proper encryption location
- Proxy
- Data diodes/unidirectional gateway
- OT-aware intrusion prevention system (IPS)/intrusion detection system (IDS)
- Wireless management
- Internal network security monitoring
  - Traffic collection
  - Flow collection
  - Log aggregation
  - Baselining
    - Asset
    - Application
    - User
    - Network
- Domain Name System (DNS) security
  - Query log collection
  - Reverse lookups
- Out-of-band (OOB) management
- Zones and conduits
  - Industrial demilitarized zone (IDMZ)

4.6 Given a scenario, recommend the appropriate identification, authentication, and authorization controls.

- Device and application account types
  - Service
  - Shared
  - Individual
  - Privileged
  - Local
- Change default passwords
- Directory services
  - Group Policy
- Use of public key infrastructure (PKI)
  - Device and user certificates
  - Registration authority
- Access protocols
  - Remote Authentication Dial-in User Service (RADIUS)
  - Terminal Access Controller Access-control System Plus (TACACS+)
- Password and credential management
  - Single sign-on (SSO)
  - Multifactor authentication (MFA)
  - Privileged access management (PAM)
- Secure remote access
  - Jump box/bastion

5.0 OT Security Operations

5.1 Summarize the purpose of asset management tasks.

- Asset inventory
  - Discovery
    - Passive
    - Active
    - Manual
  - Creation
  - Validation
  - Maintenance
- Key asset attributes
  - IP address
  - System ID
  - Model number
  - Version number
  - Media access control address
  - Physical location
    - Site
    - Panel
  - Ports
  - Owner
  - Function
  - Vendor
  - Obsolescence
  - Device type
- Software inventory
  - Map to asset inventory
- Mapping attributes to configuration management database (CMDB)
- Collection management framework

5.2 Given a scenario, analyze data in support of security operations.

- Control system
  - Process logs
  - Change logs
  - Function codes
- Network and boundary
  - IDS
  - Packet capture
  - Syslog
  - Firewall
  - Switch
  - Router
  - Edge devices
- Host and security
  - Authentication, authorization, and accounting (AAA)
    - Access logs
  - EDR
  - EPP
  - OS and application
  - Identity logs
- Threat-hunting artifacts
- Security management system tuning
  - IDS rules
  - Firewall rules
  - Network performance monitoring (NPM)
  - EPP policy
  - EDR policy
  - Security information and event management (SIEM)
  - Security orchestration, automation, and response (SOAR)

5.3 Explain the role of vulnerability remediation in an OT security program.

- Remediation options
  - Patch or update
    - Availability
    - Applicability
    - Viability
    - Dependency

        - Mitigating controls
        - Compensating controls
        - Version management
    - Internal stakeholder coordination
        - Remediation selection
        - Remediation timeline
        - Remediation implementation window
        - Spare availability
        - Backup availability
        - Scheduling planned downtime
    - Testing
    - Implementation
    - Process validation
    - Rollback plan availability

5.4 Given a scenario, apply the appropriate techniques to facilitate vulnerability management.

- External vulnerability identification
- Internal vulnerability identification
- Detection methods
    - Passive
    - Active
    - Derived
- Data sources
    - Software bill of materials (SBOM)
    - Vendor
    - National Vulnerability Database (NVD)
- Triage
    - Applicability
    - Prioritization
        - Exposure
        - Relevance
        - Exploitability
        - Severity
        - Impact
- Vulnerability remediation verification

5.5 Explain the importance of portable device security in OT environments.

- Removable media
    - Scanning
        - Kiosks
        - Anti-malware
    - Dedicated devices
    - Authorization
    - Destruction
    - Procurement
    - Tracking
    - Tamper-proofing validation
    - Sanitization
    - Secure physical storage
    - Write blocker
    - Data loss detection
- Mobile devices
    - Corporate-owned
    - Third-party laptops
    - Compute devices
    - Calibration equipment
    - Phones
    - Tablets
    - Accessories
    - Device and network authentication
    - Wearables
- Security validation/posture checks
- External connections
    - Persistent
    - Temporary
    - Geolocation

6.0 OT Incident Management

6.1 Describe incident management frameworks.

- Preparation, Identification, Containment, Eradication, Recovery, and Lessons learned (PICERL) model
  - Prepare
  - Identify
  - Contain
  - Eradicate
  - Recover
  - Lessons learned
- Incident Command System
  - Incident Command System for Industrial Control Systems (ICS4ICS)

