Appendix A: Further Reading/Resources

DISCLAIMER: This list is not meant to be a complete list of resources or a recommendation of a particular product. These resources are here to get you started on your journey to securing your ICS network.

Virtual Machine Download –

ICS-CERT/CISA Documents

- Guide to Critical Infrastructure Security and Resilience - https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf
- ICS-CERT Documents (Alerts, Advisories, White Papers,etc) – https://www.us-cert.gov/ics/Information-Products
- Seven Steps to Effectively Defend Industrial Control Systems – https://www.us-cert.gov/ics/Information-Products -> Other ICS White Papers
- ICS Recommended Practices - https://www.us-cert.gov/ics/Recommended-Practices
- Industrial Control Systems Vulnerabilities and Resources - https://www.dhs.gov/sites/default/files/publications/2019-csss-ics-vulnerabilities-resources-508.pdf

NIST Documentation

- NIST SP 800-82 Rev 2 - Guide to Industrial Control Systems (ICS) Security - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
- NIST SP 800-53 Rev 4 - Security and Privacy Controls for Federal Information Systems and Organizations - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- NIST SP 800-61 Rev. 2 - Computer Security Incident Handling Guide - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- NIST SP 800-167 - Guide to Application Whitelisting- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf
- NIST SP 800-82r2 – Guide to Industrial Control Systems (ICS) Cybersecurity - https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf
- NIST Framework for Improving Critical Infrastructure Cybersecurity – https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

NSA Documentation - https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/industrial-control-systems/index.cfm

Incident Reports

- Booz Allen Threat Reports:

    - https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf
    - https://www.slideshare.net/BoozAllen/booz-allen-industrial-cybersecurity-threat-briefing
- Dragos Year-in-Review - https://dragos.com/yearinreview/2017/
- NASA JPL Report - https://oig.nasa.gov/docs/IG-19-022.pdf
- SANS 2019 State of OT/ICS Cybersecurity Survey - https://radiflow.com/wp-content/uploads/2019/06/Survey_ICS-2019_Radiflow.pdf
- OT/ICS Survey info graphic - https://www.sans.org/media/Infographic_OT-ICS_Survey_final.pdf
- MITRE - https://collaborate.mitre.org/attackics/index.php/All_Techniques

SCADA/ICS Security Websites/Mailing Lists

- SCADA Hacker - https://scadahacker.com/index.html
- Scadasec - http://news.infracritical.com/mailman/listinfo/scadasec
- Belden Blog - http://www.belden.com/blog/index.cfm
- Awesome Industrial Control System Security Tools - https://github.com/hslatman/awesome-industrial-control-system-security
- SANS ICS Community - https://ics-community.sans.org/
- Control Things - https://www.controlthings.io/home

===

Application Whitelisting

- Lumension - http://www.lumension.com
- Microsoft AppLocker (may not be considered Application Whitelisting by regulatory agencies) - https://docs.microsoft.com/en-us/search/index?search=AppLocker
- NIST SP 800-167 - Guide to Application Whitelisting- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf
- Savant Protection - http://www.savantprotection.com
- Tripwire - https://www.tripwire.com/misc/tripwire-whitelist-profiler-register/
- Carbon Black - https://www.carbonblack.com/

Assessments

- Assess the Mess - https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/industrial-control-systems/assess-the-mess.cfm
- Open Source Risk Assessment - http://media.techtarget.com/searchSecurityUK/downloads/RHUL_Yoav_v2.pdf
- Simple Risk - https://www.simplerisk.com/
- Cyber Security Evaluation Tool (CSET) - https://www.us-cert.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_CSET_S508C.pdf

- CSET 9.0 Download - https://github.com/cisagov/cset

Asset Inventory

- Tenable Industrial Security - https://www.tenable.com/products/industrial-security
- Langer - https://www.langner.com/ot-base/
- Forescout - https://www.forescout.com/company/blog/4-business-advantages-of-efficient-asset-inventory-for-ics/
- Nozomi Networks - https://www.nozominetworks.com/blog/reduce-ot-risk-with-ics-network-visualization-and-asset-inventory/
- Security Matters - https://www.secmatters.com/product
- Splunk - https://splunkbase.splunk.com/app/4287/
- Grass Marlin - https://github.com/nsacyber/GRASSMARLIN

