Pacific Northwest
NATIONAL LABORATORY

SECURING THE **GRID** WITH **CYBERSECURITY** TECHNOLOGIES

The latest grid cyber technologies and tools from Pacific Northwest National Laboratory can:

- Determine grid vulnerabilities and other factors that might allow adversaries to take control of complex systems
- Support development of mitigation strategies to minimize the impact of cyberattacks on grid assets
- Detect possible incursions and stop them before they damage grid resources
- Assess cybersecurity in a product development lifecycle.

The tools described in this brochure were developed and tested by a variety of users, including utilities, independent system operators, regulators, commercial vendors, and other grid stakeholders.

1 Cybersecurity Maturity Models to Identify Gaps and Vulnerabilities

3 Cyber-Physical Security and Visualization Tools for Risk-Informed Decision-Making

5 Technologies to Prevent, Detect, and Defend Against Cyber Events

9 Blockchain Technology Applications to Secure Data Systems

CYBERSECURITY MATURITY MODELS

to Identify Gaps and Vulnerabilities

Secure Design and Development Cybersecurity Capability Maturity Model (SD2-C2M2) | 31581

Intertwines management and technology requirements for secure design and development

A key challenge in creating resilient systems is factoring in cybersecurity needs throughout the development process. SD2-C2M2 is an integrated tool that enables developers to design hardware and software for critical infrastructure against designated cybersecurity maturity levels. The tool can compare maturity levels against a set of management-derived requirements to identify the need for hardware and software improvements as the devices are being developed. The easy-to-use framework features a graphical user interface that allows a user to select a subset of best practices for evaluating to evaluate the technology's cybersecurity maturity. SD2-C2M2 is the only approach that intertwines management priorities with technical and security controls.

How SECURE are your DESIGNS?

2

Cybersecurity Framework Tool | 31293, 31346

Equips organizations to better manage cyber risk in the face of evolving threats

Cyberattacks plague organizations around the world, but the evolving nature of cyber threats ties the hands of cyber defenders in government and industry. The Cybersecurity Framework Tool equips organizations to better manage cyber risk, continuously improve their cybersecurity posture, and train operations technology and information technology staff on cybersecurity standards and best practices. The tool includes a Cybersecurity Training Game Simulator for training to train staff and equipping them to train others within their organizations, based on interactive scenarios that incorporate major U.S. cyberattacks experienced in the last 10 years. The easy-to-use, repeatable, holistic approach builds a culture that addresses the dynamic nature of cybersecurity risk. The Cybersecurity Framework Tool facilitates implementation of the May 2017 Presidential Executive Order (EO) on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, which calls on federal agencies and critical infrastructure owners and operators to manage their cyber risk through adoption of the ***Framework for Improving Critical Infrastructure Cybersecurity*** developed by the National Institute of Standards and Technology (EO 13636 and EO 13800).

Self-assessment tools for hardening your facilities against cyberattacks

Cybersecurity Vulnerability Mitigation Framework through Empirical Paradigm (CyFEr) | 31582

Discovers vulnerabilities and threats and identifies the ideal path for achieving a desired security posture

In a typical hardware-centric organization, such as a power utility, information technology and operations technology networks are equally important and are designed with firewalls between them that only a network administrator can navigate. If a cyberattack compromises administrator credentials, the attacker can bring down the entire system, potentially resulting in loss of power, infrastructure damage, and loss of life. CyFEr identifies critical vulnerabilities and gaps between information technology and operations technology and prioritizes requirements to reach the desired cybersecurity maturity. CyFEr's built-in optimized threat filters can be used to not only tailor the discovered vulnerabilities in relationship to the business policies but also precisely identify the most critical threats in relationship to those vulnerabilities. CyFEr can ingest various organizational bounds, such as cost and time limitations to generate ideal mitigation paths to achieve the desired cybersecurity maturity.