6.2 Summarize overarching incident management considerations.

- Cybersecurity response
- Physical response
  - Emergency services
  - Emergency shutdown (ESD)
- Crisis management
- Facilities
  - Operations
  - Engineering
  - Maintenance
- Coordination between IT and OT
  - Handling nuances of incident response (IR) in OT environments
- Mutual aid
  - Internal
  - Peers
    - ISACs
  - Incident response retainers (IRRs)
- Escalation and notification
  - Internal
  - External
    - Government agencies
    - Regulators

6.3 Given a scenario, perform activities to prepare for incidents.

- Draft or update documentation
  - OT incident response plan (IRP)
  - Playbooks
- Incident preparedness activities
  - Purple-team exercises
  - Tabletop exercises (TTXs)
  - Simulations
  - Runbooks
- Leverage understanding
  - High-value assets
  - Attack surface

6.4 Explain IR and handling.

- Flyaway kit (FAK)
  - PPE
  - Tooling
- Decision matrices
  - Declaration
  - Shutdown
  - Payment
    - Office of Foreign Assets Control (OFAC)
    - Ransom
- Triaging
  - Scoping
- Chain of custody
- IRR types
  - Third-party
  - Vendors
  - Insurers
- Primary impacts
  - Manipulation of:
    - View
    - Control
    - Safety
  - Loss of:
    - View
    - Control
    - Safety
- Advanced collection data sets
  - Process
    - Historian data
    - Sequence of events
    - Operator logs
  - Host
    - Memory
      - Workstation
      - Server
      - Device
    - Disk
    - Registry
  - User logs
    - Access
    - Activity
- Root cause analysis (RCA)

6.5 Given a scenario, analyze common data sets collected during IR.

- System documentation
  - Deviation from baseline
  - Anomalous behavior
  - Deviation from design
- Network
  - Flow data
  - Firewall logs
  - Industrial control systems protocols
  - Packet captures
  - IDS (if available)
  - Deception technologies (if applicable)
  - Internet service provider (ISP) logs
  - Syslogs
- Host (disk)
  - OS events
  - Application logs
  - Security logs
  - sudo logs
  - systemd logs

6.6 Compare and contrast concepts related to the containment, eradication, and recovery processes.

- Containment
  - Isolate
  - Quarantine
  - Disconnect IT and OT
  - Block traffic
  - Suspend accounts
- Eradication (when possible)
  - Remove compromised components
  - Remove malware from critical systems
  - Reset compromised credentials
- Recovery
  - Restoration of affected devices
  - Bare metal
  - Process validation
  - Hot swap
  - Redesign
- Lessons learned
  - Hot wash/debrief
  - Postmortem
- Mandatory reporting
  - Regulatory
  - Insurance
  - Emergency notifications
  - Contract obligation

CompTIA SecOT+ Acronym List

The following is a list of acronyms that appear on the CompTIA SecOT+ SOT-001 V1 certification exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as part of a comprehensive exam preparation program.

ACRONYM	DEFINITION
AAA	Authentication, Authorization, and Accounting
ABAC	Attribute-based Access Control
ACL	Access Control List
AI	Artificial Intelligence
AIS	Automated Information System
APT	Advanced Persistent Threat
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
BACnet	Building Automation and Control Networks
BIND	Berkeley Internet Name Domain
CA	Certificate Authority
CIP	Common Industrial Protocol
CMDB	Configuration Management Database
CRA	Cybersecurity Risk Assessment
DCS	Distributed Control System
DNP3	Distributed Network Protocol 3
DNS	Domain Name System
EDR	Endpoint Detection and Response
EPM	Endpoint Privilege Management
EPP	Endpoint Protection Platform
ESD	Emergency Shutdown
EtherCAT	Ethernet for Control Automation Technology
FAK	Flyaway Kit
HIDS	Host-based Intrusion Detection System
HMI	Human-machine Interface
I/O	Input/Output
ICS4ICS	Incident Command System for Industrial Control Systems
IDF	Intermediate Distribution Frame
IDMZ	Industrial Demilitarized Zone
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IOC	Indicator of Compromise
IP	Internet Protocol
IPS	Intrusion Prevention System