Cheat Sheets

- Scada Hacker Cheat sheets - https://scadahacker.com/library/index.html#cheatsheets
- Information Security Cheat Sheets from Lenny Zeltzer – https://zeltser.com/cheat-sheets/
- Wireshark Display Filters - https://scadahacker.com/library/Documents/Cheat_Sheets/Networking%20-%20Wireshark%20-%20Display%20Filters%202.pdf
- Nmap cheat sheets - https://blogs.sans.org/pen-testing/files/2013/10/NmapCheatSheetv1.1.pdf
- Information Security Cheat Sheets from Lenny Zeltzer – https://zeltser.com/cheat-sheets/
- ICS Ports and Protocols - https://github.com/ITI/ICS-Security-Tools/blob/master/protocols/PORTS.md
- common_ports.pdf - http://packetlife.net/media/library/23/common_ports.pdf
- Wireshark Commands - https://stationx-public-download.s3.us-west-2.amazonaws.com/Wireshark-Cheat-Sheet-v1.pdf

Data Diodes

- Air-Gaps, Firewalls And Data Diodes In Industrial Control Systems - https://www.nexor.com/wp/wp-content/uploads/2017/05/Air-Gaps-Firewalls-and-Data-Diodes-in-Industrial-Control-Systems.pdf
- Owl Cyber Defense About Data Diodes - https://owlcyberdefense.com/learn-about-data-diodes/
- Waterfall Security Use Cases - https://waterfall-security.com/scada-security/use-cases
- Tactical Data Diodes in Industrial and Automation and Control System - http://www.sans.org/reading-room/whitepapers/firewalls/tactical-data-diodes-industrial-automationcontrol-systems-36057
- Data Diode Manufacturers - https://www.securitywizardry.com/index.php/products/boundary-guard/data-diodes/all.html

Firewalls NG

- Checkpoint - https://www.checkpoint.com/products-solutions/critical-infrastructure/
- CyberRoam - https://www.cyberoam.com/ics_security.html
- PaloAlto - https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall

- Fortinet - https://www.fortinet.com/solutions/industries/scada-industrial-control-systems.html
- Tofino - https://www.tofinosecurity.com/products/tofino-xenon-security-appliance
- SANS Firewall Checklist - https://www.sans.org/media/score/checklists/FirewallChecklist.pdf

Forensic Tools

- SIFT Workstation - https://digital-forensics.sans.org/community/downloads
- Forensic Toolkit (FTK) - https://accessdata.com/products-services/forensic-toolkit-ftk
- Encase - https://www.guidancesoftware.com/encase-forensic
- NetworkMiner - https://www.netresec.com/index.ashx?page=NetworkMiner
- CAINE - https://www.caine-live.net/

Honeypots

- ADHD - https://www.blackhillsinfosec.com/projects/adhd/
- Conpot, an ICS/SCADA Honeypot – http://conpot.org/
- Honey Drive - http://bruteforcelab.com/honeydrive
- SCADA Honeynet Project - http://scadahoneynet.sourceforge.net/
- SCADA Honeynets - http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=3130&context=etd

  The attractiveness of honeypots as critical infrastructure security tools for the detection and analysis of advanced threats, Susan Wade, 2011, Iowa State University

IDS: Host Based Intrusion Systems (HIDS)

- AFICIK - Another file integrity checker - http://afick.sourceforge.net/
- AIDE - Advanced intrusion detection environment - https://wiki.archlinux.org/index.php/AIDE -
- OSSEC - Open source host-based intrusion detection system - http://www.ossec.net
- SAMHAIN - File integrity/host-base IDS - http://www.la-samhna.de/samhain/
- Tiger - An integrity checker - http://www.nongnu.org/tiger/

IDS: Network Based Intrusion Systems (NIDS)

- Zeek (aka BroIDS) - https://www.zeek.org/
- Quickdraw (Snort Rules) - http://www.digitalbond.com/tools/quickdraw/
- Security Matters - http://www.secmatters.com/products-ics
- Snort – http://www.snort.org
- Tofino - https://www.tofinosecurity.com/articles/blog-tags/ics

