The Cybersecurity Challenges in **Critical Infrastructure**

Addressing the unique demands of critical infrastructure protection in the face of increased cyber threats

BLUVECTOR®

Contents

Critical Infrastructure at Risk

Critical infrastructure covers a vast array of systems that modern societies rely on to ensure safety, security and service. The U.S. Department of Homeland Security deems 16 sectors (*dhs.gov/critical-infrastructure-sectors*) as critical as their failure to function would jeopardize public health and economic security. These industrial sectors include chemical, physical facilities, communications networks, critical manufacturing, defense, industrial, emergency services, energy, dams, financial services, food & agriculture, government facilities, healthcare, IT, nuclear materials, transportation and water and waste system.

Given the wide scope of these critical areas, each comes with their own unique challenges regarding information they utilize to ensure services—to both citizens and businesses, that rely on stability in order to prosper. Yet, they do have one thing in common, an increase in destructive malware attacks in recent years; as damaging any of these sectors can greatly affect a society.

Governments are well aware of the growing issue of infrastructure attacks. A quote which began with then Secretary of Defense Leon Panetta in 2012 has been repeated throughout government, most recently by Ret. Adm. James Stavridis telling CNBC, "We're headed toward a cyber Pearl Harbor, and it is going to come at either the grid or the financial sector"

Industrial control systems (ICS) and critical infrastructure are common targets for cybercrime, with almost 40% of them facing a cyber-attack at some point in the second half of last year.[1]

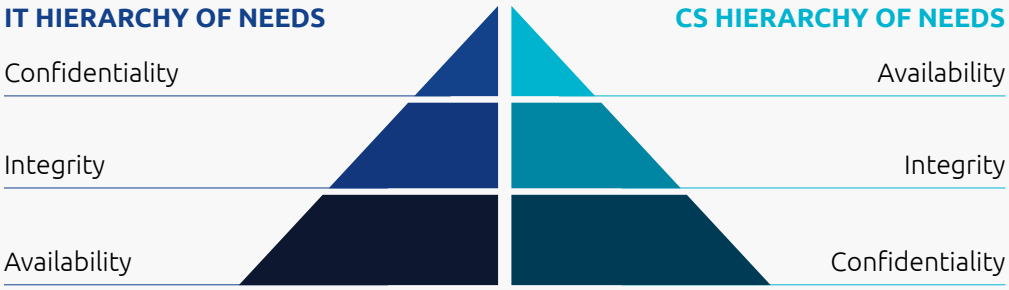
> "We're headed toward a cyber Pearl Harbor, and it is going to come at either the grid or the financial sector."
>
> *– Ret. Adm. James Stavridis*

[1] *https://www.infosecurity-magazine.com/news/40-of-ics-critical-infrastructure/*

Critical Infrastructure Differs from IT

With critical infrastructure, there are two unique systems that often run contrary to one another to enable support and reliability. While many commercial sector organizations offer IT infrastructures to ensure productivity and compliance, many critical infrastructure sectors will often utilize proprietary Control Systems (CS) that run on general purpose operating systems. This method helps to isolate these systems from unintentional updates by vendors, OS creators or outside hacks.

Understanding the challenge boils down to the hierarchy and goal priorities of each:



IT Goal: Confidentiality
Network security must protect private data.

CS Goal: Availability
Operations must survive special conditions and install configurations test and management w/out a shutdown.

The recent growth of the Internet of Things (IoT) in manufacturing operations means that more of these sectors are adopting commercial operating systems such as Windows. There are gains of scale, lower cost and refinement of operations through data and control for manufacturing. Industrial applications still rely on programmable logic controllers (PLC,) and distributed control systems (DCS) are slower to catch up as these systems were created for reliability -- but still lack a similar renown for security. For sectors that use implementations of both IT and CS, or a hybrid of both, can increase the vectors of attack.