ACRONYM	DEFINITION
IR	Incident Response
IRP	Incident Response Plan
IRR	Incident Response Retainer
ISA	International Society of Automation
ISAC	Information Sharing and Analysis Center
ISP	Internet Service Provider
JSA	Job Safety Analysis
MDF	Main Distribution Frame
MES	Manufacturing Execution System
MFA	Multifactor Authentication
ML	Machine Learning
MOU	Memorandum of Understanding
MSA	Master Service Agreement
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NPM	Network Performance Monitoring
NS2	Network Segment 2
NVD	National Vulnerability Database
OEM	Original Equipment Manufacturer
OFAC	Office of Foreign Assets Control
OOB	Out-of-band
OPC DA	Open Platform Communications Data Access
OPC UA	Open Platform Communications Unified Architecture
OpenSSL	Open Secure Sockets Layer
OS	Operating System
OSINT	Open-source Intelligence
OT	Operational Technology
PAM	Privileged Access Management
PICERL	Preparation, Identification, Containment, Eradication, Recovery, and Lessons learned
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PPE	Personal Protective Equipment
QR	Quick Response
RA	Registration Authority
RACI	Responsible, Accountable, Consulted, Informed
RADIUS	Remote Authentication Dial-in User Service
RCA	Root Cause Analysis
RTOS	Real-time Operating System
RTU	Remote Terminal Unit
SBOM	Software Bill of Materials
SCADA	Supervisory Control and Data Acquisition
SDN	Software-defined Network

ACRONYM	DEFINITION
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SIS	Safety Instrumented System
SLA	Service-level Agreement
SOAR	Security Orchestration, Automation, and Response
SOW	Statement of Work
SSO	Single Sign-on
STIX	Structured Threat Information Expression
TACACS+	Terminal Access Controller Access-control System Plus
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
TTP	Tactics, Techniques, and Procedures
TTX	Tabletop Exercise
TX	Transmitter
VFD	Variable Frequency Drive
VHF	Very High Frequency
VLAN	Virtual Local Area Network
VM	Virtual Machine
VSAT	Very Small Aperture Terminal
YARA	Yet Another Recursive Acronym

CompTIA SecOT+ Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the SecOT+ SOT-001 V1 certification exam. This list may also be helpful for training companies that wish to create a lab component for their training offering. The bulleted lists below each topic are sample lists and are not exhaustive.

HARDWARE

- Tablet
- Server-class hardware
- Laptops with legacy serial (RS-232, etc.) port capability
- Web server
- Firewall
- Router
- Switches (with ability to clone/span ports)
- Serial cables
- Cat 5e/Cat 6 Ethernet cables
- Optical cables
- Unidirectional gateway/one-way taps/transmitter (TX)-only fiber
- Network tap
- Spectrum analyzers
- PLC and HMI hardware
- Sensors (e.g., speed, environmental)

SOFTWARE

- Windows OS
- Linux OS
- FreeRTOS
- Embedded Linux variants
- Reverse and forward proxy software
- Endpoint protection
  - Malware protection
  - HIDS
- Web server with Transport Layer Security (TLS) support
- DNS daemon (e.g., Berkeley Internet Name Domain [BIND])
- Lightweight PKI with certificate authority (CA) and registration authority (RA)
- Crypto tools (e.g., Open Secure Sockets Layer [OpenSSL])
- OT- and OT-protocol-aware security appliances
  - Firewall
  - IDS
- Packet analyzers
- Open-source SIEM
- Lightweight log aggregation service
- Controllers, including lightweight/inexpensive PLCs (e.g., OpenPLC, Velocio)
- SCADA platform
- Historian
- Hypervisor(s)
- OT-specific virtual machine (VM) images like vPLCs
- SDN-capable virtual infrastructure
- Passive and/or active enumeration utilities
- Tool set platform (e.g., ControlThings.io)
- Incident management tool set (e.g., REMnux)
- PLC and HMI programming software

OTHER

- Packet captures (pcaps) of common protocols (Modbus, CIP, etc.)
- Pcaps of known-bad traffic, tied to IoCs
- Sample IoCs (e.g., in STIX format for manipulation)
  - Network level
  - Host/device level
  - Application level
- Organizational and operational risk management templates
  - Vulnerability assessment and risk assessment templates (DOCX/PPTX)
  - Sample risk register
  - Sample RACI matrix