Incident Response Checklists and Tools

- LM-White-Paper-Intel-Driven-Defense.pdf - http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
- OIG-13-027-A.pdf - https://www.oig.doc.gov/oigpublications/oig-13-027-a.pdf
- SANS Incident Handler's Handbook – https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
- SANS Sample Incident Handling Forms – https://www.sans.org/score/incident-forms
- Information Security Cheat Sheets from Lenny Zeltzer – https://zeltser.com/cheat-sheets/
- Fireeye Incident Response Tools - https://www.fireeye.com/services/freeware.html
- FTK Imager - https://accessdata.com/product-download/ftk-imager-lite-version-3.1.1

Information Sharing and Analysis Centers

- National Council of ISACs (see Appendix E) - https://www.nationalisacs.org/
- Information Sharing and Analysis Organizations - https://www.isao.org/information-sharing-groups/
- DOE Cyber Risk Information Sharing Program - https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity
- DHS Information Sharing Program (CISCP) - https://www.dhs.gov/cisa/cyber-information-sharing-and-collaboration-program-ciscp

MITRE ATT&CK Framework

- Enterprise Version - https://attack.mitre.org/matrices/enterprise/
- ICS version - https://collaborate.mitre.org/attackics/index.php/Main_Page
- Pre ATT&CK Matrix - https://attack.mitre.org/matrices/pre/
- Mobile Version - https://attack.mitre.org/matrices/mobile/

Netflow

- EHNT - http://ehnt.sourceforge.net/
- FlowScan - http://pages.cs.wisc.edu/%7Eplonka/FlowScan/
- JKFlow - http://jkflow.sourceforge.net/
- Lancope - https://www.lancope.com/resources/solution-briefs/improving-performance-security-and-compliance-utilitiesenergy-networks
- NFdump - http://nfdump.sourceforge.net/
- NfSen - http://nfsen.sourceforge.net/
- NTop - http://www.ntop.org/
- Plixer – http://www.plixer.com
- SiLK - http://tools.netsa.cert.org/

Network Discovery/Situational Awareness/Scanning Tools

* indicates ICS specific tools or companies with ICS specific products

- Assess the Mess* - https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/industrial-control-systems/assess-the-mess.cfm
- EtherApe - http://etherape.sourceforge.net/
- Grassmarlin* – ICS Network Awareness Tool - https://github.com/iadgov/GRASSMARLIN
- Moloch – large scale full packet capturing, indexing and database system - https://molo.ch/
- Nessus and ICS* - https://www.tenable.com/taxonomy/term/357
- NexDefense Integrity - https://www.nexdefense.com/
- Nexpose - https://www.rapid7.com/products/nexpose/
- Nikto – Web Scanning Tool - https://cirt.net/Nikto2
- Nmap cheat sheets - https://blogs.sans.org/pen-testing/files/2013/10/NmapCheatSheetv1.1.pdf
- Nmap Scripts
    - https://github.com/SpiderLabs/Nmap-Tools/tree/master/NSE
    - https://github.com/digitalbond/Redpoint
    - https://github.com/ITI/ICS-Security-Tools/tree/master/scripts
- OWASP ZAP (ZED Attack Proxy) – Web Scanning Tool - https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
- Red Seal – Network Visulization - https://www.redseal.net/
- Solarwinds Tools - https://www.solarwinds.com/downloads (scroll down the page to Free Tools)

Network Headers

- common_ports.pdf - http://packetlife.net/media/library/23/common_ports.pdf
- ipv6_tcpip_pocketguide.pdf - https://www.sans.org/security-resources/ipv6_tcpip_pocketguide.pdf
- packetlife.net.pdf – http://packetlife.net/library/cheat-sheets/
- IANA ports and services - https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml
- http://www.tcpipguide.com/free/t_IPDatagramEncapsulation.htm
- Protocols and network security in ICS infrastructures - https://www.incibe.es/extfrontinteco/img/File/intecocert/ManualesGuias/incibe_protocol_net_security_ics.pdf
- ICS Ports and Protocols - https://github.com/ITI/ICS-Security-Tools/blob/master/protocols/PORTS.md