According to a 2017 report published in the Journal of Cyber Security Technology (Ani et al. at 44), essentially all ICS infrastructures are vulnerable to attack for reasons including:

- ⚠ The replacement of traditional controllers of CS with OS and micro processing devices
- ⚠ Adoption of internetworking technologies
- ⚠ Use of commercial OS (COTS), which have open designs and standards
- ⚠ Increased size and functionality of systems
- ⚠ Dependency on highly trained IT staff
- ⚠ Inability to shut down operations for upgrade
- ⚠ Employment of low memory or processing ability, which runs counter to security needs

Tackling CI Challenges with BluVector

Challenge: Segmentation

As with any governmental classification, there are many guidelines, rules and regulations around the use of IT and CS within these industries, designed to lower the potential for breaches and catastrophic events. Regulatory compliance (NERC CIP CIP-005/007, HIPAA technical safeguards), industry-specific security reference architectures (IEC 62443, Cisco GridBlocks) and security frameworks (NIST, CIS) encourage segmentation and threat detection.

Personally identifiable information (PII), proprietary data, and safety concerns of adversaries manipulating control system traffic result in their IoT networks being segmented from enterprise or DMZ networks. Sensitive IoT networks, such as hydraulic weapon system platforms or utility substations, will have minimal to no external connectivity with the outside world. This reduces the effectiveness of traditional next-generation security appliances or those technologies leveraging cloud-based reputational services.

Due to the utilization of legacy devices (embedded Windows CE, XP, 7 operating systems), their usability and reliability can, at times, be reprioritized over security. Therefore, these devices may simply be placed in an 'IoT' virtual LAN without even the marginal protections of a firewall. This is even more common in the traditional enterprise networks for ancillary devices, such as conference video systems, HVAC, bar-code scanners, multi-function printers and smaller smart devices.

Customers who use segmentation, or require it due to regulatory compliance, can benefit from adding BluVector to their infrastructure. BluVector sits passively upstream of IoT devices providing unprecedented visibility into all traffic that enters or leave the network segment. Our patented, supervised machine learning technology detects malware targeting Windows, Mac OS X, Linux and Android operating systems, not to mention support for common file types, within milliseconds. BluVector's ability to detect cyber-attacks upon delivery has led to our award of the Department of Homeland Security Safety Act (*https://www.dhs.gov/science-and-technology/safety-act*) accreditation.

BluVector's patented, supervised machine learning technology detects malware targeting Windows, Mac OS X, Linux, and Android operating systems, not to mention support for common file types, within milliseconds.

Challenge: Network Monitoring

Insecure protocols with known vulnerabilities (e.g., Modbus, DNP) or lack of encryption are widely utilized throughout the IoT space. Protocol selection amongst vendors and the industry has become political, influenced by lobbyist and special interest groups (Industrial Internet Consortium, IPSO Alliance, etc.). Unfortunately, network monitoring of even the oldest of IoT protocols are still in their infancy as many of them leverage proprietary extensions or modified to a non-standard state. This reduces the effectiveness of defenders to detect enumeration attempts and exploitation attacks.

BluVector's placement within a network and additional network analytics capabilities support the monitoring to ensure detection coverage of all devices including IoT and mobile. Leveraging a targeted logging functionality, defenders can easily deduce who an affected system has been communicating with before and after the event up to a 15-minute duration. No longer do analysts need to pivot to an additional platform (such as a SIEM or IPS), nor open a service ticket with the networking team to review NetFlow data. As BluVector is not a closed-box appliance, customers have full access to our modified Bro configuration allowing them to run their own scripts or IoT-specific policies. Additionally, BluVector learns about the IoT network once connected and adjusts its detection based upon traffic observed. This ensures each BluVector appliance is unique per region, network segment and even use case.

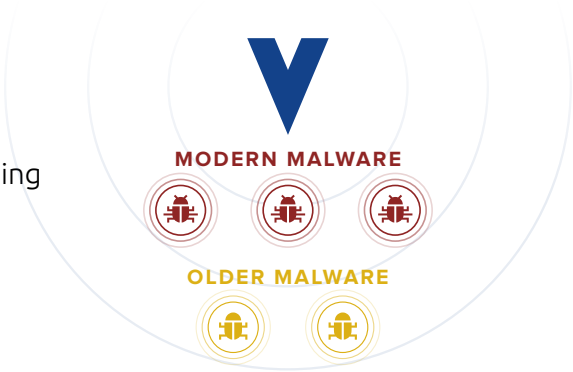
BluVector's placement within a network and additional network analytics capabilities support the monitoring to ensure detection coverage of all devices including IoT and mobile.

