INL/EXT-17-42229
Revision 1

# A Survey of Security Tools for the Industrial Control System Environment

Carl M. Hurd,
ORCID: 0000-0001-6732-5780,

Michael V. McCarty
ORCID: 0000-0001-7133-556X

May 2017

* A Survey of Security Tools for the Industrial Control System Environment [DISTAR Case 28295]

This document was cleared by DARPA on August 4, 2017. All copies should carry the Distribution Statement "A" (Approved for Public Release, Distribution Unlimited). If you have any questions, please contact the Public Release Center.

DARPA Public Release Center (PRC)
675 N. Randolph Street, Room 03-028
Arlington, VA 22203-1714
Main: (571) 218-4235

The INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance

Idaho National Laboratory

**INL/EXT-17-42229**
**Revision 0**

# A Survey of Security Tools for the Industrial Control System Environment

Carl M. Hurd, Michael V. McCarty
**ORCID: 0000-0001-6732-5780, ORCID: 0000-0001-7133-556X**

**May 31, 2017**

**Idaho National Laboratory**
**Idaho Falls, Idaho 83415**

**http://www.inl.gov**

# A Survey of Security Tools for the Industrial Control System Environment

**INL/EXT-17-42229**
**Revision 0**

# EXECUTIVE SUMMARY

This report details the results of a survey conducted by Idaho National Laboratory (INL) to identify existing tools which could be used to prevent, detect, mitigate, or investigate a cyber-attack in an industrial control system (ICS) environment. This report compiles a list of potentially applicable tools and shows the coverage of the tools in an ICS architecture.

ICS environments are comprised largely of components with custom operating systems (OS) and network protocols and thus, tools to address cyber-security issues are hard to find, especially in those areas of the architecture closest to field and input/output (I/O) devices. This paper focuses on these little-covered areas to highlight the need for a more expansive toolset and to raise awareness of tools that may not be well known but may help mitigate attacks in an ICS environment. Although INL did not target enterprise-level solutions for this paper, enterprise-level solutions that extend into the ICS environment or demonstrate applicability beyond the business network have been included.

During the survey, INL found growing interest in development for the ICS security market; however, there were few established tools to detect malicious anomalies common to areas of an ICS environment. Tools for log review and outlier analysis within the controller Local Area Network / Field I/O Device zone were the most difficult to find. The survey found no tools to investigate proprietary log files or scan ladder logic applications for malicious behavior. Although some field devices may have embedded Linux or a similar embedded OS that lends itself to standard log formats and investigation methods, the majority of devices use a proprietary vendor-specific OS that is opaque to traditional security tools.

The survey identified tools such as Bro, Snort, and YARA which are, by design, highly extensible; enough so, that with minor development they could be used as ICS solutions for which there is no current toolset. For example, INL did not find any tools to check programmable logic controller application software for ladder logic bombs; however, existing tools such as YARA with a definition of known bytes in malicious ladder logic could scan for it in logic files. Similarly, intrusion detection system/intrusion prevention system solutions would only require a ruleset to alarm on ICS-specific malicious network traffic. Any new tool development should first evaluate existing tools and tool sets to determine if it could interface with existing tools and broaden their abilities, rather than create another independent tool.

The research team did not test the tools identified for suitability, nor did they verify vendors' claims about tool abilities and functions. A follow-on phase would allow deeper investigation into the tools and evaluation of the claims made by tool vendors, as well as investigation into the learning curves and usability of the tools.

# CONTENTS

# ACRONYMS

| | |
|---|---|
| BOM | bill of materials |
| CERT | computer emergency response team |
| CVE | common vulnerabilities and exposures |
| GPL | general public license |
| GUI | graphical user interface |
| HIDS | host-based intrusion detection system |
| HMI | human machine interface |
| ICS | industrial control system |
| IDS | intrusion detection system |
| IED | intelligent electronic device |
| INL | Idaho National Laboratory |
| I/O | input/output |
| IOC | indicator of compromise |
| IP | internet protocol |
| IPS | intrusion prevention system |
| IT | information technology |
| LAN | local area network |
| LR | log review |
| NIDS | network-based intrusion detection system |
| NSM | network security monitoring |
| NTAD | network traffic anomaly detection |
| OA | outlier analysis |
| OT | operational technology |
| OS | operating system |
| OSI | open system interconnection |
| PLC | programmable logic controller |
| RE | reverse engineering |
| RTU | remote terminal unit |
| SAR | system artifact review |
| SCADA | supervisory control and data acquisition |
| SIEM | security information and event management |
| SME | subject matter expert |

# A Survey of Security Tools for the Industrial Control System Environment

## 1. Introduction

### 1.1 Purpose

This survey was conducted to provide a glimpse into the current state of security tools available for industrial control system (ICS) applications, and to shed light on areas lacking tools to handle anomalies and malware remediation. This survey offers readers an idea of currently available tools and tool inabilities to detect malware or malicious anomalies. The survey includes a list of open source or licensable tools that could be extended upon to meet security needs; a gap analysis highlighting ICS environments that lack tools to fulfill specific security purposes; and desired attributes of future technologies to fill these gaps.

The purpose of this survey is to:

- Assess the currently available solutions to prevent, detect, mitigate, or investigate an existing or future attack in an ICS environment;
- Investigate any overlap of solutions between the enterprise, control center, local human machine interface (HMI), and field input/output (I/O) device zones;
- Provide the reader with a list of current tools and their areas of coverage, as well as a brief overview of what each tool does and how it applies; and
- Conduct a gap analysis to show where tools are lacking ICS-centric features.

### 1.2 Scope

The intention of this paper is not only to serve as a survey of current security solutions for an ICS environment, but also to investigate the availability of tools in this area so the reader understands which areas are already covered by available tools. This survey was conducted under the assumption that enterprise zone security solutions are readily available and well supported. Under this assumption, this survey did not pursue tools that were specifically for the enterprise zone. Instead, the focus of this paper is to explore tools available for ICS device security, as well as identify areas that the application of current tools could benefit the state of ICS security. Using the diagram of a notional ICS architecture in Figure 1 below, Idaho National Laboratory (INL) researched tools which might apply within the Control Center/Processing Local Area Network (LAN), the Local HMI LAN, and the Controller LAN/Field I/O Devices (i.e., the industrial network where field devices and their supporting peripherals abide).

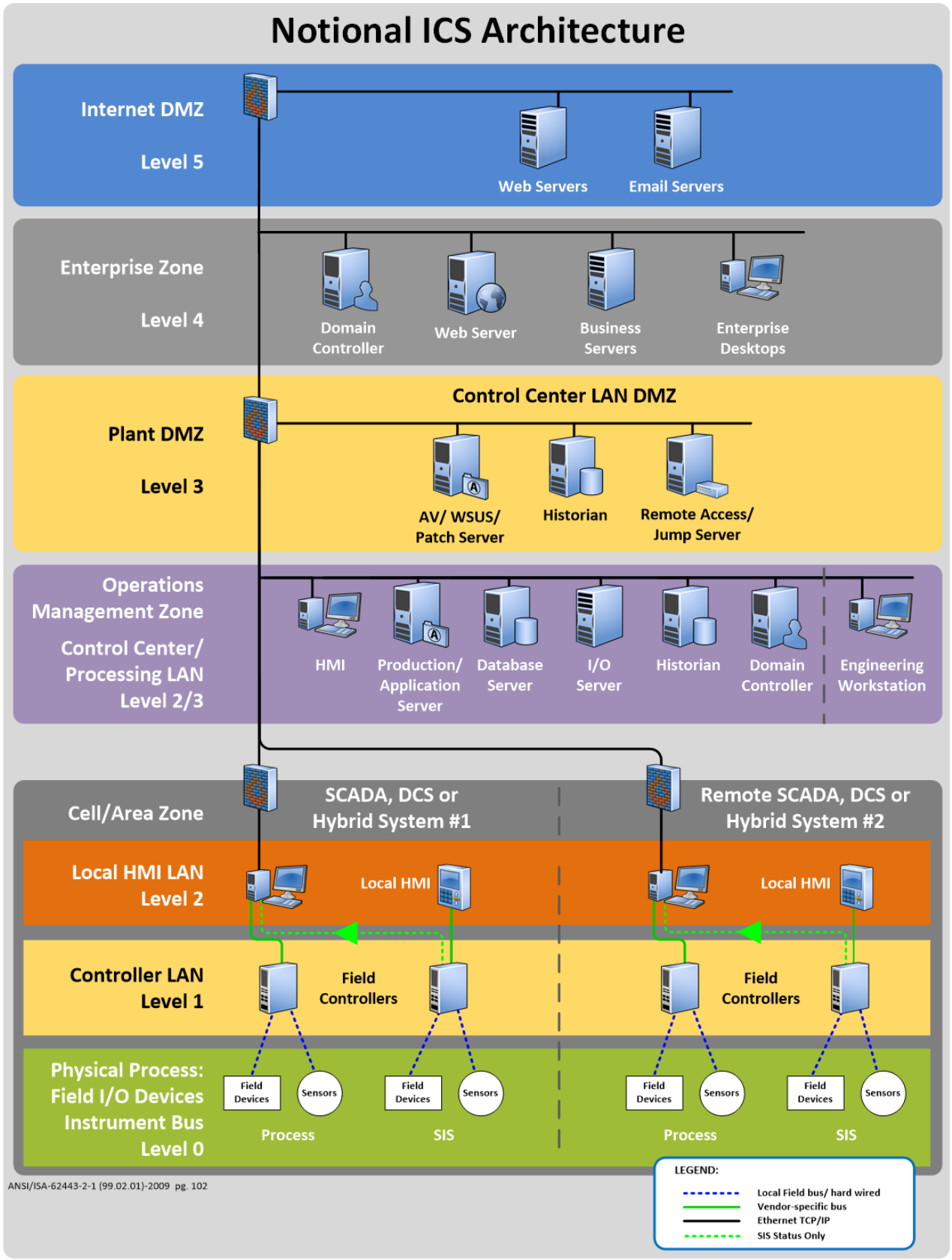


**Figure 1: Notional ICS Architecture**

The survey focused on security-related tools specific to an ICS environment; therefore the survey did not focus on vendor-specific software unless it had security functionality. There are many different ICS vendors, each with its own configuration software to validate the ICS device configuration and retrieve log files. These operations are sometimes the only way to validate and investigate the field devices themselves. Unfortunately most vendor software does not implement more advanced security operations such as anomaly detection or outlier analysis; this leaves room for additional tools to be utilized to improve security. Although these tools would be useful to include in a computer emergency response team (CERT) toolbox, listing every vendor-specific historian or device programming software would overwhelm the survey with potentially unhelpful tools and is beyond the scope of the survey.

During the research for the survey, INL encountered several tools that should be included in a CERT toolbox but do not meet the criteria for the survey. INL labeled these tools "tool enablers" because they are a device, software, or resource that would enable a tool to perform its function but do not fulfill the security functions themselves. For example, hardware to read the JTAG bus should be part of a CERT toolbox; however, listing every JTAG reader is outside of the scope of this paper. Selected tool enablers are listed and described in Appendix B.

During the survey, no attempt was made to confirm the claims made by tool vendors or to assess the maturity or market penetration of the tools in the survey. As such, the reader should be aware that some of the tools in the survey may not perform as described by the vendor or may have other unforeseen obstacles, such as a high learning curve or limited applicability to the readers specific areas of concern. Also the reader should be aware that several tools were found with blanketing terminology to describe their feature sets; given the lack of specification the burden is left to the reader to investigate further into nebulous claims made by vendors.

## 2. Attributes

Building upon the notional ICS architecture, INL categorized the tools surveyed with respect to their performance within an ICS zone(s), their intended purpose, transport, and availability. The definitions for each are below.

**ICS Zone:** The zone in the ICS environment affected by the tool.

- **Enterprise** – The information technology (IT) portion of the network used for billing and business operations.
- **Control Center/Processing LAN** – A local segregated network used to support and collect data for supervisory control and data acquisition (SCADA), billing, log gathering, etc.
- **Local HMI LAN** – Computers and kiosks in remote substations or buildings that provide onsite feedback and allow for local troubleshooting.
- **Controller LAN/Field I/O Devices** – Embedded device(s) field exposed to the elements in remote locations used for switching and raw data gathering.

**Purpose:** The main function of the tool from a security perspective.

- **Indicator of Compromise (IOC) Detection** – An IOC is a forensic artifact, observed on the network or host, that with a high confidence indicates a computer intrusion. IOCs are observable, which link them directly to measurable events. Some IOC examples include: hashes of known

malware, signatures of malicious network traffic, URLs or domains that are known malware distributors, and registry keys created after compromise. A successful tool should be able to detect all malicious data that is bounded by the provided rule set.