Network Taps

- Gigamon - https://www.gigamon.com/products/visibility-nodes/network-taps.html
- Ixia - https://www.ixiacom.com/products/network-taps-regenerators-and-aggregators
- Throwing Star Lan Tap Pro - https://hakshop.com/products/throwing-star-lan-tap-pro
- What are Network Taps - http://www.networkcritical.com/more/resources/what-are-taps

Open Source Intelligence (OSINT)

- Shodan – shodan.io
- Zmap – censys.io
- How Shodan works - https://ics-community.sans.org/t/18rphp/public-facing-industrial-control-systems
- 7 steps to searching with Shodan - https://www.darkreading.com/iot/7-steps-to-start-searching-with-shodan/d/d-id/1332684?image_number=1
- Security Trails Total Internet Inventory - http://www.securitytrails.com/

OPSEC

- NIST 800-53 SC 38 - https://nvd.nist.gov/800-53/Rev4/control/SC-38
- Using Operational Security (OPSEC) to Support a Cyber Security Culture in Control Systems Environments - https://www.us-cert.gov/sites/default/files/recommended_practices/RP_Using%20OpSec_v1_Draft.pdf
-

Password Management Tools/Data

- Beyond Trust - https://www.beyondtrust.com/solutions/enterprise-password-management/
- ManageEngine - https://www.manageengine.com/products/passwordmanagerpro/
- CyberArk - https://www.cyberark.com/
- World's biggest data breaches - https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks

Penetration Testing Tools

- CoreImpact - https://www.coresecurity.com/core-impact
- SAINT - http://www.saintcorporation.com/
- Metasploit (Rapid7) - https://www.metasploit.com/
- SANS_Meterpreter_Cheat_Sheet.pdf - https://www.sans.org/security-resources/sec560/misc_tools_sheet_v1.pdf
- Armitage Tutorial - Cyber Attack Management for Metasploit.pdf - http://www.fastandeasyhacking.com/manual

Proxy Servers/Web Filters

- Squid - http://www.squid-cache.org/Intro/
- Artica - http://www.articatech.com/
- IPFire - https://www.ipfire.org/features

Purdue Enterprise Reference Architecture

- Wikipedia description - https://en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture
- Secure Architecture for Industrial Control Systems - https://www.sans.org/reading-room/whitepapers/ICS/paper/36327
- Cybersecurity at the edge (Purdue Reference Model Level 0,1 field devices cybersecurity risks) - https://www.isa.org/intech/20180605/

Security Awareness Training Resources – The Human aspect of Cyber Security

Available online resources for Security Awareness Training (this list is not all inclusive):

Source	URL	Type	Cost
Cyber Safe Workforce, LLC	https://www.cybersafeworkforce.com/	Tookit, Materials	$
DHS National Cyber Security Awareness	http://www.dhs.gov/national-cyber-security-awareness-month	Toolkit, Materials	FREE
DHS Stop.Think.Connect	https://www.dhs.gov/publication/stopthinkconnect-industry-resources	Toolkit, Materials	FREE
DOD IASE Training	http://iase.disa.mil/eta/Pages/index.aspx	Videos	FREE
DOD Cyber Exchange Public Training	https://public.cyber.mil/cyber-security-training/ NOTE: This training is also good for cyber defenders	Online	Free
ICS-CERT Virtual Learning Portal	https://ics-cert-training.inl.gov	Training, Materials	FREE
Knowbe4	http://www.knowbe4.com/	Training, Materials	$
MSI Simple Phish	http://microsolved.com/free-tools.html	Phishing Test	FREE
Multi State Information Sharing and Analysis Center	http://msisac.cisecurity.org/	Materials	FREE
National Cyber Security Alliance	https://www.staysafeonline.org/	Materials	FREE
Native Intelligence	http://www.nativeintelligence.com/	Videos, Newsletters, Materials	FREE/$
OpenDNS quiz	https://www.opendns.com/phishing-quiz/	Training	FREE
Cofense (Phish Me)	https://cofense.com/	Phishing Test	$
PhishBox	http://www.phishingbox.com/	Phishing Test	$
SANS: IT Information Security Awareness Training	http://www.securingthehuman.org/utility	Toolkit, Training, Materials	FREE/$

