Pacific Northwest
NATIONAL LABORATORY

CYBERSECURITY SOLUTIONS

For Critical Operational Technologies

Cybersecurity technologies and tools from Pacific Northwest National Laboratory can:

- Determine 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 critical infrastructure, such as buildings, the electric grid, water and sewage systems, and even pipelines.
- Detect possible incursions and stop them before they damage critical infrastructures, such as electric transmission and distribution systems.
- Assess cybersecurity in a product development lifecycle.

The technologies and tools described in this brochure were developed and tested by a variety of users, including utilities, cybersecurity consultants, system operators, and stakeholders, as well as industry collaborators.

CYBERSECURITY MATURITY MODELS

to Identify Gaps and Vulnerabilities

Secure Design and Development Cybersecurity Capability Maturity Model (SD2-C2M2) | 31581, 31858, 31859

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 the user to select a subset of best practices to evaluate the technology's cybersecurity maturity. SD2-C2M2 is the only approach that intertwines management priorities with technical and security controls.

Cybersecurity Framework Tool | 31293, 31346, 32094

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 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.

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.

Federal Emergency Management Program (FEMP) Cybersecurity Arsenal | 31949

Evaluates threats in federal facilities

A comprehensive suite of software solutions for identifying threats in federal facilities has been developed through the Department of Energy's FEMP. Listed below, these tools are available at no cost to users through a PNNL-sponsored website. However, the goal is to find a licensee that will offer the copyrighted software to industry.

- The Facility Cybersecurity Framework (FCF) is a suite of maturity models for assessing the cybersecurity maturity of facilities based on the National Institute of Standards and Technology cybersecurity framework to help facility owners and operators better manage cybersecurity risks. This tool can perform a standard assessment and generate compliance and maturity scores.
- The FCF-Primer enables the user to conduct a quick review of their facility's security posture before committing resources to a full FCF assessment. The FCF-Primer can be used prior to a more comprehensive assessment or as a checklist during the post-assessment and gap-mitigation phase to track enhancements.
- The Cybersecurity Maturity Model (C2M2) Lite Assessment tool provides flexible guidance to help organizations assess the maturity of their facility's cybersecurity. The dynamic tool adapts and self-customizes questions based on the user's responses.
- The Qualitative Risk Assessment (QRA) tool is designed to assist facility owners and operators performing risk-based asset management. QRA enables asset owners to qualitatively define the estimated vulnerability of an asset and the potential impact if the asset is compromised and categorizes the asset in an appropriate risk bucket—low, medium, or high.
- The FCF Cybersecurity Training Game is designed for a spectrum of facility owners and operators. It provides dynamic, game-based cybersecurity training. Users pick a scenario and are then confronted with a series of real-world cyberattacks on their facility. Cybersecurity resources to thwart the attack are constrained to mimic real-world limitations. Attacks may impact information and operational technology systems.

Automatic Cybersecurity Policy Scoring System (AutoPol) | 32211

Scans and analyzes end-user documents

AutoPol is a software tool that uses natural language processing to scan and analyze end-user documents that contain cybersecurity guidelines and policies and map those against existing cybersecurity assessment and framework tools. The tool enables end-users to automatically identify relevant text segments within a user-provided document that satisfy or address the requirements of a cybersecurity compliance framework policy. The copyrighted software also returns a cumulative score that can be used to assess a document's overall compliance level with respect to the reference policy. Additionally, a set of visualization tools enable the end user to graphically interpret the results and filter out false positives, accelerating compliance reviews—without the need for human resources. This feature reduces the number of resources allocated for compliance evaluations and human-induced errors, which ultimately leads to better assessments.

RISK AND VULNERABILITY ANALYSIS

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 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.

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.

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.