CYBER-PHYSICAL SECURITY AND VISUALIZATION TOOLS

for Risk-Informed Decision-Making

Framework to Analyze Cybersecurity Risks and Consequences for Critical Infrastructure (FRisC) | 31694

Analyzes the consequences of cybersecurity vulnerabilities for risk-informed decision-making

Current cybersecurity vulnerability assessments are missing a critical piece: the ability to analyze risks and consequences. Without information derived from such analysis, organizations cannot design programs that reach a desired security posture. FRisC identifies critical assets and their relationships to business processes, then analyzes the consequences of a disruption of those processes. Designed specifically for the power industry,

the framework takes a multi-dimensional approach that enables FRisC to be used as a standalone system or in line with existing systems to analyze risks and consequences for decision-makers. FRisC's unique means of connecting business functions with engineering processes to identify the value-at-risk and consequences makes the technology scalable and applicable to other critical infrastructures beyond the power industry.

Risk Model for Autonomous Adaptive Cyber Controllers | 31282, 31407

Factors business operations and risk into cyber control

To help operations technology systems prevent, mitigate, and respond to cyber threats and events, some utilities are considering using adaptive cyber controllers that detect incursions and trigger defenses. What is often missing is a risk assessment. PNNL's risk model interfaces with cyber controllers to determine the expected impact of a cyber incursion on operational functions based on a list of potential cyber network reconfiguration alternatives. The model then characterizes trade-offs so that operators can take informed actions to prevent progression of an attack and minimize business disruption.

Operations Technology Cybersecurity Visualization Tool | 31612

Improves situational awareness and assessment in control rooms

Providing cybersecurity in control rooms for operations technologies is challenged by a lack of common taxonomy among control room operators and cybersecurity professionals. The Operations Technology Cybersecurity Visualization Tool bridges the communication gap and improves situational assessment and awareness for operators and cyber experts. The tool allows them to work together to assess a situation and determine the best outcomes. It has been tested in an operational setting and enabled adequate communications for cybersecurity issues to be addressed. Because the tool is html-based, it can be used by any control center and cybersecurity operations center.

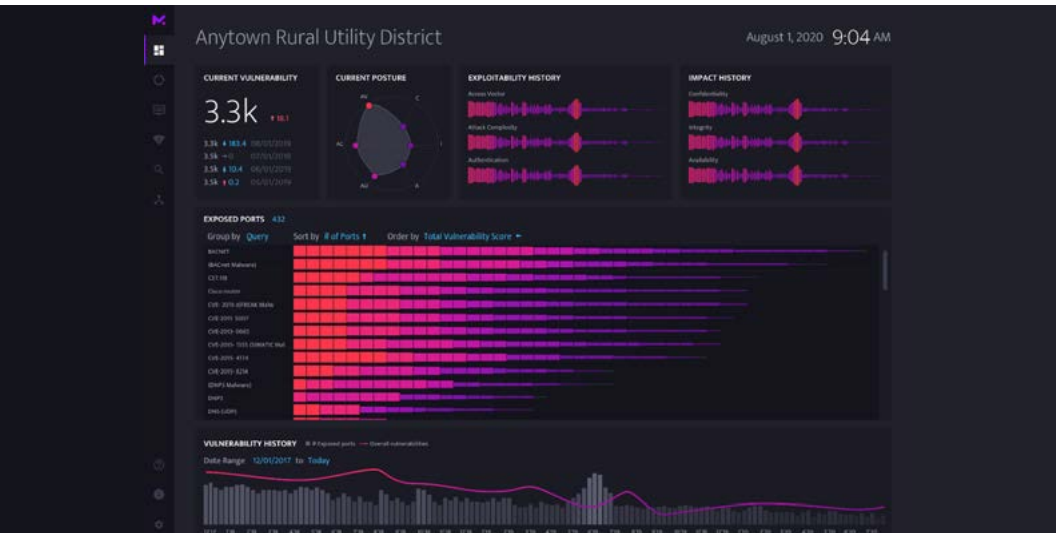
TECHNOLOGIES TO PREVENT, DETECT, AND DEFEND

Against Cyber Events

Mitigation of External Exposure of Energy Delivery Systems (MEEDS) | 31731

Identifies energy delivery system technologies that are externally exposed that currently may have little protection