- **Network Traffic Anomaly Detection** – Network traffic anomaly detection is based on the statistical properties of the network upon which the tool is deployed. These properties can include, but are not limited to IP address, port, frequency of communication, content of packet, etc. Anomaly detection differs from IOC detection by not requiring updates when new threats are detected. A new threat should, by definition, be an anomaly on the network or a false positive. A successful tool should be able to be trained on a network for "normal" traffic, and then deployed with the associated machine learning model to determine anomalous traffic.

- **Outlier Analysis** – Outlier analysis is the ability to analyze anomalous data for future threat intelligence. This data is usually identified by searching for anomalies across many hosts that share common configurations. A successful tool will be able to scale to handle large datasets and aid the analyst in recognizing meaningful differences.

- **Log Review** – Log review is the process of analyzing computer-generated records that typically include a temporal reference. Difficulties of log analysis include the removal of uninteresting data while maintaining the integrity of the log file. A successful tool may implement anomaly analysis within the logs to quickly generate areas of interest in a log file, or may be able to correlate different logs into a timeline of event activity.

- **System Artifact Review** – System artifact review is the process of analyzing system artifacts that are created as a byproduct of execution. These could include registry files, data files, memory-resident information, environment variables, and many others. A successful tool would be able to quickly extract all possibly useful information from a system and save it for future analysis.

- **Reverse Engineering (RE) Analysis** – RE analysis is the process of extracting information from a given set of data. This most often refers to files and/or firmware of a device, but can be extended to network traffic as well. A successful tool would be able to disassemble multiple architectures, as well as display the information in a way that is easy to understand and facilitates the fastest possible RE process.

**Transport:** The medium by which the tool interfaces with electronic signals.

- **File** – The tool works with files from the system or on the system itself.
- **Ethernet** – This includes all layers of the seven-layer Open System Interconnection (OSI) model and any specific ICS protocols that implement data transfer on top of the Ethernet layer.
- **Backplane** – Messaging bus used by ICS control devices to communicate with I/O modules or through a communication module to an HMI. Each manufacturer typically has its own proprietary backplane communications protocol.
- **Web** – The tool exists on the cloud or interfaces mainly through Web traffic with a remote server.
- **USB** – The tool addresses data transferred across the universal serial bus.

**Availability:** The mechanism by which to procure the product.

- **Commercial** – The tool is available for purchase from a manufacturer/vendor.
- **Open Source** – The tool is available free via open source outlets (e.g., Github).
- **Non-commercial Intellectual Property** – Originally developed by a university, research facility, or national laboratory, the tool is now available for purchase, licensing, or via open source markets.

# 3. Currently Available Technologies

INL conducted an survey of tools designed for security of the ICS environment. Open source research coupled with subject matter expert (SME) consultation formed the basis of INL's findings. Table 1 provides a quick-reference snapshot of the tools and their capabilities as mapped to their purpose and ICS zone; the table also denotes transport and acquisition.

**Table 1 – Available Technologies as Applicable to ICS Zones**.

| | Enterprise | | | | | | Control Center | | | | | | Local HMI LAN | | | | | | Field I/O Devices | | | | | | Transport | | | | | Acquisition | | | Coverage | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IOC Detection | NTAD | Outlier Analysis | Log Review | SAR | RE Analysis | IOC Detection | NTAD | Outlier Analysis | Log Review | SAR | RE Analysis | IOC Detection | NTAD | Outlier Analysis | Log Review | SAR | RE Analysis | IOC Detection | NTAD | Outlier Analysis | Log Review | SAR | RE Analysis | Ethernet | File | Web | Backplane | USB | Commercial | Open | University | Enterprise | Control Center | HMI | Field |
| | 10 | 11 | 4 | 8 | 10 | 10 | 15 | 18 | 8 | 9 | 13 | 10 | 13 | 27 | 9 | 9 | 14 | 11 | 10 | 23 | 9 | 3 | 5 | 4 | 36 | 29 | 0 | 1 | 1 | 29 | 14 | 5 | 36 | 44 | 52 | 30 |
| ABB Cyber Security Benchmark | | | | | | | ■ | | | | | | ■ | | | | | | ■ | | | | | | ■ | ■ | | | | | | | | | | |
| AlienVault Unified Security Management SIEM | ■ | ■ | ■ | ■ | | | ■ | ■ | ■ | ■ | | | ■ | | | | | | ■ | | | | | | ■ | ■ | | | | | | | | ■ | | |
| Binary Ninja | | | | | | ■ | | | | | | ■ | | | | | | ■ | | | | | | | ■ | | | | | ■ | | | ■ | ■ | ■ | |
| Binwalk | | | | | | ■ | | | | | | ■ | | | | | | ■ | | | | | | ■ | ■ | ■ | | | | | ■ | | ■ | ■ | ■ | ■ |
| Bro | | ■ | | | | | | ■ | | | | | | ■ | | | | | | | | | | | ■ | | | | | | ■ | | | ■ | ■ | |
| Centrifuge | | | | | | | | | | | | | | | | | | ■ | | | | | | ■ | ■ | ■ | | | | | | | | ■ | ■ |
| CheckPoint Software - SandBlast | ■ | ■ | | | | | | | | | | | | | | | | | | | | | | | ■ | | | | | ■ | | | ■ | | | |
| CHIPSEC | | | | | ■ | | | | | | ■ | | | | | | ■ | | | | | | | | ■ | | | | | | ■ | | | ■ | ■ | |
| Claroty | | | | | | | | ■ | ■ | | | | | ■ | ■ | | | | | ■ | ■ | | | | ■ | | | | | ■ | | | | ■ | ■ | ■ |
| CodeDNA | | | | | ■ | | | | | | ■ | | | | | | ■ | | | | | | | | ■ | | | | | | | | ■ | ■ | ■ | |
| ConPot | | | | | | | | | | | | | | ■ | | | | | | ■ | | | | | ■ | | | | | | ■ | | | | ■ | ■ |
| CyberX XSense | | | | | | | | ■ | | | | | | ■ | | | | | | ■ | | | | | ■ | | | | | ■ | | | ■ | ■ | ■ | ■ |
| DarkTrace ICS | | ■ | ■ | | | | | ■ | ■ | | | | | ■ | ■ | | | | | ■ | ■ | | | | ■ | | | | | ■ | | | ■ | ■ | ■ |
| Digital Ants | | | | | ■ | | | | | | ■ | | | | | | ■ | | | | | | | | ■ | | | | | | | ■ | ■ | ■ | ■ | |
| Dragos | | | | | | | ■ | ■ | | | | | ■ | ■ | ■ | | | | ■ | ■ | ■ | | | | ■ | | | | | ■ | | | ■ | ■ | ■ | ■ |
| Elastic Stack | | | | ■ | | | | | | ■ | | | | | | ■ | | | | | | | | | ■ | ■ | | | | | | | ■ | ■ | ■ | |
| fcd | | | | | | ■ | | | | | | ■ | | | | | | ■ | | | | | | | ■ | ■ | | | | | ■ | | | ■ | ■ | ■ | |
| FireEye IOC Editor | ■ | | | | | | ■ | | | | | | | | | | | | | | | | | | ■ | ■ | | | | ■ | | | ■ | ■ | | |
| FireEye IOC Finder | ■ | | | | | | ■ | | | | | | | | | | | | | | | | | | ■ | ■ | | | | ■ | | | ■ | ■ | | |
| Fortinet-Nozomi Networks | | | | | | | | | | | | | | ■ | | | | | | ■ | | | | | ■ | | | | | ■ | | | ■ | ■ | ■ | ■ |
| Graylog | | | | ■ | | | | | | ■ | | | | | | ■ | | | | | | | | | ■ | ■ | | | | | | | ■ | ■ | ■ | |
| GridPot | | | | | | | | | | | | | | ■ | | | | | | ■ | | | | | ■ | | | | | | ■ | | | | ■ | ■ |
| Hex-Rays IDA Pro | | | | | | ■ | | | | | | ■ | | | | | | ■ | | | | | | ■ | ■ | ■ | | | | | | | ■ | ■ | ■ | ■ |
| Hopper Disassembler | | | | | | ■ | | | | | | ■ | | | | | | ■ | | | | | | ■ | ■ | ■ | | | | | | | ■ | ■ | ■ | ■ |
| Hyperion | | | | | | ■ | | | | | ■ | ■ | | | | | ■ | ■ | | | | | | | ■ | ■ | | | | | | ■ | ■ | ■ | ■ | |
| Indegy Platform | | | | | | | | | | | | | | ■ | ■ | ■ | ■ | | | ■ | ■ | ■ | ■ | | ■ | ■ | | | | ■ | | | | | ■ | ■ |
| MB Connect Line mbSECBOX | | | | | | | | | | | | | | ■ | | | | | | ■ | | | | | ■ | ■ | | | | ■ | | | | | ■ | ■ |
| McAfee | ■ | ■ | ■ | ■ | | | ■ | ■ | ■ | ■ | | | ■ | ■ | ■ | | | | ■ | ■ | ■ | ■ | | | ■ | ■ | | | | | | | ■ | ■ | ■ | ■ |
| MSi Sentinel and MSi 1 | | | | | | | ■ | ■ | | | | | ■ | ■ | ■ | | | | ■ | ■ | ■ | | | | ■ | | | | | ■ | | | | ■ | ■ | ■ |
| N-Dimension Solutions n-Platform 340S or 440D | | | | | | | | ■ | | | | | | ■ | | | | | | ■ | | | | | ■ | | | | | ■ | | | | ■ | ■ | ■ |
| Nessus | ■ | | | | ■ | | ■ | | | | ■ | | ■ | | | | ■ | | | | | | | | ■ | | | | | ■ | | | ■ | ■ | ■ | |
| Nextnine ICS Shield | | | | | | | ■ | ■ | ■ | ■ | ■ | | ■ | ■ | ■ | ■ | ■ | | ■ | ■ | ■ | ■ | ■ | | ■ | | | | | ■ | | | | ■ | ■ | ■ |
| OSSEC | | ■ | | ■ | ■ | | | ■ | | ■ | ■ | | | ■ | | ■ | ■ | | | | | | | | ■ | ■ | | | | | | | ■ | ■ | ■ | |
| Plaso - Log2timeline | | | | ■ | | | | | | ■ | | | | | | ■ | | | | | | | | | ■ | ■ | | | | ■ | | | ■ | ■ | ■ | |
| Protecode | | | | | | ■ | | | | | | ■ | | | | | | ■ | | | | | | | ■ | ■ | | | | | | | ■ | ■ | ■ | |
| Radare | | | | | | ■ | | | | | | ■ | | | | | | ■ | | | | | | ■ | ■ | ■ | | | | | ■ | | | ■ | ■ | ■ |
| Radiflow | | | | | | | | | | | | | ■ | ■ | ■ | | | | ■ | ■ | ■ | | | | ■ | ■ | | | | ■ | | | | ■ | ■ | ■ |
| Security Onion | | ■ | | | | | | ■ | | | | | | ■ | | | | | | ■ | | | | | ■ | | | | | ■ | | | | ■ | ■ | ■ |
| SecurityMatters SilentDefense | | | | | | | ■ | ■ | | | | | ■ | ■ | | | | | ■ | ■ | | | | | ■ | | | | | ■ | | | | ■ | ■ | ■ |
| Senami IDS | | | | | | | | | | | | | | ■ | | | | | | ■ | | | | | ■ | | | | | | ■ | | | | ■ | ■ |
| Snort | ■ | ■ | | | | | ■ | ■ | | | | | ■ | ■ | | | | | | | | | | | ■ | | | | | | | | ■ | ■ | ■ | |
| Snowman | | | | | | ■ | | | | | | ■ | | | | | | ■ | | | | | | | ■ | ■ | | | | | ■ | | | ■ | ■ | |
| Splunk | | | ■ | ■ | | | | ■ | ■ | ■ | | | | | ■ | ■ | | | | | | | | | ■ | ■ | | | | | ■ | | | ■ | ■ | |
| Suricata | | ■ | | | | | | ■ | | | | | | ■ | | | | | | | | | | | ■ | | | | | | ■ | | | ■ | ■ | |
| Symantec Anomaly Detection for ICS | | | | | | | | ■ | | | | | | ■ | | | | | | ■ | | | | | ■ | | | | | ■ | | | | ■ | ■ |
| Symantec Embedded Security: CSP | ■ | ■ | | | ■ | | ■ | ■ | | | ■ | | ■ | ■ | | | ■ | | ■ | ■ | | | ■ | | ■ | | | | | ■ | | | ■ | ■ | ■ |
| Tofino Xenon Security Appliance (Tofino SA) | | | | | | | | | | | | | | ■ | | | | | | ■ | | | | | ■ | | | | | ■ | | | | ■ | ■ |
| T-Pot | | ■ | | | | | | ■ | | | | | | ■ | | | | | | ■ | | | | | ■ | | | | | | ■ | | | ■ | ■ |
| Tripwire | ■ | | | | ■ | | ■ | | | | ■ | | ■ | | | | ■ | | | | | | | | ■ | | | | | ■ | | | ■ | ■ | ■ | |
| TruffleHog | | | | | | | | | | | | | | ■ | | | | | | ■ | | | | | ■ | | | | | | ■ | | | | ■ | ■ |
| USB-ARM | | | | | ■ | | | | | | ■ | | | | | | ■ | | | | | | | | ■ | | | | ■ | | | ■ | ■ | ■ | |
| Verve Security Center | | | | | | | ■ | ■ | | | ■ | | ■ | ■ | | | ■ | | ■ | ■ | | | ■ | | ■ | | | | | ■ | | | | ■ | ■ | ■ |
| Volatility Framework | | | | | ■ | | | | | | ■ | | | | | | ■ | | | | | | | | ■ | ■ | | | | ■ | ■ | | | ■ | ■ | |
| Waterfall BlackBox | | | | ■ | | | | | | ■ | | | | | | ■ | | | | | | | | | ■ | | | | | ■ | | | ■ | ■ | ■ | |
| WeaselBoard | | | | | | | | | | | | | | | | | | | | | ■ | | | | ■ | | | ■ | | ■ | | ■ | | | | ■ |
| X64dbg | | | | | | ■ | | | | | | ■ | | | | | | ■ | | | | | | | ■ | | | | | | ■ | | | ■ | ■ | |
| YARA | ■ | | | | ■ | | ■ | | | | ■ | | ■ | | | | ■ | | ■ | | | | ■ | | ■ | | | | | | ■ | | | ■ | ■ | ■ |