Challenge: Known Malware & Exploit Detection

The ability to detect older malware and known exploits via signature-based and file white-listing solutions still have their place, especially in IoT networks that contain legacy, embedded devices. Traditional anti-virus solutions are often a regulatory compliance requirement as they can reduce common infections impacting unsuspecting users without needing to invoke the incident response process. As an example, the Conficker worm (2008) is still one of the leading threats to legacy, Windows-based industrial control system networks.

BluVector supports network and host-based signatures, as well as integration with threat data and Indicator of Compromise publishers (e.g., ThreatConnect, Threat Stream, STIX/TAXII). Leveraging YARA, ClamAV, and Snort-style network signatures, your team can easily detect known threats while allowing BluVector's patented, machine learning technology to identify previously unseen malware at line rate speeds. BluVector has undergone multiple malware detection rate and performance tests, which validates our ability to immediately detect malware.

As our supervised machine learning model has been trained on hundreds of millions of malicious and benign files, BluVector can even detect older malware that is no longer being pushed to endpoints via bulky signature updates. For organizations leveraging traditional network Intrusion Detection Systems (IDS), we've incorporated Suricata IDS within our platform, so users can still leverage their existing data loss prevention, DoD classification marking detection, or custom network signatures.



Challenge: Detect Unknown & Zero Day Attacks

Fileless and ransomware attacks are evading traditional detection mechanisms as they often require user interaction. Firmware attacks, as observed in Ukraine's Power Grid, and the threat of malicious over-the-air updates require more than traditional sandboxing technologies. In fact, their virtual emulators may not even support the targeted IoT device's operating system.

BluVector leverages supervised machine learning and network emulation analytics for file-based and fileless detection. The solution comes preconfigured with its own training library based on over 100 million samples obtained from public and private repositories. Unlike unsupervised machine learning offerings, BluVector is ready to detect suspicious events following a 30-minute configuration. We support many operating systems, including legacy Windows executables and Linux binaries. For all others, including real-time operating systems (e.g., VxWorks), BluVector's HuRI engine easily detects botnet traffic leveraging randomly-generated domain algorithms while the underlying Bro functionality alerts to files with high entropy, such as ransomware or compressed intellectual property being exfiltrated.

The Risk is Real

On Aug. 22, President Donald Trump's National Infrastructure Advisory Committee released a draft report on the threat of cyberattacks on the nation's critical infrastructure. As NIAC said so eloquently:

> "There is a narrow and fleeting window of opportunity before a watershed, 9/11-level cyber-attack to organize effectively and take bold action."

While this warning may seem "apocalyptic," it is by no means inflated. The risk is real and increasing.

The potential for disruption of critical infrastructure industries poses a unique and existential risk. These industries include, but are not not limited to:

FINANCIAL INDUSTRY | **TRANSPORTATION INDUSTRY** | **HEALTH INDUSTRY** | **FOOD INDUSTRY** | **WATER INDUSTRY** | **POWER INDUSTRY**

This critical infrastructure -- which is designed generally to meet end-user expectations related to both low cost and reliability -- is often "static." Taking down systems to patch or upgrade is both costly and disruptive. In some industries -- like health care -- where IT is responsible for the delivery of life-saving/continuing services, such management is impossible.

There is pressing need to improve security and protection of particularly vulnerable targets. As the committee stated, "The U.S. government and private sector collectively have tremendous cyber capabilities and resources to defend critical private systems from aggressive cyberattacks -- provided they are properly organized." We should "use this moment of foresight to take bold, decisive actions." ▼

BLUVECTOR®

BluVector has reinvented network intrusion detection with machine learning so that it can finally deliver on its promise: defend the network against even the newest and most sophisticated cyberattacks. Unlike today's security solutions that rely on a known signature, sandbox or post-breach evidence of infection, BluVector accurately finds and prioritizes all threats at the point of delivery, enabling organizations to defend against cyber threats before damage can be done. BluVector has invested 8 years in training its patented, machine learning-based detection and intelligent decision support engines to enable security analysts to find, confirm, and contain even the newest and most sophisticated threats.

Learn more about BluVector

www.bluvector.io • 571.565.2100