Operations technologies, industrial control systems, devices, and energy delivery systems are inadvertently externally exposed, where threat actors can exploit them to gain control of critical networks and systems. MEEDS provides an effective, affordable, and easy-to-use cyber-risk management system designed specifically for energy utilities. The advanced cyber defense technology offers a defense-in-depth solution to mitigating externally exposed energy delivery systems without degradation or disruption of services. It can distill data from Shodan, one of the world's largest public database and search engines, which is used by more than 50 percent of Fortune 1000 companies. It provides advance identification for important operations technologies, industrial controls systems, and other systems, that are exposed and vulnerable to outside threats.



Integration of Green Renewable Energy Sources Securely (INGRESS) | 31449, 31450

Prevents malicious control commands on distributed energy sources

Control systems may issue messages alerting building and grid owners and operators about cybersecurity problems, but nothing defines whether those problems could result in unsafe or unstable conditions or shorten equipment lifetimes dramatically. INGRESS is an advanced attack detection and resiliency-enabling cybersecurity platform for behind-the-meter distributed energy resources. It can be deployed within legacy and emerging energy system environments to establish and verify the behaviors of devices, information, and command sequences. The platform builds and continuously improves models of the equipment that it protects, and it automatically prevents malicious control commands or operations in real time. The platform also supports secure communication with other systems and utilities.

Threat Model-Based Response (TMBR) | 31676

Identifies defensive techniques even for unique malware

Malware can extract a heavy toll on systems, but fighting it means determining how to defend against each piece of malware and ultimately attributing the source to prevent future incursions. Both approaches can prove challenging for most organizations. TMBR reduces these challenges by linking behaviors of particular types of malware to known threats as well as successful defensive techniques. The technology uses hierarchical data clustering to identify common patterns and distinguish behavioral characteristics. This approach is particularly useful when confronted by malware that has unique features that may be otherwise difficult to predict.

The Cymbiote | 31551, 31560

Detects cyberattacks in embedded field devices for real-time event recovery

Embedded field devices that sense and control physical processes in critical infrastructure are soft targets for cyberattack because they lack the fundamental features for cybersecurity monitoring and control. A combination of hardware and software, and the only device of its kind, The Cymbiote collects data from multiple sources, synthesizes them to detect events of importance, and enables dynamic and real-time device reconfiguration for event recovery. It includes hardware to replace the Y cable to allow data to flow between pieces of equipment without disrupting normal operations or communications.

Shadow Figments | 31305

Generates deceptive systems to foil cyberattacks on control systems

Deception is an approach to cybersecurity defense that slows attackers by diverting their attention and increases detection when attackers interact with the deceptive systems. Because control systems rely on physical rather than data processes, this approach is difficult for them to mimic, allowing attackers to easily reengage and penetrate the real system. Shadow Figments generates and runs high-fidelity deceptions of control systems. Using a model of the real process, the software generates controllers and sensors that respond to an attack in realistic ways to deceive intelligent attackers targeting control systems.

End-to-End Segmentation Via Containerization and Network Labeling | 31230

Protects all business systems while maintaining efficiencies

Critical business systems are often protected by the defense-in-depth approach—use of layers of defensive controls to prevent unauthorized access. However, in trying to retain the efficiency of less critical systems, industry may strip away these layers and leave a path through which adversaries can access more important systems. End-to-End Segmentation Via Containerization and Network Labeling creates containers around processes and allows each process to communicate with the others via labels that provide important contextual information. When an incursion is detected, the technology can dynamically alter network behavior to prevent any damage. This technology enables a level of segmentation never before possible, while providing strong protections that prevent threats to one business process from impacting other processes. All the while, the technology keeps processes agile and efficient.