As noted in Section 1.2, INL primarily focused on security tools for the ICS environment and did not research tools for the Enterprise Zone. For correlation to the ICS notional architecture, INL included tools collectively applicable to the Enterprise Zone and the various ICS zones.

Expanded summaries of the tools uncovered during the project are located in Appendix A. Highlights of the tools' features/functionality are provided below.

## 3.1 Multi-Purpose Tools

**AlienVault® Unified Security Management™ (USM™) SIEM –** AlienVault USM combines powerful Security Information and Event Management (SIEM) and log management capabilities with security tools, such as asset discovery, vulnerability assessment, and intrusion detection, to provide users with centralized security monitoring of cloud, hybrid cloud, and on-premises environments.

**CheckPoint Software - SandBlast** – SandBlast is a software application that is installed on enterprise-level gateways. It has several different software blades to thwart infection and propagation of malware. Files traveling across the network are scanned and removed if they are flagged as dangerous. The software blades run on SandBlast's hardware appliance.

**Claroty** – A passive monitoring system, Claroty monitors all network communication to find hidden issues and to establish a high-fidelity baseline model so that it can detect anomalous behavior. It combines native operational technology (OT) knowledge with advanced models and algorithms to generate detailed alerts, complete with actionable insights, for both cyber security and process integrity issues.

**Dragos** – Dragos Industrial Cybersecurity Ecosystem combines an on-premise platform, threat operations service, and global threat intelligence. The platform compiles and correlates suspicious events at scale and speed. The suite offers asset discovery and compromise assessment; threat hunting and detection; and forensics, automated workflows, and incident response.

**Indegy Platform** – A deep packet inspection engine, specifically designed for industrial control systems, the Indegy platform provides passively monitors standard operational communication protocols (like Modbus & DNP3) and provides in-depth, real-time visibility into all activities performed over the operational network. It captures all changes to programmable logic controllers (PLCs) and remote terminal units (RTUs), whether performed over the network or directly on the physical devices. The Indegy Platform conducts periodic verification of controller device firmware, application, and configuration to provide visibility with details for each controller.

**McAfee** – McAfee offers a suite of security products geared towards the critical infrastructure sector categorized into four areas: database and endpoint security; data protection; network security; and SIEM. Together, the tools enable discovery, prevention, detection, response, audit, and management across data, the network, and endpoints within enterprise IT, SCADA, and ICS zones.

**Nessus (N) ™ –** Nessus is a proprietary vulnerability scanner developed by Tenable Network Security. It is free of charge for personal use in a non-enterprise environment. Offered as Nessus Professional (NP)™ or Nessus Manager (NM)™, the tool protects IT environments by running vulnerability scans, configuration and compliance checks, malware detection, Web application scanning; includes assessment capabilities, agent-less and agent-based scanning; and runs reports and filters data.

**Nextnine's ICS Shield** – A top-down OT security management solution for securing connected ICS/SCADA environments, ICS Shield secures remote field assets from a single operations center. It automates the deployment and enforcement of plant-wide security policies while focusing on security essentials such as inventory visibility, patching, log collection, incident alarm and response, and compliance reporting.

**SecurityMatters SilentDefense** – SilentDefense's Industrial Threat Library includes a wide variety of industry-specific threats, enabling users to identify rogue and malfunctioning devices, intrusions and attacks, and detect undesired configuration changes. Users can define custom checks for their industrial environment; the SilentDefense can be integrated with Splunk, ABB, Siemens, Rockwell, Schneider, Honeywell, Emerson, and Yokogawa systems.

**Symantec Embedded Security: Critical System Protection** – Symantec Embedded Security: Critical System Protection provides a host firewall, device and configuration control, file integrity monitoring, intrusion detection, operating system (OS) hardening, application whitelisting, and automatic sandboxing. Designed to run on devices such as ICS, it has been optimized for embedded OS, including: Microsoft® Windows Embedded Family (multiple versions), and QNX® Real-Time Operating System, as well as non-embedded systems, including Linux, Microsoft® Windows (multiple versions), and Microsoft® Windows Server Family (multiple versions).

**Tripwire®** – The Tripwire Configuration Compliance Manager (CCM) utilizes active and passive scanning to discover and audit configurations. Users receive detailed information on the configurations of systems, applications, firewalls, routers, and switches. The agentless architecture requires no software installation on the monitored endpoints, and automates continuous configuration and compliance assessment.

**Verve Security Center** – This security suite includes vulnerability scans, patching, backup management, application whitelisting, antivirus, change management, SIEM, and compliance tools. It is marketed to be vendor agnostic, simple to use, and non-disruptive to communications. Verve Security Center monitors and remediates security and compliance from one console, and protects ICS devices including relays, intelligent electronic devices (IEDs), PLCs, etc.

## 3.2 IOC Detection Tools

**ABB Cyber Security Benchmark** – Cyber Security Benchmark utilizes ABB's proprietary tool collection to automatically and non-invasively gather data. It conducts proactive analysis of Key Performance Indicators to detect possible security weaknesses and features a Web-based "stoplight" report that provides an easy-to-read overview of security status immediately available after data collection.

**FireEye IOC Editor** – The IOC Editor provides an interface for managing data and manipulating the logical structures of IOCs. IOCs are XML documents that help incident responders capture diverse information about threats, including attributes of malicious files, characteristics of registry changes and artifacts in memory. The IOC Editor includes manipulation of the logical structures that define the IOC; application of meta-information to IOCs, including detailed descriptions or arbitrary labels and conversion of IOCs into XPath filters.

**FireEye IOC Finder** – The IOC Finder collects host system data and reports the presence of IOCs. The IOC Finder features collection of full data, sufficient for general IOC matching requirements; usage of a portable storage device for collection from multiple hosts; IOC hit reporting in simple text, full HTML and full MS Word XML formats; and generation of reports for specific hosts or all hosts.

**Radiflow** – Radiflow's ICS Security Checkup detects all known threats and vulnerabilities, including SCADA-specific threats, such as Black Energy malware and malware spreading across PLCs Logical changes in PLCs Open remote SSH sessions.

## 3.3 Network Traffic Anomaly Detection Tools

**Bro** – Bro is an open source intrusion detection system (IDS) that runs on standard hardware with a Linux-based OS. It is a Network IDS (NIDS) that specializes in traffic analysis. Bro keeps comprehensive logs and offers a range of analysis and detection techniques, including signature-based and anomaly detection. Bro's signature engine is not based on Snort, but is capable of detail-oriented matching like Snort. There is an effort to convert Snort signatures to Bro signatures. Bro supports port-independent analysis of application-layer protocols, including DNP3 and Modbus, and file content analysis.

**Conpot** – Conpot is an ICS honeypot with the goal to collect intelligence about the motives and methods of adversaries targeting ICS. This dockerized ICS-specific honeypot includes Modbus, s7, http, snmp, bacnet, snmp, and Ipmi protocols. Conpot has built-in support for HPFeeds, a generic data sharing protocol used by the Honeynet Project.

**CyberX XSense** – XSense continuously monitors networks for OT threats and vulnerabilities, such as unauthorized remote connections and unpatched or unknown devices. It provides both alerts and actionable intelligence with recommended mitigations.

**Darktrace ICS** – Darktrace analyzes raw network data and leverages machine learning algorithms to form an evolving understanding of an organization's 'pattern of life' (or 'self'), spotting very subtle changes in behaviors, as they occur. These behavioral changes are correlated and filtered to detect emerging threats and anomalies. Delivered as a physical appliance, installed at a SPAN or TAP port within the customer network(s), Darktrace passively monitors raw network data in real time, without disrupting business operations, and provides instant visibility into all network activity, notifying of in-progress attacks or emerging anomalies.

**Fortinet-Nozomi Networks** – This joint solution combines Nozomi Networks' SCADAguardian with Fortinet's FortiGate. Placed onto the OT network, SCADAguardian passively monitors network traffic creating an internal representation of the entire network, its nodes, and the state and behavior of each device in the network. Using predefined and continually updated signatures, the FortiGate can identify and police most of the common ICS/SCADA protocols to define conduits. This is done through the configuration of security policies in which multiple services, such as intrusion prevention system (IPS), antivirus, and application control can be mapped to each protocol.

**GridPot** – GridPot is a Symbolic Cyber-Physical Honeynet Framework. Its symbolic simulation of cyber-physical systems emulates SCADA/HMI and ICS protocols. GridPot uses ETSY's skyline project for anomaly detection and shows real-time attacks.

**MB Connect Line mbSECBOX** – The mbSECBOX PLC security solution detects malware similar to STUXNET and other possible threats on the S7 Controllers. After a threat is found, the mbSECBOX PLC malware detector immediately alerts the operator before any damage occurs.

**MSi Sentinel and MSi 1** – Together, MSi Sentinel and MSi 1 conduct continual, multi-layered system monitoring at the IP level and digital and analog signals. The tools provide real-time analysis and automated incident detection, and allow users to remotely restore control devices to a "known good" state.

**N-Dimension Solutions n-Platform 340S or 440D** – The n-Platform software features two modes – surveillance and gateway. The surveillance mode features include the following SCADA IDS, vulnerability scan, port scan, availability monitor, and performance monitor. The Gateway mode features routing, firewall, antivirus, proxy filter, network device control, virtual private network, and ldap.

**OSSEC** – OSSEC features include HIDS, log monitoring, signature analysis (based on a Snort2 engine), anomaly detection, file integrity checking capabilities, and central logging service. It contains a central management server and agent based on agentless monitoring of systems. OSSEC runs on standard hardware with a Linux-based OS.

**Security Onion** – This is a network security monitoring (NSM) open source suite of tools, which is a compilation of all the open source solutions previously mentioned. It includes a NIDS, a HIDS, a full packet capture, and analysis tools. Security Onion includes Suricata or Snort, Bro, OSSEC, Sguil (management console), SQUERT (Web application interface to the database), Snorbyg (Web application interface), ELSA (an enterprise log search and archive tool), and many other tools. It is typically deployed as a client-server model, but it can be standalone.

**Senami IDS** – SENAMI is a bespoke IDS for Siemens S7 ICS environments. SENAMI combines traditional NIDS methodologies with "active" intrusion detection, which requests values directly from the PLC to monitor; it introduces the concept of "selective, non-invasive active monitoring" to avoid overloading legacy ICS devices. Combining passive IDS with an active IDS, Senami generates alerts, reported live in the IDS terminal, and saves them to a logfile for further analysis with the SIEM. SENAMI should work in all Siemens S7 environments that have their PLC memory configuration set up as above - a standard way amongst many ICS vendors.

**Snort** – Snort is an open source network IDS/IPS. Best known for its signatures and signature engine, it also performs protocol analysis, content searching/analysis, and anomaly detection. Signatures are available for free or by a paid subscription, the difference being how recent the signatures are. Support for this software is available through various means including mailing lists, blogs, webcasts, email, and paid subscriptions. Snort was purchased by Cisco and is used in its products; however, it is continuing to support the open source model. Use of Snort for commercial purposes requires a license agreement with Cisco.