Risk-Informed Verification and Validation Recommendation (RIVVR) | 32178

Evaluates the security risk of electric utility devices

RIVVR is a software tool for evaluating the security risk of specific electric utility devices (e.g., protective relays, PMUs) from procurement, through operation, to disposal. This risk assessment uses a novel approach to incorporating existing standards and risk protocols to provide a single tool for the entire lifecycle of a device or system. This software tool is based on a patented framework that will provide Energy Delivery System stakeholders with a cybersecurity-focused verification and validation (V&V) approach, which includes a list of potentially relevant vulnerabilities to test or address, as well as pre-procurement guidance. RIVVR also provides separate lists of relevant standards, tools, and techniques to be considered by utilities and vendors. The framework will help in conducting a security assessment before procurement, as well as thorough, risk-informed V&V testing on a device at different stages in its product life cycle, which includes pre-purchase, commissioning, operation, and all the way up to disposal of the device.

Cyber Contingency Analysis | 30776

Explores the what-ifs of cyber resilience

While a cyber system may seem in a good state, does it remain so when an element becomes compromised or disabled? To deal with this, power grid operators use a technique known as contingency analysis, in which they observe what the system might look like given a list of possible contingencies and adjust the system so that no violations will occur. The Cyber Contingency Analysis tool applies a similar approach to user accounts or network resources that may become compromised: users analyze possible contingencies and calculate the severity regarding confidentiality, integrity, and availability of data.

PACRAT: Physical and Cyber Risk Analysis Tool | 30318

Identifies vulnerability and risk in critical infrastructure

PACRAT is a first-of-its-kind vulnerability and risk analysis software that identifies vulnerabilities in critical facilities and infrastructures by blending cyber and physical security. Compared to the typical, independently performed cyber and physical vulnerability assessments, which do not account for the interdependence of the security apparatus, PACRAT performs holistic vulnerability analyses and recommends prioritized cyber and physical security upgrades to reduce risk and optimize investments. This both significantly reduces analysis time and produces results driven by a defensible algorithm and modeling software, instilling confidence in security investment decisions.

THREAT DETECTION AND MITIGATION TECHNOLOGIES

to Protect Against Cyber Events

Shadow Figment | 31305, 31883, 31884

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 Figment 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, 31898

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 that 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.

Detection of Attacks on Cyber-Physical System Sensors | 31983

Identifies cyberattacks on infrastructure sensors

The primary objective of this copyrighted tool is to identify cyberattacks on infrastructure sensors (e.g., SCADA or PMU sensors for electric grids) that can spoof the control systems into taking erroneous actions, especially during some other system event in which these attack signals could amplify instability. This tool uses Koopman non-linear analysis methodology to detect cases where an attacker injects a multiplicative signal right after a natural event to introduce oscillations in the system. The impact of this signal injection can cause the system to oscillate widely, even though there is no external fault or attack happening at that time. This tool will allow the system operator to detect such an attack and respond correctly to the given situation to minimize the impact on the system and its customers.

Control System Cybersecurity Network Enumeration and Correlation | 32176

Scans and reviews an electric utility's connected devices automatically

This tool was developed to automatically scan and review an electric utility's connected devices, regardless of age and operating system, to determine cybersecurity vulnerabilities and connectivity issues. It can be used to scan any industrial control system to enumerate and correlate all connected devices from a cybersecurity sensitivity viewpoint. The tool uses passive packet gathering to systematically create a complete list of devices on a sensitive operational network through non-intrusive means, thus, allowing full situational awareness for the operator. This list enables network owners to have an accurate view of their network with no need for intrusive scanning, which may be detrimental to older operational and control equipment. For more robust networks, there is an option for network owners to use tailored active scans for a more thorough analysis of attached devices.

MLSTONES: Machine Learning String Tools for Operational and Network Security | 30751

Includes bio-inspired cybersecurity

Malware is an increasingly prevalent cyberthreat for consumers, business, and government agencies. MLSTONES borrows from biology to convert software code into DNA-like structures and identify code that contains similarities with known malware. MLSTONES applies the power of high-performance computing to vast amounts of biological data being captured to study protein similarity. This biological-based approach allows MLSTONES to recognize evolving, never-seen-before malware by detecting similarities in evolving malware—something that conventional malicious software detectors cannot do effectively.