Kritikos/Caddy | 30649, 30720

Determines cyber dependencies to help recover from cyberattacks

Cyber defenders in an industry are often unaware of dependencies between various information technology assets. Kritikos/Caddy automatically discovers the relationships among assets using pattern recognition of network monitoring data. The technology uses an artificial neural network that groups and labels patterns to pinpoint dependencies. Understanding dependencies gives an organization better situational awareness and the ability to assess, triage, and recover from cyberattacks. Such knowledge also supports planning for business continuity, disaster recovery, and development of infrastructure investment strategies.

BLOCKCHAIN TECHNOLOGY APPLICATIONS

to Secure Data Systems

Blockchain Applicability Framework (BAF) | 31608

Determines whether and recommends which blockchain features are valuable

Blockchain technology has been gaining great interest from a variety of industry sectors, including the financial, food processing, and power and energy markets. The strength of blockchain technology is being realized beyond its successful application in the cryptocurrency arena. Emerging applications include supply chain management, transactive industry (both financial and energy), system integrity, device cybersecurity, identity management, and many more. BAF evaluates the requirements of an application or use case and precisely determines what kind of blockchain features are most valuable or whether the application even needs a blockchain. BAF is divided into five domains, 18 subdomains, and about 100 controls. It ingests detailed user requirements to perform a weighted evaluation built on mathematical constructs to determine the ideal combination of blockchains appropriate for an application.

Blockchain Cybersecurity Audit Platform (BCAP) | 31540

Automates security audits and NERC compliance, and enforces supply chain and patch management

Assessments of cyber vulnerabilities in energy delivery systems are largely manual, expensive, incomplete, and ineffective. BCAP helps reduce costs and increases the effectiveness of grid cybersecurity efforts by automating security audits and compliance with North American Electric Reliability Corporation (NERC) critical infrastructure protection requirements. The blockchain technology cryptographically monitors the movement of critical cyber assets throughout their entire chain of custody, including monitoring the integrity of the devices when they are deployed. Focused on energy management systems and distribution

management systems, BCAP detects integrity violations and data tampering whether the data are stored or in transit. It automates the audit process to provide a clear, traceable chain of custody for energy assets. In addition, BCAP can be used to ensure secure configuration management (baselining, patch management, and vulnerability management) and to maintain a tamper-proof chain of custody of the assets throughout their supply chain and lifecycle.

Blockchain-Based Cybersecurity Solution (BCS) | 31611

Secures data and prevents cyberattack propagation

Software programs called data historians store vast amounts of data related to industrial control systems, but if these data stores become corrupted by a cyberattack, adversaries can disrupt the operations of these important control systems. Using blockchain technology, BCS protects data historians from spoofing, corruption, or destruction by creating a copy of the data set and storing it in an immutable database using a unique hash value. When cyberattacks are suspected, the program can compare the hash value between two data sets to determine which is uncorrupted. BCS can secure data-at-rest and data-in-transit and autonomously register, verify, and trace data. It works with field measurements, device states, and syslogs/alerts. System registration and system-to-system verification in the blockchain could also prevent an attack from propagating further.