**Suricata** – Suricata is an open source next generation intrusion detection and prevention engine. It is designed to work with Snort signatures, but Suricata-optimized rules are available from Emerging Threats. Suricata features includes multithreading (provides speed), protocol detection, gzip decompression, flow analysis, IP reputation, log analysis, GeoIP, and anomaly detection. It runs on standard hardware with a Linux-based OS. Typically, Suricata or Snort, one or the other, is used, not both.

**Symantec Anomaly Detection for Industrial Control Systems** – Anomoly Detection for ICS provides visibility into ICS devices and their communications, and performs deep packet inspection of all ICS protocols. Its advanced machine learning algorithms analyze small behavior variations to catch subtle attacks and offers criticality based incident prioritization with forensic data provided for remediation. The on-premise, software solution can use existing hardware without Internet access.

**Tofino Xenon Security Appliance (Tofino SA)** – The Tofino SA provides a simple and cost-effective way to create zones of security − tailored protection for groups of PLCs, DCS, RTUs, IEDs, and HMIs − as recommended by ISA/IEC-62443 Standards. It is a Plug-n-Protect™ product, designed to be installed in a live network with no pre-configuration, no network changes, and no plant downtime.

**T-Pot** – T-Pot combines the dockerized honeypots conpot, cowrie, dionaea, elasticpot, emobility, glastopf, and honeytrap with suricata, a NSM engine and the ELK stack to visualize all events. Events are correlated by T-Pot's data submission tool ewsposter which also supports Honeynet project HPfeeds honeypot data sharing.

**TruffleHog** – Started as a university project at the Karlsruhe Institute of Technology, TruffleHog requires a modified version of Snort including a PROFINET-preprocessor to collect "Truffles" representing a semantic analysis of one PROFINET-network package. It keeps track of all incoming Truffles, uses the semantic information to build a network topology (or rather a network map), and displays it to look at in quasi real time.

## 3.4 Outlier Analysis Tools

**WeaselBoard** – WeaselBoard is a PLC backplane analysis system that connects directly to the PLC backplane; it provides zero-day exploit protection for PLCs. WeaselBoard captures and analyzes backplane traffic among PLC modules, thereby detecting changes to process control settings, sensor values, module configuration information, firmware updates, and process control program (logic) updates.

## 3.5 Log Review Tools

**Elastic Stack** – The stack of tools available from Elastic allows a user to gather data from any source and then search through and filter the data. Then the user can create visualizations of the data to create a command center. This allows the users to see anomalies and issues as they come up, provided the user creates the correct rulesets and is able to retrieve the data they need.

**Graylog** – Graylog is a platform for gathering log data into a centralized management system. It has user access control to fine tune who can attend what, and it has a restful API for extending the platform further. Graylog also has the ability to add alerts via a simple graphical user interface (GUI) interface to create new alert conditions and set callbacks.

**Plaso Log2timeline** – Log2timeline is designed to extract timestamps from various files found on a typical computer system(s) and aggregate them. It creates logs by adding new parsers or parsing plug-ins; adding new analysis plug-ins; and writing one-off scripts to automate repetitive tasks in computer forensic analysis or equivalent.

**Splunk®** – Splunk offers a platform for operational intelligence; it pulls security data from ICS devices (PLC data, HMI and historians, DHCP/DNS, servers, industrial endpoints, etc.) and reviews network protocols, authentication, device behavior, HMI behavior, and operational changes. It offers incident investigations and forensics; security and compliance reporting; real-time monitoring of known threats; monitoring of unknown threats; fraud detection; and insider threat.

**Waterfall BlackBox** – BlackBox is a high-speed, high-capacity logging and analysis system, which can be used to reveal attackers' tracks, detection of attempted changes, manipulation, and abnormal activities. In time of need, data can be retrieved and inspected securely by physical access to the BlackBox appliance.

## 3.6 System Artifact Review Tools

**CHIPSEC** – CHIPSEC is a framework for analyzing the security of PC platforms including hardware, system firmware (BIOS/UEFI), and platform components. Originally developed by Intel to help internal teams find and fix vulnerabilities in platform hardware and software, the now open source tool includes a security test suite, tools for accessing various low level interfaces, and forensic capabilities. It can be run on Windows, Linux, Mac OS X, and UEFI shell.

**CodeDNA** – CodeDNA detects families of attacks and supports a navigable means of exploring attack family development, leading to insights and predictions about what a broad range of future zero-day attacks may look like, so that the defenders can detect them. It generates unique DNA-like fingerprints from incoming files and computes similarity scores across a database of fingerprints to automate the identification of related malware binaries and link variants.

**Digital Ants** – Digital Ants uses dynamic, decentralized mechanisms inspired by nature to provide mobile, resilient cybersecurity for protecting large enterprise IT networks and critical infrastructures. Individual ant-like sensor programs swarm to the location of anomalies and enable human operators to focus on areas and issues of concern.

**USB-ARM** – USB-ARM provides a simple, efficient, and customizable layer of security that brokers all communication between removable media and the OS. USB-ARM guarantees that a set of user-defined criteria are met prior to allowing access to the removable media.

**Volatility Framework** – The Volatility Framework is a completely open collection of tools, implemented in Python under the GNU General Public License (GPL), for the extraction of digital artifacts from volatile memory (RAM) samples. The extraction techniques are performed completely independent of the system being investigated but offer visibility into the runtime state of the system.

**YARA** – YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. YARA users can create descriptions of malware families (or others) based on textual or binary patterns. Each description, a.k.a. rule, consists of a set of strings and a boolean expression which determine its logic.

## 3.7 Reverse Engineering Analysis Tools

**Binary Ninja** – Binary Ninja is a reverse engineering platform. It focuses on a clean and easy to use interface with a multithreaded analysis built on a custom intermediate language to quickly adapt to a variety of architectures, platforms, and compilers.

**Binwalk** – Binwalk is a tool for analyzing, reverse engineering, and extracting firmware images. It can be used to quickly find offsets to filesystem sections in a binary image, extract files from within the image and perform entropy analysis on images.

**Centrifuge** – Centrifuge takes binary files containing firmware images and performs full evaluations to detect CVE using its cloud based service. The cloud based service will also point out any vulnerable code so you can remediate the risk if you have access to the source code. The service provides easy to read reports per file.

**fcd** – fcd is a burgeoning LLVM-based native program decompiler. Most of the code is licensed under the GNU GPLv3 license, though some parts, such as the executable parsing code, are licensed under a less restrictive scheme. Currently, fcd works best with executables that follow the x86_64 System V ABI. fcd

supports ELF executables out-of-the-box, but also ships with Python scripts that can be used as plug-ins to parse Mach-O and PE executables.

**Hex-Rays IDA Pro** – IDA (Interactive DisAssembler) is written entirely in C++ and runs on the three major OS: Microsoft Windows, Mac OS X, and Linux. IDA also serves as the foundation on which the Hex-Rays Decompiler is built. The Hex-Rays facilitates binary software analysis by converting executable programs into a readable C-like pseudocode text.

**Hopper Disassembler** – The Hopper Disassembler is a RE tool designed for Mac OS and Linux that allows users to disassemble, decompile, and debug applications. Hopper analyzes function's prologues to extract procedural information such as basic blocks and local variables. The Mac OS version makes full use of the Cocoa framework, and the Linux version makes use of Qt 5. Most of the Hopper features can be invoked from Python scripts; it can use LLDB or GDB to debug and analyze the binary dynamically (Intel CPU only).

**Hyperion** – Hyperion is a cyber security technology designed to "look inside" an executable program and determine software's function or "behavior" without the use of the software's source code. It generates associated program behaviors and the complete set of conditions under which they occur; these behaviors can be automatically checked for known malicious signatures and inspected by domain experts to assure correct operation and the absence of malicious content.

**Radare** – Radare is a portable reversing framework that can: disassemble (and assemble for) many different architectures; debug with local native and remote debuggers; run on Linux, *BSD, Windows, OSX, Android, iOS, Solaris, and Haiku; perform forensics on filesystems and data carving; support collaborative analysis using the embedded webserver, visualize data structures of several file types; and patch programs to uncover new features or fix vulnerabilities.

**Snowman** – Snowman is a native code to C/C++ decompile that supports ARM, x86, and x86-64 architectures. It reconstructs functions; their names and arguments; local and global variables; expressions; integer, pointer, and structural types; and all types of control-flow structures, including switch. The GUI allows one-click navigation between the assembler code and the reconstructed program. It includes a command-line interface for batch processing and offers an IDA Plug-in.

**Synopsys Protecode** – Protecode is now owned by Synopsys. Protecode creates a BOM of all of the shared libraries used in application code and provides a list of known vulnerabilities. Synopsys also has tools to scan for new vulnerabilities in code and provides developers with a way to make more robust code.

**X64dbg** – Using a single interface, X64dbg can debug both x64 and x32 applications. Built on open-source libraries (Qt, TitanEngine, capstone, Yara, Scylla, Jansson, Iz4, XEDParse, Keystone, asmjit, and Snowman), X64dbg is customizable and extendable and offers executable patching and analysis.

# 4. Gap Analysis

Upon conclusion of the survey and analysis of the results, INL conducted a quantitative analysis (depicted in Figure 2) of the number of tools found per zone by purpose to determine additional gaps in availability. The findings are presented below. The graph shows a lack of tools for log review, RE, and outlier analysis within the Controller LAN/Field I/O Devices Zone, as well as a lack of tools for outlier analysis for the Control Center/Processing LAN and Local HMI LAN Zones.

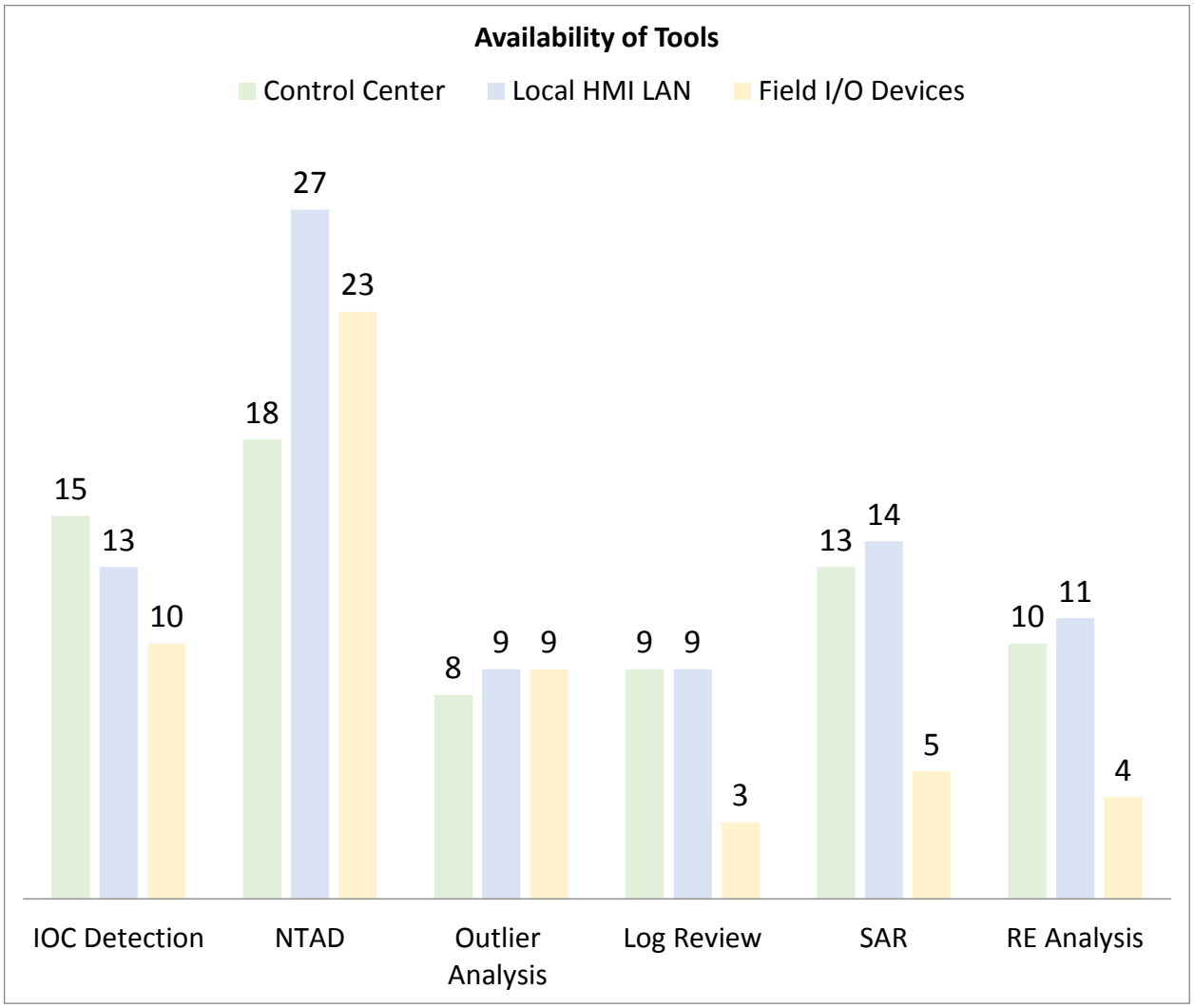


**Figure 2: Quantitative Analysis of Identified Tools by ICS Zone and Purpose (Excluding Enterprise)**

## 4.1 ICS Security Tool Gaps

As noted in Section 1.2, INL considered the Enterprise Zone to be well covered for the purpose of this survey. In line with the outlined scope parameters, INL did not focus specifically on the Enterprise Zone; rather it compared the Control Center/Processing LAN Zone and the Controller LAN/Field I/O Devices Zone. For analysis purposes, INL considered the Local HMI LAN Zone to be a network that inherits a mixture of attributes from both of the previous zones.