SecureWorks	http://www.secureworks.com/	Training, Materials	$

Security Controls (System Hardening)

- Australian Defense Signals Directorate (DSD.gov.au) “Top 35 Mitigation Strategies” - http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
- Bastille Unix - Supports Linux, Unix, HP-UX and Mac OSX - http://bastille-linux.sourceforge.net/
- Center for Internet Security - http://www.cisecurity.org/
- DISA Information Assurance Support Environment Checklists - https://iase.disa.mil/stigs/Pages/index.aspx
- ISA62443, Industrial Automation and Control Systems Security - https://www.isasecure.org/en-US/
- ISO/IEC 27019:2017 - Information security controls for the energy utility industry - https://www.iso.org/standard/68091.html
- NIST 800-82 - Guide to Industrial Control Systems (ICS) Security - https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
- NERC CIP Controls - http://www.nerc.com/pa/CI/Comp/Pages/default.aspx
- SANS “Top Cyber Security Risks” - http://sans.org/top-cyber-security-risks/
- SANS “Twenty Critical Controls for Effective Cyber Defense” - https://www.sans.org/critical-security-controls
- A Short Guide to Infrastructure Security and Resiliency - https://www.cisecurity.org/blog/a-short-guide-to-infrastructure-security-and-resiliency/

Supply Chain

- Deloitte Report, Managing cyber risk in the electric power sector - https://www2.deloitte.com/insights/us/en/industry/power-and-utilities/cyber-risk-electric-power-sector.html
- Department of Homeland Security: Cyber Security Procurement Language for Control Systems - https://www.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf
- Cybersecurity Procurement Language for Energy Delivery Systems - https://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf
- Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector: Recognizing Risks and Recommended Mitigation Actions - https://www.odni.gov/files/PE/Documents/11---Supply-Chain-Risks-of-SCADA-Industrial-Control-Systems-in-the-Electricity-Sector_Risks-and-Mitigations.pdf
- Simplifying the ICS Cyber Security Vendor Selection Process - https://www.nozominetworks.com/blog/simplifying-the-ics-cyber-security-vendor-selection-process/

Test Lab Ideas

- Building a Modest Test Lab - https://www.toreon.com/ics-security/how-do-you-build-a-modest-ics-testing-training-lab/
- Industrial Protocols:security tools - https://www.certsi.es/en/blog/industrial-protocols-security-tools

- Modbus Simulator - http://www.modbustools.com/modbus_slave.html
- Matrikon OPC - https://www.matrikonopc.com/products/opc-drivers/opc-simulation-server.aspx
- OpenDPN3 Simulator - https://www.automatak.com/opendnp3/docs/guide/current/
- Open PLC - http://www.openplcproject.com/
- Scada BR - http://www.scadabr.com.br/ (use Google Translate)

Threat Intelligence: Software

- Structured Threat Information Graph - https://github.com/idaholab/STIG

Threat Intelligence: Top Public Cyber Feeds

- AlienVault.com: Multiple sources including large honeynets that profile adversaries.
- CrowdStrike.com: Advanced threat intel as part of their threat protection platform.
- EmergingThreats.net: A variety of feeds.
- FireEye.com: DTI- Dynamic Threat Intelligence service.
- HexisCyber.com: Feed supports automated actions.
- InternetIdentity.com: Threat feeds from their big data solution ActiveTrust.
- iSightPartners.com: ThreatScape series.
- MalwareCheck.org: Intelligence on any URL.
- MalwareDomains.com: A list of domains known to be associated with malware.
- RecordedFuture.com: Organizes information from the Internet.
- RedSkyAlliance.com: A vetted team of corporate computer incident responders and security professionals.
- SecureWorks.com: Provides feeds and also instruments networks.
- SurfWatch.com: Insights tailored to your business.
- Symantec.com: DeepInsight feeds on a variety of topics including reputation.
- Team-Cymru.com: Threat intelligence plus bogon lists.
- ThreatConnect.com by Cyber Squared: Focused on information sharing.
- ThreatGrid.com: Unified malware analysis. Now part of Cisco.
- ThreatIntelligenceReview.com: Updated reviews of threat intelligence sources.
- ThreatStop.com: Block Botnets by IP reputation.
- ThreatStream.com: Famous team. Multiple sources in interoperable platform.
- ThreatTrack.com: Stream of malicious URLs,IPs and malware/phishing related data.
- Verisigninc.com: iDefense feeds highly regarded by some key institutions.