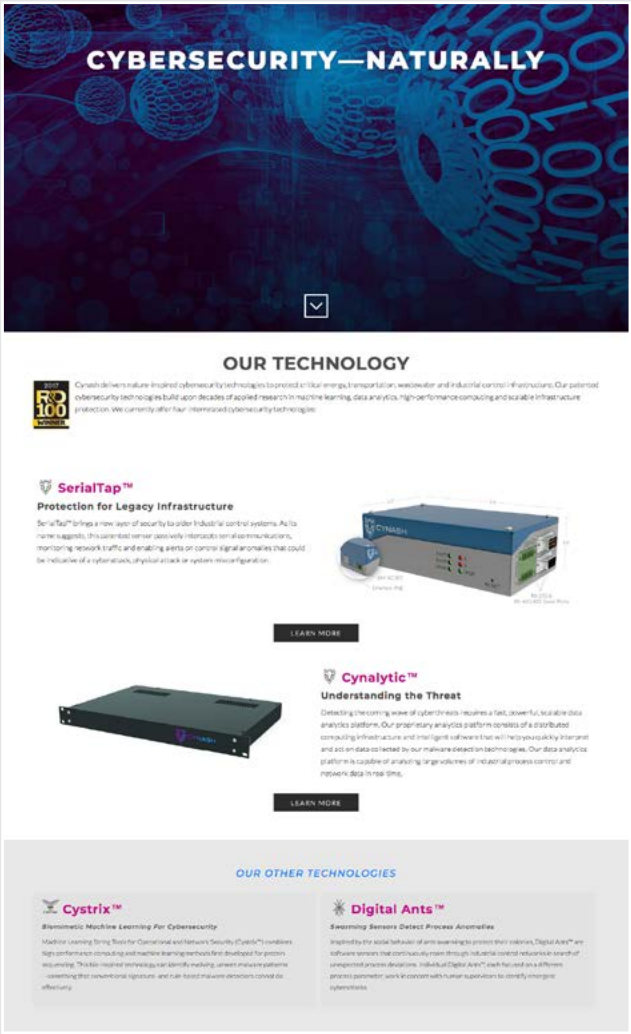
SUCCESS STORY

Startup Takes on Cyberattacks

Our grid technologies for cybersecurity transition well to the market. For example, IP Group, an intellectual property commercialization company, started Cynash, Inc. specifically to commercialize three of our technologies: MLSTONES, which stands for Machine Learning String Tools for Operational and Network Security; Digital Ants; and SerialTap.

MLSTONES applies the power of high-performance computing to vast amounts of data to identify evolving malware threats. Digital Ants are embedded sensors that hide from surveillance when not being used and monitor networks from device to device to detect suspicious behavior and alert users and other systems to take appropriate action. SerialTap allows serial communications to be cloned and then analyzed by ethernet-based security tools.

Cynash has incorporated these unique technologies into a comprehensive and compelling cyber-defense solution that will address the ever-increasing threat of these costly attacks.



WORKING WITH US

Although these innovative tools are protected by proprietary copyrights and pending and issued patents, they are available through commercial licenses. We also offer a low-cost, six-month exploratory research and option agreement to "test-drive" these technologies.

At PNNL, we can collaborate with you to customize these tools for your systems and needs. We can test, demonstrate, and integrate technologies at your site or ours. A specialized facility—the Electricity Infrastructure Operations Center—is available on the PNNL campus in Richland, Washington. It integrates industry hardware and software, real-time grid data, and advanced computation in three functional control rooms with a dedicated server farm. This facility is available via physical and remote access to utilities, vendors, government agencies, and universities for development, integration, verification/validation, testing, and training purposes.

Pacific Northwest
NATIONAL LABORATORY

ABOUT PNNL

Interdisciplinary teams at Pacific Northwest National Laboratory address many of America's most pressing issues in energy, the environment, and national security through advances in basic and applied science. Founded in 1965, PNNL employs more than 4,400 staff and has an annual budget of nearly $1 billion. PNNL is managed by Battelle for the U.S. Department of Energy's Office of Science.

PNNL is a recognized leader in electricity infrastructure, transactive controls, cybersecurity, and buildings research. We collaborate with industry, utilities, universities, and government to improve the resilience, reliability, and security of the nation's electricity delivery system.

You can view all of our innovations available for commercialization at availabletechnologies.pnnl.gov.

CONTACT

Peter Christensen
Senior Commercialization Manager
509.371.6159
peter.christensen@pnnl.gov

U.S. DEPARTMENT OF
ENERGY

PNNL-SA-149987