### 4.1.1 Control Center/Processing LAN Zone

Within the Control Center/Processing LAN Zone (Control Center), IOC Detection tools are relatively complete and well tested. These tools are produced by well-recognized companies with vast experience in the security sector. The major weakness in this area is embedded devices on the network, such as bump-in-the-wire solutions for protocol conversion. Without significant knowledge of how the device works, there is no way to detect indicators of compromise. The performed survey did not discover any solutions that would solve this issue.

Control Center Network Traffic Anomaly Detection (NTAD) tools are plentiful, but do not completely cover the area of concern. Although the identified NTAD tools are well suited for TCP communication, the control center network could possibly see some industrial protocols, such as OPC, for historian usage. Currently available tools do not completely cover the slightly more obscure protocols, and therefore do not completely cover the domain that is required.

Outlier Analysis (OA) within the Control Center network is fairly well covered due to big names such as McAfee and AlienVault. These programs work well with large amounts of data to train what is considered "normal traffic" in addition to typically (only) running on Windows devices. This means host-based OA, such as sand-boxing on anomalous system access, can only be conducted on Windows. Moreover, OA is almost impossible for embedded devices on the network due to the lack of access to most devices in this designation, as well as the lack of traffic fingerprinting that is performed by device manufacturers.

Log Review (LR) is well covered on a Control Center network due primarily to the fact that most devices on the network are syslog capable. Even devices that contribute to the more obscure protocols on the network typically run on a Windows device which can provide logs to a syslog server equally as well as any other Windows or NIX device. Many well-developed tools already exist for this purpose due to the common log format shared by Windows and NIX devices.

System Artifact Review (SAR) is covered by large tools such as Nessus on Windows. By performing credentialed scans, Nessus is able to check registry values and other artifacts to determine if vulnerabilities are present, or if known malware processes are running on the system. This covers the most valuable system artifacts automatically. Although tools like Nessus work on NIX environments, they do not have the same ease of use due to the lack of data aggregation that occurs in the Windows environment. The same problem plagues embedded devices on the Control Center network. Often credentials are not available, and access may or may not be available making system artifact collection, let alone review, very difficult.

RE analysis is very well covered in this environment. Tools such as IDA pro, Binary Ninja, WinDbg, and x64Dbg all support static and dynamic binary analysis. Due to the massive amount of x86 architectures in this network, it would be rare to find a binary that a current RE tool could not handle with ease.

### 4.1.2 Local HMI LAN Zone

As the Local HMI LAN Zone inherits devices from both the Control Center Zone and the Controller LAN/Field I/O Devices Zone, it will not be discussed in depth. The Local HMI LAN Zone comprises a mix of industrial control devices, whose issues mirror those discussed in Section 5.1.1 and 5.1.3. With respect to tools discussed within the Control Center Zone, the effectiveness of the tools that previously performed well decreases within the Local HMI LAN Zone due to less normal TCP traffic on the network and an increase in industrial protocols.

### 4.1.3 Controller LAN/Field I/O Devices Zone

IOC within field devices are much harder to detect and categorize. Existing tools claim they can successfully detect IOC on an ICS network, but these mostly stem from newer companies with unknown reputations. Some examples of this are Verve Security Center and NextNine ICS Shield. These tools would need to be reviewed for effectiveness before it is reasonable to assume that this purpose is covered

in an embedded environment. Often, tools claim detection but in reality the tool only applies to a specific configuration or subset of devices.

NTAD for field devices is partially covered. NTAD tools such as BroIDS and several others have parsers for industrial communication protocols such as DNP3 and Modbus; the DNP3 parser in Bro is incomplete, but a good starting point for development. This demonstrates that extensible tools such as these can be adapted for anomaly detection on field networks. Since not every protocol, or even every common protocol, is covered, this purpose is not covered completely.

OA, LR, and SAR in the field zone all lack tool sets. INL coupled these together due to the significant lack of variety in this area. All areas of interest are claimed to be covered by untested, new tools such as Indegy Platform, NextNine ICS Shield, and Claroty. Logs and system artifacts are often only obtainable through vendor software (which is not covered in this survey – see Section 1.2) and does not check for anomalies or interface with software that does. This severely limits the effectiveness of tools for recovery. Of all of the purposes/zones covered by this survey, OA, LR, and SAR within the Field I/O Devices Zone are in need of significant investment of attention to increase tool availability.

RE analysis is well covered for only static analysis. IDA Pro, Binary Ninja, and Radare all support multiple architectures. Many times, disassembling a binary is not an issue regardless of where it is found. The difficulty that is inherited in the Field I/O Devices Zone is the loss of dynamic analysis which often can significantly increase the difficulty of analysis. Further, difficulty is added when working with raw firmware dumps instead of a set file type that includes valuable information such as entry points and hardware peripheral connections. Current tools do not include mechanisms to automatically analyze binaries to find the proper entry point. The difficulty increases exponentially when embedded systems have multiple processors each with their own program; frequently memory and artifacts are stored across different processors' memory and this information is lost in static analysis.

# 5. Future Technologies / Desired Attributes

Using quantitative data obtained during the survey, INL identified "low hanging fruit" in terms of extending existing tools to fill a discovered gap. Further, INL compiled a "wish list" of tool attributes that could be developed to fill specific, niche areas for which no current capabilities exist. These are both presented below.

## 5.1 Tool Extension / Modification

During the survey, INL identified gaps it determined would be fairly simple to fix given an extension of an already existing tool. For example, Bro IDS is not currently qualified as a "field" anomaly detection tool; Bro does not have built-in support for most protocols that would be present in a field network. Even though parsers exist for DNP3 and Modbus, they are not complete. Additional protocols, such as PROFINET, BACnet, S7COMM, GOOSE, and MMS would all be useful additions to Bro and would extend its capability into the realm of field networks. These additions are supported by the original tool, but would require development effort to be put forth. This effort could present a large payout for a small amount of effort to improve the ICS security tool landscape. Once anomaly detection is covered, the SMEs must also develop rulesets based off of their knowledge and ICS-specific flags before a tool is able to alert users.

Another example of "low hanging fruit" identified by INL would be to address the gap of SAR tools. During the survey, items that were deemed potentially useful, but not part of an implementable tool, were designated a "tool enabler." To address SAR on a field device, it is possible that a JTAG device could be used for direct memory access to the device and to review specific memory addresses for artifacts. This

technique also could be used for a host-based IDS/IPS with the proper implementation. Although this type of tool would require major development work, a tool like this does not currently exist in any form for any network. In terms of effort to reward, this would most likely be moderate effort for moderate payout. These types of opportunities are far more attractive for development than trying to re-invent a network-based anomaly detection tool that is specialized for ICS networks.

Although these two examples were easily identified, many more options for extending currently available tools exist. Extending/modifying tools does not solve all of the issues present in the ICS security world; however, it can provide fast and efficient solutions for many current gaps.

## 5.2 Desired Tool Attributes

Desired attributes to address the most prevalent gaps found in this survey include:

- Additional rulesets for well- known IDS systems for a deep inspection of protocols such as PROFINET, BACnet, S7COMM, GOOSE, MMS, and other industrial protocols;
- Better entry point detection and plugins to support disassembly and debugging of firmware dumps for non x86_64 platforms;
- Log retrieval tools for systems with proprietary log formats, or converters that convert logs into common formats such as syslog for consumption by anomaly detection applications;
- SAR specific to field devices that monitors system load and events for malicious activities;
- Rulesets for applications such as YARA to detect discrepancies between PLC logic infected with malware and PLC logic that is the gold standard for the field; and
- Tools that can automatically scan a field of devices and provide a list of known vulnerabilities.

# 6. Conclusions

During the survey, INL found a growing number of tools available for ICS networks and devices; however, there are very few tools available to combat attacks in several common areas. The purpose areas with the least number of tools available were LR and OA within Controller LAN/Field I/O Device zone. The survey found no tools to investigate proprietary log files for anomalies or scan ladder logic applications for malicious behavior. Although some field devices may have embedded Linux or a similar embedded OS that lends itself more to standard log formats and investigation, the majority of devices use proprietary vendor-specific software that is opaque to security tools.

Focusing efforts on devices with few to no forensic tools available, a lack of active tools exist for use on SCADA equipment. A few advertised tools – most notably from Symantec and Honeywell – are currently being developed to address this area, but are not commercially available at this time. The most common area of concern is at the firmware or ladder logic level, where there are no publicly available security-centric tools to validate that the device has not been compromised. Further, malware can reside at the chip level; research did not uncover any tools to validate the contents of a chip's internal structure. INL discovered only one tool that would help with ladder logic compliance (listed in Appendix A).

The survey did not find any vendor-specific security solutions that penetrate deep into field devices. INL discovered vendors that have designed field devices with built-in security, such as BedRock Solutions. Further, vendor solutions were found that offer security solutions to monitor the network and perform deep packet inspection of industrial protocols.

INL found no security-specific tools to extract the proprietary logs from field devices for anomaly detection. If the field device supports standard log mechanisms, such as syslog, tools exist to monitor and

parse through the logs; however, several field devices use their own vendor-specific log format which must be extracted and converted before it would contain useful information that an anomaly detection tool could use. In these cases, the only option is to use the vendor software to extract the logs and then feed them into the tool or consult a SME.

Several tools are extensible enough that with minor development, they could be used to cover specific ICS issues for which there is no tool. For example, INL did not find any tools to check PLC application software for ladder logic bombs; however, a tool such as YARA could do this by simply creating a definition of some known bytes in malicious ladder logic. Similarly, tools such as Bro, Snort, and other IDS/IPS solutions would only require a ruleset to alarm on ICS-specific malicious network traffic. Any new tool development should first evaluate existing tools and tool sets to determine if the tool could interface with existing tools and broaden its abilities, rather than create another independent tool. Currently, several toolsets, such as Security Onion, simply take existing tools and provide the "glue," enabling them to work together and to provide the user with valuable information.

Without extensive testing and investigation, a definitive conclusion cannot be made as to whether a particular tool would be a good fit for a specific ICS security problem. Many of the commercial and some of the open source tools offered blanketing documentation to give the user the impression that the tool solved a broad range of ICS issues but lacked basic details about how the tool operates. Terms such as "unique machine learning" and "automated learning" are helpful, but often leave out needed information such as the exact platforms supported, or how the tool interfaces with the system under test. Many of the tools point the reader to sign up for a demo which would be the only way to assess how the tool actually performs and interacts within a system. A follow on phase to this survey would allow deeper investigation into the tools and evaluation of the claims made by tool vendors, as well as investigation into the learning curves and usability of the tools.

# Appendix A
# Currently Available Technologies

## Multi-Purpose Tools

**AlienVault® Unified Security Management™ (USM™) SIEM**
https://www.alienvault.com/
AlienVault USM combines powerful SIEM and log management capabilities with security tools to provide users with centralized security monitoring of cloud, hybrid cloud, and on-premises environments. It features asset discovery and inventory, vulnerability assessments, intrusion detection, behavioral monitoring, and SIEM and log management. Users receive threat intelligence updates from the AlienVault Labs Security Research Team, which also leverages data from the Open Threat Exchange® (OTX®).

**CheckPoint Software - SandBlast**
https://www.checkpoint.com/products-solutions/zero-day-protection/
SandBlast is a software application that is installed on enterprise level gateways. It has several different software blades to thwart infection and propagation of malware. Files traveling across the network are scanned and removed if they are flagged as dangerous. The software blades run on SandBlast's hardware appliance.