Threat Intelligence: Government Sources

- European Union Agency for Network and Information Security (ENISA) - https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada

- FBI Cyber Crime - http://www.fbi.gov/about-us/investigate/cyber
- Industrial Control Systems Computer Emergency Response Team (ICS_CERT) - https://www.us-cert.gov/ics/ICS-CERT-Feeds
- InfraGard - https://www.infragard.org
- The Defense Cyber Crime Center (DC3) - http://dc3.mil/
- US Computer Emergency Response Team (US-CERT) - https://www.us-cert.gov/

Threat Intelligence: Reports

- Checkpoint Security Report - https://www.checkpoint.com/resources/2014-security-report/
- Cisco Midyear Security Report - http://www.cisco.com/web/offers/lp/midyear-security-report/index.html?keycode=000502658
- Fireeye Current Threats Reports - https://www.fireeye.com/current-threats.html
- Human Factor Report - https://www.carahsoft.com/download_file/view_inline/61250
- Symantec Intelligence Report - https://www.symantec.com/security-center/threat-report
- Verizon Data Breach Investigations Report - http://www.verizonenterprise.com/verizon-insights-lab/dbir/
- Versign iDefense Cyber Threats and Trends - https://www.verisign.com/en_US/forms/reportcyberthreatstrends.xhtml

Training, Other and Podcasts

- Industrial Security Podcast - https://waterfall-security.com/scada-security/podcasts-on-ics-cybersecurity/
- CISA Training - https://www.cisa.gov/critical-infrastructure-training
- ICS-CERT Virtual Learning Portal - https://ics-cert-training.inl.gov/learn

Unified Cyber Security for ICS

- Tripwire Cybersecurity for ICS - https://www.tripwire.com/solutions/industrial-control-systems/

Unix Commands

- Unix_Commands.pdf - https://www.cmu.edu/computing/accounts/storage/afs-unix/commands.html
-

USB Management

- ODIX Kiosk - https://odi-x.com/critical-infrastructure-us-power-plant/
- Kingston Data Traveler - https://www.eset.com/us/business/kingston-datatraveler/
- USB Lock-RP - www.usb-lock-rp.com
- Honeywell Secure Media Exchange - https://www.honeywellprocess.com/en-us/online_campaigns/industrialcybersecurity/pages/smx/home.html

Web Application Firewalls (Open Source)

- AQTRONIX WebKnight - https://www.aqtronix.com/?PageID=99
- IronBee - https://www.ironbee.com
- ModSecurity - http://www.modsecurity.org/
- Smoothwall - http://www.smoothwall.org/about/
- WebCastellum - http://mvnrepository.com/artifact/org.webcastellum/webcastellum/1.8.3

VPN in Control Systems Network

- Managing Remote Access - https://www.us-cert.gov/ics/sites/default/files/recommended_practices/RP_Managing_Remote_Access_S508NC.pdf

Vulnerabilities and Risks

- Detect and Prevent Web Shell Malware - https://media.defense.gov/2020/Apr/22/2002285959/-1/-1/0/DETECT%20AND%20PREVENT%20WEB%20SHELL%20MALWARE.PDF
- NSA shares list of vulnerabilities commonly exploited to plant web shells - https://www.zdnet.com/article/nsa-shares-list-of-vulnerabilities-commonly-exploited-to-plant-web-shells/

Wireshark and BPF

- bpf_syntax.pdf - http://biot.com/capstats/bpf.html
- JStebelton_BPF.pdf - http://www.infosecwriters.com/text_resources/pdf/JStebelton_BPF.pdf
- snort_manual.pdf - https://www.snort.org/documents/snort-users-manual
- Wireshark_Display_Filters.pdf - http://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf
- Wireshark_user-guide - https://www.wireshark.org/download/docs/user-guide-a4.pdf

Unix Commands

- Unix_Commands.pdf - https://www.cmu.edu/computing/accounts/storage/afs-unix/commands.html