**Claroty**
https://www.claroty.com/
Claroty explores OT protocols to identify the elements encapsulated in traffic. It monitors all network communication to find hidden issues and to establish a high-fidelity baseline model so that it can detect anomalous behavior. Claroty combines native OT knowledge with advanced models and algorithms to generate detailed alerts, complete with actionable insights, for both cybersecurity and process integrity issues. A passive monitoring system, Claroty does not require active scanning or the installation of software on endpoint devices.

**Dragos**
https://dragos.com/product.html
Dragos Industrial Cybersecurity Ecosystem combines an on-premise platform, threat operations service, and global threat intelligence. The platform compiles and correlates suspicious events at scale and speed. The suite offers asset discovery and compromise assessment; threat hunting and detection; and forensics, automated workflows, and incident response.

**Indegy Platform**
http://www.indegy.com/
The Indegy platform provides visibility into ICS networks, identifying changes to critical controllers, including change to firmware, logic, and configuration updates. It features a deep packet inspection engine, specifically designed for the unique characteristics of industrial control systems. Patent-pending technology detects control-layer events in vendor-specific communications, used for operating IEC-61131 compatible industrial control systems. It passively monitors standard operational communication protocols (like Modbus & DNP3) and provides in-depth, real-time visibility into all activities performed over the operational network. Indegy utilizes patent-pending technology used for validating control device state and ensuring no unauthorized changes were made. It periodically verifies controller device firmware, application, and configuration to provide full visibility with details for each controller. It captures all changes to PLCs and RTUs, whether performed over the network or directly on the physical devices.

**McAfee**
https://www.mcafee.com/us/solutions/critical-infrastructure.aspx
McAfee offers a suite of security products geared towards the critical infrastructure sector categorized into four areas: database and endpoint security; data protection; network security; and SIEM. Together, the tools enable discovery, prevention, detection, response, audit, and management across data, the network, and endpoints within enterprise IT, SCADA, and ICS zones. In addition, McAfee offers incident response and forensics for security breaches into SCADA networks.

**Nessus (N)™**
http://www.tenable.com/plugins/index.php?view=all&family=SCADA\
https://www.tenable.com/products/nessus-vulnerability-scanner
Nessus is a proprietary vulnerability scanner developed by Tenable Network Security. It is free of charge for personal use in a non-enterprise environment. Offered as Nessus Professional (NP)™ or Nessus Manager (NM)™, the tool protects IT environments by running vulnerability scans, configuration and compliance checks, malware detection, Web application scanning; includes assessment capabilities, agent-less and agent-based scanning; and runs reports and filters data.

**Nextnine ICS Shield**
https://nextnine.com/solutions/ics-shield/
ICS Shield is Nextnine's top-down OT security management solution for securing connected ICS/SCADA environments. ICS Shield secures remote field assets from a single operations center. It automates the deployment and enforcement of plant-wide security policies while focusing on security essentials such as inventory visibility, patching, log collection, incident alarm and response, and compliance reporting. It is currently deployed at industrial plant operations in the oil and gas, utility, chemical, mining and manufacturing sectors.

**SecurityMatters SilentDefense**
https://www.secmatters.com/product
SilentDefense's offers built-in detection capabilities and allows users to define custom checks for their specific industrial environments. It pulls from SilentDefense's Industrial Threat Library to detect a wide variety of industry-specific threats. Users can learn and validate network communication patterns and process operations with the in-depth analysis of industrial protocols (DPBI™ patented technology); identify rogue and malfunctioning devices, intrusions, and attacks; and detect undesired configuration changes before they can affect the process. SilentDefense integrates with Splunk, ABB, siemens, Rockwell, Schneider, Honeywell, Emerson, and Yokogawa.

**Symantec Embedded Security: Critical System Protection**
https://www.symantec.com/products/information-protection/encryption/embedded-security
Symantec Embedded Security: Critical System Protection provides a host firewall, device and configuration control, file integrity monitoring, intrusion detection, OS hardening, application whitelisting, and automatic sandboxing. Designed to run on devices such as industrial control systems, the agent has been optimized for embedded OS, including Microsoft® Windows Embedded Family (multiple versions), and QNX® Real-Time Operating System, and non-embedded systems, including: Linux, Microsoft® Windows (multiple versions), and Microsoft® Windows Server Family (multiple versions).

**Tripwire® Configuration Compliance Manager (CCM)**
https://www.tripwire.com/products/tripwire-configuration-compliance-manager/
Tripwire CCM utilizes active and passive scanning to discover and audit configurations. Users receive highly detailed information on the configurations of systems, applications, firewalls, routers, and switches. Tripwire CCM utilizes an agentless architecture, requiring no software to install on the

monitored endpoints. It automates continuous configuration and compliance assessment, making it easy for user's policy engines to tune and modify custom policies.

**Verve Security Center**
http://verveindustrial.com/products/
The Verve Security Center suite includes vulnerability scans, patching, backup management, application whitelisting, antivirus, change management, SIEM, and compliance tools. It is marketed to be vendor agnostic, simple to use, and non-disruptive to communications. The tool integrates the latest security tools into one console; protects ICS systems with an ICS-safe cybersecurity solution; monitors and remediates security and compliance; and protects all vendor equipment, including ICS devices including relays, IEDs, PLCs, etc.

## IOC Detection Tools

**ABB's Cyber Security Benchmark**
http://new.abb.com/process-automation/process-automation-service/advanced-services/cyber-security-services/cyber-security-benchmark-and-fingerprint/cyber-security-benchmark1
Cyber Security Benchmark utilizes ABB's proprietary tool collection to automatically and non-invasively gather data. It conducts proactive analysis of Key Performance Indicators to detect possible security weaknesses and features a Web-based "stoplight" report that provides an easy-to-read overview of security status immediately available after data collection.

**FireEye IOC Editor**
https://www.fireeye.com/services/freeware/ioc-editor.html
The FireEye Indicators of Compromise (IOC) Editor is a free tool that provides an interface for managing data and manipulating the logical structures of IOCs. IOCs are XML documents that help incident responders capture diverse information about threats, including attributes of malicious files, characteristics of registry changes and artifacts in memory. The IOC Editor includes manipulation of the logical structures that define the IOC; application of meta-information to IOCs, including detailed descriptions or arbitrary labels; conversion of IOCs into XPath filters; and management of lists of "terms" used within IOCs.

**FireEye IOC Finder**
https://www.fireeye.com/services/freeware/ioc-finder.html
The FireEye Indicators of Compromise (IOC) Finder is a free tool for collecting host system data and reporting the presence of IOCs. IOCs are open-standard XML documents that help incident responders capture diverse information about threats. The IOC Finder features collection of full data, sufficient for general IOC matching requirements; usage of a portable storage device for collection from multiple hosts IOC hit reporting in simple text, full HTML and full MS Word XML formats; and generation of reports for specific hosts or all hosts.

**Radiflow**
http://radiflow.com/
http://radiflow.com/wp-content/uploads/2016/12/radiflow_free_assessment.pdf
Radiflow's ICS Security Checkup detects all known threats and vulnerabilities, including SCADA-specific threats, such as Black Energy malware and malware spreading across PLCs Logical changes in PLCs Open remote SSH sessions. Users record network traffic for three days on Radiflow's mini PC and then send it to Radiflow for review and analysis. The company provides a comprehensive status and vulnerability report.

## Network Traffic Anomaly Detection Tools

**Bro**
www.broala.com
Bro is an open source IDS that runs on standard hardware with a Linux-based OS. It is a NIDS that specializes in traffic analysis. Bro keeps comprehensive logs and has a range of analysis and detection techniques, including signature-based and anomaly detection. Bro's signature engine is not based on Snort. It is capable of detail-oriented matching like Snort. There is an effort to convert Snort signatures to Bro signatures. The converted signatures and rules can be found on its website. Bro supports port-independent analysis of application-layer protocols, including DNP3 and Modbus, and file content analysis. Support for this software is available through various means including a mailing list and email. Commercial support is available through Broalo, which is a commercial spin off of Bro.

**Conpot**
https://github.com/mushorg/conpot
Conpot is an ICS honeypot with the goal to collect intelligence about the motives and methods of adversaries targeting ICS. This dockerized ICS-specific honeypot includes modbus, s7, http, snmp, bacnet, snmp, and Ipmi protocols. Conpot has built-in support for HPFeeds, a generic data sharing protocol used by the Honeynet Project. Raw data is in JSON format and a Python client uses the HPFeeds library. Users that want to access to the conpot data must create a HPFriends account; by sending data via HPFeeds, users agree that it might be shared with third parties.

**CyberX X-Sense**
https://cyberx-labs.com/en/xsense/
XSense continuously monitors networks for OT threats and vulnerabilities, such as unauthorized remote connections and unpatched or unknown devices. It provides both alerts and actionable intelligence with recommended mitigations. XSense provides REST APIs and supports any ICS vendor, industrial protocol, or SIEM.

**Darktrace ICS**
https://www.darktrace.com/products/
Darktrace (Core) is a threat detection and defense capability based on unsupervised machine learning and probabilistic mathematics. Developed by mathematicians from the University of Cambridge, Darktrace is capable of detecting cyber-threats and anomalous behaviors that bypass traditional security tools, without prior knowledge of specific threats, or using rules or signatures. It analyzes raw network data, creating unique behavioral models for every user and device, and for the relationships between them. Leveraging machine learning algorithms, Darktrace forms an evolving understanding of an organization's 'pattern of life' (or 'self'), spotting very subtle changes in behaviors, as they occur. These behavioral changes are correlated and filtered to detect emerging threats and anomalies. Darktrace is delivered as a physical appliance and installed at a SPAN or TAP port within the customer network(s). The appliance passively monitors raw network data in real time, without disrupting business operations, and provides instant visibility into all network activity, notifying of in-progress attacks or emerging anomalies.

**Fortinet-Nozomi Networks**
https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/SB-Securing-Industrial-Control-Systems-with-Fortinet.pdf
This joint solution combines Nozomi Networks' SCADAguardian with Fortinet's FortiGate. Placed onto the OT network, SCADAguardian passively monitors network traffic, creating an internal representation of the entire network, its nodes, and the state and behavior of each device in the network. Using predefined and continually updated signatures, the FortiGate can identify and police most of the common

ICS / SCADA protocols for the purpose of defining conduits. This is done through the configuration of security policies in which multiple services, such as IPS, antivirus, and application control, can be mapped to each protocol. In parallel to this specific protocol support, additional vulnerability protection is provided for applications and devices from major ICS manufacturers through a complementary set of signatures. This provides a more granular application-level control of the traffic between zones and enables the FortiGate to detect attempted exploits of known vulnerabilities relating to any of the supported vendors' solutions. The solution is able to learn the behavior of all protocols as well as define custom ones.

**GridPot**
https://gridpot.org
https://github.com/sk4ld/gridpot
https://github.com/sk4ld/vagrant-skyline-puppet
Symbolic Cyber-Physical Honeynet Framework.Symbolic simulation of cyber physical systems emulate SCADA/HMI and industrial control system protocols. Uses ETSY's skyline project for anomaly detection. Shows real time attacks.

**mbSECBOX**
http://www.mbconnectline.com/
https://worldindustrialreporter.com/plc-malware-detector-mbsecbox/
The mbSECBOX PLC security solution detects malware similar to STUXNET and other possible threats on the S7 Controllers. After a threat is found, the mbSECBOX PLC malware detector immediately alerts the operator before any damage occurs. The order number and the serial number from the PLC are read and stored in memory. Based on the reference data, the PLC malware detector continuously monitors the static memory area of S7-300 and S7-400 controllers. The program blocks are read in a user-specified interval and compared with the reference backup. When changes are executed to the program data, the system operator will be informed via an email, text message, a warning light, or siren triggered from an output interface. Manipulation by malware and viruses are recognized as unauthorized changes to the controller's program. The connection to the controller is established via the MPI-/Profibus or Ethernet. For security reasons, the device is not accessible over the company network of the Internet.

**MSi Sentinel and MSi 1**
http://www.missionsecure.com/solutions/
Together the MSi Secure Sentinel™, MSi 1™ and MSi Console™ provide plant, facility, and control systems security. The MSi suite offers vertical analysis to ensure key control system components are aligned and have not been compromised; continual and secure multi-layered system monitoring at the IP level and digital and analog signals; real-time analysis and automated incident detection; secure and dedicated communications systems with trusted system operators and cyber security professionals; system data from the digital and analog sensors and actuators and controllers for forensic purposes; and automated, or operator guided, response and restoration of mission and/or system function to a safe operating state.

**N-Dimension Solutions n-Platform 340S or 440D**
https://cdn.selinc.com/assets/Literature/Publications/Application%20Notes/AN2009-07_20090617.pdf?v=20151202-140030
http://www.hometownconnections.com/assets/DataSheet-nPlatform-440D.pdf
The N-Dimension Solutions n-Platform 340S or 440D Unified Threat Management Systems provide a suite of network security functionalities. The n-Platform 340S or 440D software is coupled with a hardware platform, such as the SEL-1102 – a "rugged" computer. The software features two modes – surveillance and gateway. Surveillance mode features include SCADA intrusion detection system (IDS),

vulnerability scan, port scan, availability monitor, and performance monitor. The Gateway mode features routing, firewall, antivirus, proxy filter, network device control, virtual private network, ldap.

**OSSEC**

www.ossec.net

This is a HIDS. OSSEC features include HIDS, log monitoring, signature analysis (based on a Snort2 engine), anomaly detection, file integrity checking capabilities, and central logging service. It contains a central management server and agent based on agentless monitoring of systems. OSSEC runs on standard hardware with a Linux-based OS. The OSSEC website provides some options for commercial support.

**Security Onion**

www.securityonionsolutions.com

This is a network security monitoring (NSM) open source suite of tools, which is a compilation of all the open source solutions previously mentioned. It includes a NIDS, a HIDS, a full packet capture, and analysis tools. Security Onion includes Suricata or Snort, Bro, OSSEC, Sguil (management console), SQUERT (web application interface to the database), Snorbyg (web application interface), ELSA (an enterprise log search and archive tool), and many other tools. A complete listing of the tools it includes can be found at https://code.google.com/p/security-onion/wiki/Tools. It is typically deployed as a client-server model, but it can be standalone. Commercial support is available through its website.

**SENAMI IDS**

https://github.com/WilliamJardine/SENAMI/

SENAMI is a bespoke IDS for Siemens S7 ICS environments. It combines traditional Network IDS methodologies with "active" intrusion detection, which requests values directly from the PLC to monitor. Specifically, it introduces the concept of “selective, non-invasive active monitoring” to avoid overloading legacy ICS devices. SENAMI features two core components. First a passive IDS checks the quantity of received packets by function code, the time they arrive, and the IP source, destination, and presence of logic upload packets. These passive checks are compared against set heuristics for the system and occur at set interval. Second, a selective, non-invasive active monitoring IDS reads in specific values and compares the difference between these values every five seconds. Differences out of the acceptable limit indicate an attempt to tamper with monitoring. The two components both generate alerts, reported live in the IDS terminal and saved to a logfile for further analysis with the SIEM.

**Snort**

https://www.snort.org/

Snort is an open source network IDS/IPS. Best known for its signatures and signature engine, it also performs protocol analysis, content searching/analysis, and anomaly detection. Signatures are available for free or by a paid subscription, the difference being how recent the signatures are. Support for this software is available through various means including mailing lists, blogs, webcasts, email, and paid subscriptions. Snort was purchased by Cisco and is used in it products; however, it is continuing to support the open source model. Use of Snort for commercial purposes requires a license agreement with Cisco.

**Suricata**

www.securityonionsolutions.com

Suricata is an open source next generation intrusion detection and prevention engine. It is designed to work with Snort signatures, but Suricata-optimized rules are available from Emerging Threats. Suricata features includes multithreading (provides speed), protocol detection, gzip decompression, flow analysis, IP reputation, log analysis, GeoIP, and anomaly detection. It runs on standard hardware with a Linux-

based OS. Typically, Suricata or Snort, one or the other, is used, not both. Support for this software is available through various means including mailing lists, training, Internet relay chat (IRC) and bug tracker. Commercial support is available through its website.

**Symantec Anomaly Detection for Industrial Control Systems**
https://www.symantec.com/content/dam/symantec/docs/data-sheets/anomaly-detection-for-industrial-control-systems-en.pdf
Anomoly Detection for ICS provides visibility into ICS devices and their communications. Deep Packet Inspection of all ICS protocols allows the tool to learn expected field types (such as op codes) and values (such as temperature ranges) from inside message payloads and identify. Its advanced machine learning algorithms analyze small behavior variations to catch subtle attacks and offers criticality based incident prioritization with forensic data provided for remediation. Through automated learning, Anomaly Detection learns user's networks and creates rules without complex policy settings. The on-premise, software solution can use existing hardware without Internet access.

**Tofino Xenon Security Appliance (Tofino SA)**
https://www.tofinosecurity.com/
https://scadahacker.com/library/Documents/OPC_Security/Securing%20Your%20OPC%20Classic%20Control%20Systems.pdf
The Tofino SA provides a simple and cost-effective way to create zones of security − tailored protection for groups of PLCs, DCS, RTUs, IEDs, and HMIs − as recommended by ISA/IEC-62443 Standards. It is a Plug-n-Protect™ product, designed to be installed in a live network with no pre-configuration, no network changes, and no plant downtime. It offers pre-emptive threat detection, threat termination, and threat reporting. Tofino is compatible with all DCS, PLC, SCADA, networking, and software products and secures networks with security zones as per NERC, ANSI/ISA, and IEC standards. It also protects connections to partner networks and wireless network and improves SCADA and process control network reliability and performance.

**T-Pot**
https://dtag-dev-sec.github.io/mediator/feature/2016/03/11/t-pot-16.03.html
T-Pot combines the dockerized honeypots conpot, cowrie, dionaea, elasticpot, emobility, glastopf and honeytrap with suricata, a Network Security Monitoring engine, and the ELK stack to visualize all the events captured by T-Pot. The T-Pot project provides users with the tools and documentation necessary to build their own honeypot system and contribute to its community data view. Events will be correlated by the data submission tool ewsposter which also supports Honeynet project HPfeeds honeypot data sharing.

**TruffleHog**
https://github.com/TruffleHog/TruffleHog
Started as a university project at the Karlsruhe Institute of Technology, this program requires a modified version of Snort including a PROFINET-preprocessor to collect "Truffles" representing a semantic analysis of one PROFINET-network package. It keeps track of all incoming Truffles, uses the semantic information to build a network topology (a network map) and displays it to look at in quasi real time. More advanced features, such as replaying network changes, applying filters to network participants, and alerts and notifications, are planned to appear in a later version of the program.

## Outlier Analysis Tools

**WeaselBoard**
http://www.sandia.gov/news/publications/labnews/articles/2016/04-03/weaselboard.html
WeaselBoard provides zero-day exploit protection for programmable logic controllers (PLCs). By capturing and analyzing backplane traffic among PLC modules, WeaselBoard detects changes to process control settings, sensor values, module configuration information, firmware updates, and process control program (logic) updates. WeaselBoard is a PLC backplane analysis system that connects directly to the PLC backplane to capture backplane communications between modules. It forwards inter-module traffic to an external analysis system that detects changes to process control settings, sensor values, module configuration information, firmware updates, and process control program (logic) updates.

## Log Review Tools

**Elastic Stack**
https://www.elastic.co/products
The stack of tools available from Elastic allow a user to gather data from any source and then search through and filter the data. Then the user can create visualizations of the data to create a command center. This allows the users to see anomalies and issues as they come up, provided the user creates the correct rulesets and is able to retrieve the data they need.

**Graylog**
https://www.graylog.org/features
Graylog is a platform for gathering log data into a centralized management system. It has user access control to fine tune who can attend what, and it has a restful API for extending the platform further. Graylog also has the ability to add alerts via a simple GUI interface to create new alert conditions and set callbacks.

**Plaso - Log2timeline**
https://github.com/log2timeline/plaso
Log2timeline is designed to extract timestamps from various files found on a typical computer system(s) and aggregate them. It creates logs by adding new parsers or parsing plug-ins; adding new analysis plug-ins; and writing one-off scripts to automate repetitive tasks in computer forensic analysis or equivalent.

**Splunk®**
https://conf.splunk.com/session/2015/conf2015_TMcCorkle_Splunk_SecurityCompliance_SplunkForIndustrialControl.pdf
https://conf.splunk.com/files/2016/slides/splunk-and-control-systems-enabling-a-secure-iot-strategy.pdf
Splunk offers a platform for operational intelligence; it pulls security data from ICS devices (PLC data, HMI and historians, DHCP/DNS, servers, industrial endpoints, etc.) and reviews network protocols, authentication, device behavior, HMI behavior, and operational changes. It offers incident investigations and forensics; security and compliance reporting; real-time monitoring of known threats; monitoring of unknown threats; fraud detection; and insider threat.

**Waterfall BlackBox**
https://waterfall-security.com/products/waterfall-blackbox

BlackBox is a high-speed, high-capacity logging and analysis system, which can be used to reveal attackers' tracks, detection of attempted changes, manipulation, and abnormal activities. To keep log repositories more secure than the attacked network, Waterfall developed the BlackBox to maintain the integrity of log repositories. It was developed with response teams, forensics, and other audit professionals in mind, to maintain trust in logged information. Based on Waterfall's patented unidirectional security technology, the Waterfall BlackBox secures logs "behind" a unidirectional gateway, ensuring that logs are physically kept trustworthy and out-of-reach of cyber attackers. With the BlackBox, there is a physical barrier between the network and the logged data so that the data sent to the BlackBox is stored physically "outside" the network, inaccessible and untouchable to anyone looking to cover their tracks. In time of need, data can be retrieved and inspected securely by physical access to the BlackBox appliance.

## System Artifact Review Tools

**ChipSec**
https://github.com/chipsec/chipsec
CHIPSEC is a framework for analyzing the security of PC platforms including hardware, system firmware (BIOS/UEFI), and platform components. It includes a security test suite, tools for accessing various low level interfaces, and forensic capabilities. It can be run on Windows, Linux, Mac OS X and UEFI shell.

**CodeDNA**
http://www.jhuapl.edu/ott/technologies/technology/articles/P03366.asp
CodeDNA detects families of attacks and supports a navigable means of exploring attack family development, leading to insights and predictions about what a broad range of future zero-day attacks may look like, so that the defenders can detect them instantly. CodeDNA is a patented defensive technology that facilitates community-based defense against malware attacks. By generating unique DNA-like fingerprints from incoming files and computing similarity scores across a database of fingerprints, CodeDNA can automate the identification of related malware binaries and link variants.

**Digital Ants**
http://i4.pnnl.gov/news/digitalants.stm
Digital Ants uses dynamic, decentralized mechanisms inspired by nature to provide mobile, resilient cybersecurity for protecting large enterprise IT networks and critical infrastructures. Individual ant-like sensor programs swarm to the location of anomalies and enable human operators to focus on areas and issues of concern.

**USB-ARM**
https://www.dhs.gov/sites/default/files/publications/csd-ttp-finance-five.pdf
USB-ARM provides a simple, efficient, and customizable layer of security that brokers all communication between removable media and the OS. It executes user-defined stages and either grants or disallows access on a per- file basis. USB-ARM guarantees that a set of user-defined criteria are met prior to allowing access to the removable media.

**Volatility Framework**
https://github.com/volatilityfoundation/volatility
The Volatility Framework is a completely open collection of tools, implemented in Python under the GNU General Public License, for the extraction of digital artifacts from volatile memory (RAM) samples. The extraction techniques are performed completely independent of the system being investigated but offer visibility into the runtime state of the system. The framework is intended to introduce people to the

techniques and complexities associated with extracting digital artifacts from volatile memory samples and provide a platform for further work. The Volatility Framework is only for Windows (XP-10), Linux, and Mac; it does not scan mem in embedded Windows or PLCs unless they are running Linux.

**YARA**
http://virustotal.github.io/yara/
YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA users can create descriptions of malware families (or whatever they want to describe) based on textual or binary patterns. Each description, a.k.a. rule, consists of a set of strings and a boolean expression which determine its logic.

## Reverse Engineering Analysis Tools

**Binary Ninja**
https://binary.ninja/
Binary Ninja is a reverse engineering platform. It focuses on a clean and easy to use interface with a powerful multithreaded analysis built on a custom intermediate language to quickly adapt to a variety of architectures, platforms, and compilers.

**Binwalk**
https://github.com/devttys0/binwalk
Binwalk is a fast, easy to use tool for analyzing, reverse engineering, and extracting firmware images.

**Centrifuge**
https://www.tacnetsol.com/pages/firmware-evaluations
Centrifuge takes binary files containing firmware images on them and does full evaluations to detect CVE using their cloud based service. The cloud based service will also point out any vulnerable code so you can remediate the risk if you have access to the source code. The service provides easy to read reports per file.

**fcd**
https://zneak.github.io/fcd/
fcd is a burgeoning LLVM-based native program decompiler. Most of the code is licensed under the GNU GPLv3 license, though some parts, such as the executable parsing code, are licensed under a less restrictive scheme. Currently, fcd works best with executables that follow the x86_64 System V ABI. fcd supports ELF executables out-of-the-box, but also ships with Python scripts that can be used as plug-ins to parse Mach-O and PE executables.

**Hex-Rays IDA Pro**
https://www.hex-rays.com/index.shtml
IDA (Interactive DisAssembler) is written entirely in C++ and runs on the three major OS: Microsoft Windows, Mac OS X, and Linux. IDA also serves as the foundation on which the Hex-Rays Decompiler is built. The Hex-Rays facilitates binary software analysis by converting executable programs into a readable C-like pseudocode text.

**Hopper Disassembler**
https://www.hopperapp.com/
The Hopper Disassembler is a reverse engineering tool designed for macOS and Linux that allows users to disassemble, decompile, and debug applications. Hopper analyzes function's prologues to extract procedural information such as basic blocks and local variables. The macOS version makes full use of the

Cocoa framework, and the Linux version makes use of Qt 5. Most of the Hopper features can be invoked from Python scripts; it can use LLDB or GDB to debug and analyze the binary dynamically (Intel CPU only).

**Hyperion**
https://www.ornl.gov/partnerships/ornl%E2%80%99s-hyperion-technology
Hyperion is a cyber security technology designed to "look inside" an executable program and determine software's function or "behavior" without the use of the software's source code. Hyperion accomplishes this by generating associated program behaviors and the complete set of conditions under which they occur. These behaviors can be automatically checked for known malicious signatures and inspected by domain experts to assure correct operation and the absence of malicious content. Hyperion can also be used to check a program's security properties and to optimize a program.

**Radare**
http://radare.org/r/
Radare is a portable reversing framework that can: disassemble (and assemble for) many different architectures; debug with local native and remote debuggers (gdb, rap, webui, r2pipe, winedbg, windbg); run on Linux, *BSD, Windows, OSX, Android, iOS, Solaris, and Haiku; perform forensics on filesystems and data carving; be scripted in Python, Javascript, Go, etc.; support collaborative analysis using the embedded webserver; visualize data structures of several file types; patch programs to uncover new features or fix vulnerabilities; use powerful analysis capabilities to speed up reversing; and aid in software exploitation.

**Snowman**
https://derevenets.com/
Snowman is a native code to C/C++ decompile that supports ARM, x86, and x86-64 architectures. It reconstructs functions, their names and arguments, local and global variables, expressions, integer, pointer and structural types, all types of control-flow structures, including switch. The graphical user interface allows one-click navigation between the assembler code and the reconstructed program. It includes a command-line interface for batch processing and offers an IDA Plug-in.

**Synopsys Protecode**
https://www.synopsys.com/software-integrity.html
Protecode is now owned by Synopsys. Protecode creates a BOM of all of the shared libraries used in application code and provides a list of known vulnerabilities. Synopsys also has tools to scan for new vulnerabilities in code and provides developers with a way to make more robust code.

**x64dbg**
http://x64dbg.com/#start
Using a single interface, X64dbg can debug both x64 and x32 applications. Built on open-source libraries (Qt, TitanEngine, capstone, Yara, Scylla, Jansson, Iz4, XEDParse, Keystone, asmjit, and Snowman), X64dbg is customizable and extendable and offers executable patching and analysis.

# Appendix B
# Tool Enablers

**Bedrock Solutions**
https://www.bedrockautomation.com/bedrock-advantage/
Bedrock™ has layered and embedded cyber security that begins at the transistor level with secure microcontrollers and memory, hardware accelerators, and random number generation. Bedrock's controller is built upon a secure RTOS, allowing it to continue operating while facing persistent attacks. The Black Fabric™ communication with no I/O pins enables strong anti-snoop protection while sealed all-metal modules keep cyber predators at bay. The only way to open a controller module is with a metal saw, which would trigger the casing sensors to destroy the memory and keep IP safe. The supply chain is also secured via a proven Device Lifecycle Management (DLM) system for supply chains enables all hardware and software used in the control system to be authenticated. This platform cryptography can then be extended and authenticated to third-party software and applications.

**Bus Pirate**
http://dangerousprototypes.com/docs/Bus_Pirate
Bus Pirate is a universal bus interface that talks to most chips from a PC serial terminal, eliminating a substantial amount of early prototyping effort when working with new or unknown chips. Many serial protocols are supported at 0-5.5volts, and more can be added. Protocols include 1-Wire, I2C, SPI, JTAG, Asynchronous Serial, MIDI, PC Keyboard, HD44780 LCD, and UART.

**Cyber Security Evaluation Tool (CSET®)**
https://ics-cert.us-cert.gov/Assessments
The Cyber Security Evaluation Tool (CSET®) is a Department of Homeland Security (DHS) product that assists organizations in protecting their key national cyber assets. It was developed by cybersecurity experts under the direction of the DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). The tool provides users with a systematic and repeatable approach to assessing the security posture of their cyber systems and networks. It includes both high-level and detailed questions related to all industrial control and IT systems.

**Flyswatter 2**
http://www.tincantools.com/JTAG/Flyswatter2.html
Universal JTAG Adapter. Supports USB 2.0 and OpenOCD. ARM compatible with a 20-pin JTAG interface.

**Forensic Analysis of Industrial Control Systems**
https://www.sans.org/reading-room/whitepapers/forensics/forensic-analysis-industrial-control-systems-36277
This whitepaper by the SANS Institute specifically addresses what can be done today to be in a good position to handle malware incidents and attacks on ICS. It covers recommended practices for forensics, network monitoring, logging and response team training. There are several real world examples at the end of the paper.

**GRASSMARLIN**
https://github.com/iadgov/GRASSMARLIN
GRASSMARLIN provides IP network situational awareness of industrial control systems (ICS) and Supervisory Control and Data Acquisition (SCADA) networks to support network security. It passively

maps and visually displays an ICS/SCADA network topology while conducting device discovery, accounting, and reporting on cyber-physical systems.

**HackRF**
https://greatscottgadgets.com/hackrf/
HackRF One from Great Scott Gadgets is a Software Defined Radio peripheral capable of transmission or reception of radio signals from 1 MHz to 6 GHz. Designed to enable test and development of modern and next generation radio technologies, HackRF One is an open source hardware platform that can be used as a USB peripheral or programmed for stand-alone operation.

**IEDScout**
https://www.omicronenergy.com/index.php?id=3953
IEDScout provides access to 61850-based IEDs and offers simulations. Specifically, IEDScout lets users look inside the IED and at its communication. All data modeled and exchanged becomes visible and accessible. It shows an overview representing the typical workflow of commissioning, but also provides detailed information upon request.

**JTAGulator**
http://www.grandideastudio.com/jtagulator/
Universal JTAG Adapter. Supports USB mini and includes a 24-pin JTAG interface.

**National Institute of Standards and Technology National Vulnerability Database (NVD)**
https://nvd.nist.gov/view/vuln/search-results?query=&search_type=last3months&cves=on&uscert_ta=on&uscert_vn=on&oval_query=on
NVD data is freely available from XML Data Feeds. The NVD is updated whenever a new vulnerability is added to the Common Vulnerabilities and Exposures dictionary of vulnerabilities. The vulnerabilities are then analyzed by NVD analysts and augmented with vulnerability attributes (e.g., vulnerable versions) within two-business days.

**Nmap**
https://nmap.org/
Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Systems and network administrators have also used it for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what OS (and OS versions) they are running, what type of packet filters/firewalls are in use, etc. It was designed to rapidly scan large networks, but also works against single hosts. Nmap runs on all major computer OS, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

**NooElec SDR**
http://www.nooelec.com/store/sdr.html
SDR radio hardware for anomaly detection. NooElec manufactures a variety of SDR: Nano2, XTR, Mini2+, Mini2.

**Offensive Security's Exploit Database**
https://www.exploit-db.com
The Exploit Database is a Common Vulnerabilities and Exposures compliant archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability

researchers. The database is a repository for exploits and proof-of-concepts rather than advisories, making it a resource for those who need actionable data quickly.

**OpenOCD**
http://openocd.org/
Universal JTAG Adapter (software). When paired with debugging adapter (physical module), this softare Software provides boundary-scan testing, debugging, and in-system programming for target embedded components. OpenOCD supports a USB and serial dongles.

**Owl 0PDS-5D**
http://www.owlcti.com/network-security-solutions.html#opds-5d
The OPDS-5D was developed as an entry level data diode solution to address cybersecurity use cases with lower, fixed bandwidth requirements of 5 Mbps or less. The OPDS-5D provides deterministic, one-way transfer and effective network segmentation. The OPDS-5D features a compact DIN Rail form factor designed specifically for a range of industrial and commercial applications, from climate controlled IT centers to indoor/outdoor environments with extreme temperatures, dust or smoke.

**PLC Checker**
http://www.itris-automation.com/plc-checker/
PLC Checker automatically analyzes PLC programs and comprehensively verifies their compliance with generic rules and, if needed, rules specific to an industry or a given process. In a customer / supplier relationship, PLC Checker sets the level of quality to be achieved and the way to demonstrate compliance to meet the requirements of the standards, such as ISO / IEC 9126, CMMi (Capability Maturity Model + Integration), FDA, and the nuclear industry.

**Procentec ProfiTrace**
https://procentec.com/products/profitrace/?content-1
A mobile analyzer for PROFIBUS networks, ProfiTrace is a portable tool that can be used by service, maintenance, and engineering technicians for maintenance and troubleshooting. It combines the following tools to detect several PROFIBUS faults: bus monitor, oscilloscope, bar graph, topology scan, reporting, and DP master. The tool can easily identify typical failures such as noise, voltage drops, termination problems, double addresses, wire breaks, and configuration faults. Results can be exported to detailed reports, allowing for predictive maintenance and asset management.

**RFCat**
https://int3.cc/products/rfcat
https://bitbucket.org/atlas0fd00m/rfcat
The RFCat USB Radio Dongle is capable of transmitting, receiving, snooping, and SpectrumAnalysis on frequencies between 300-928MHz giving the user the ability sniff or attack any wireless data protocols that transmit in those frequency ranges. These include: home automation systems, smart meters, SCADA systems, Internet of Things devices, mobile devices, etc.

**SerialTap**
https://www.dhs.gov/sites/default/files/publications/csd-ttp-technology-guide-volume-2.pdf
The SerialTap is a small, embedded device that is placed passively in-line on the legacy links between process control devices. It collects the data sent between the devices, determines message boundaries, and transmits those messages via a secure UDP packet. It is designed to encapsulate data and transmit it to a centralized location to leverage current enterprise analysis solutions, such as cyber security incident and event management systems.

**Sophia**
http://www.prweb.com/releases/2015/10/prweb13025083.htm
Sophia is a passive scanning tool designed for ICS networks. Sophia graphically lays out a map of the ICS network and includes packet filtering by protocol and device. Packets can be saved and reviewed later similar to other network scanners.

**SparkCognition, Cognitive Infrastructure**
https://sparkcognition.com/
SparkCognition offers three products: DeepArmor, SparkPredict®, and SparkSecure®. DeepArmor, leverages machine learning, natural language processing, and artificial intelligence (AI) algorithms to analyze files and provide signature-free security. SparkPredict® learns from sensor data, identifies impending failures before they occur, and alerts operators to sub-optimal operation before it can cause any harm. SparkSecure® adds a cognitive layer, increasing the operational efficiency and knowledge retention of incident response and security analyst teams.

**Vulnerability Intelligence Manager**
http://learn.flexerasoftware.com/SVM-EVAL-Vulnerability-Intelligence-Manager
Vulnerability Intelligence Manager is a vulnerability databases covering more than 50,000 applications and systems across all platforms. It tracks all software vendors and products, including industrial control systems. Vulnerability Intelligence Manager includes a comprehensive set of management features to drive alerts, risk assessment, mitigation, verification, and continuous reporting.

**Wiggler**
http://www.macraigor.com/usbWiggler.htm
The usbWiggler™ is a mid-cost interface used in the design, debug, and programming of microprocessor based embedded systems. One side of the usbWiggler interfaces to the USB port of a host IBM compatible PC and the other side connects to an On-Chip Debug port of the target system. This port may be JTAG, E-JTAG, OnCE, COP, BDM or any of several other types of connections. When connected to a USB 2.0 or USB 3.0 port on the user's PC, the usbWiggler will operate up to Hi-Speed USB rates (480Mb/s).

**YardStickOne**
https://greatscottgadgets.com/yardstickone/
YARD Stick One (Yet Another Radio Dongle) can transmit or receive digital wireless signals at frequencies below 1 GHz. It uses the same radio circuit as the popular IM-Me. The radio functions that are possible by customizing IM-Me firmware can be accessed by attaching YARD Stick One to a computer via USB.