Trustworthy CPU | 30306

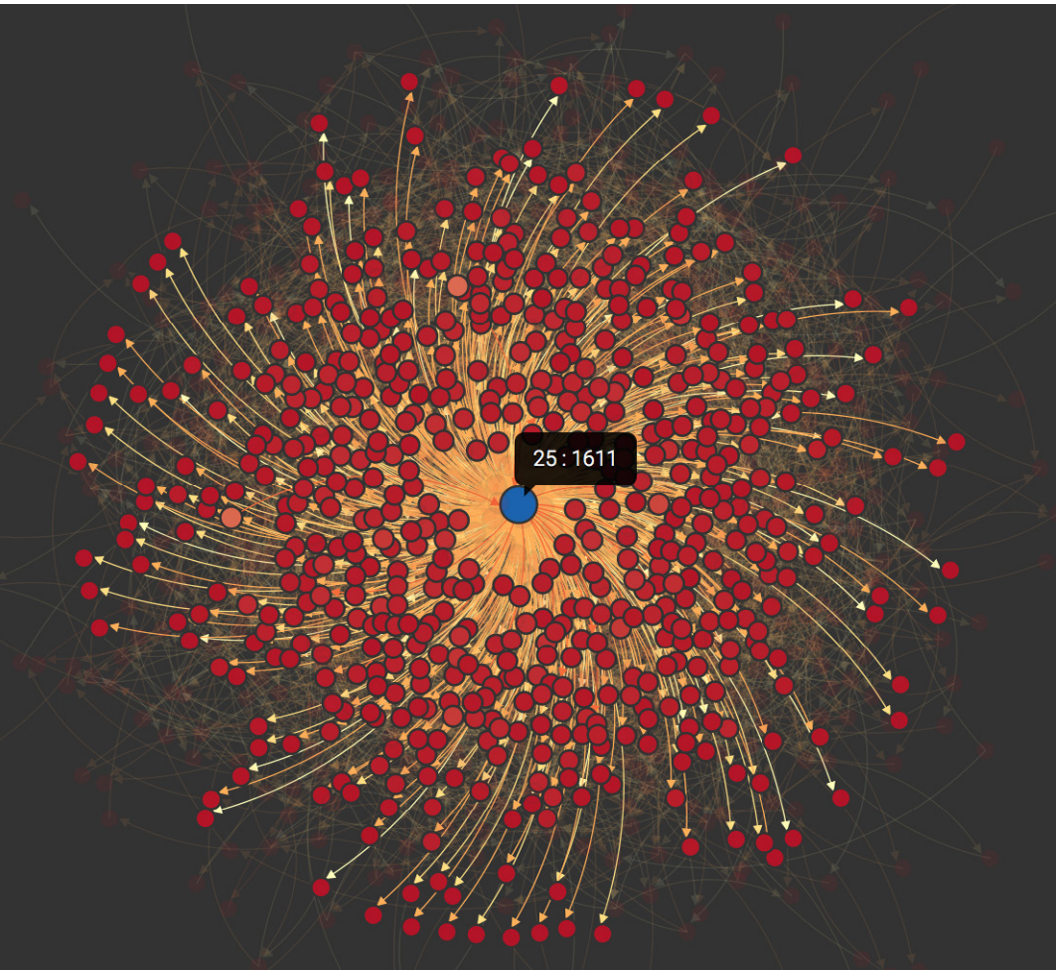
Incorporates encrypted CPU instruction stream

Successful cyberattacks often leverage the fact that an instruction set architecture of a targeted system is well known. Attackers can prepare malicious software, knowing with high confidence that it will run when introduced into the system. A Trustworthy CPU only executes software encrypted for that specific CPU. Perfectly suited for resource-constrained, embedded systems and Internet-of-Things devices, it is immune from code-injection attacks, malicious firmware updates, and many other types of malware. PNNL's patented Trustworthy CPU technology maintains system integrity in the face of increasingly sophisticated attacks—both those known today and those that will be invented years from now.

StreamWorks | 30996, 31083

Continuous pattern detection on streaming data

One hundred forty-six days—that's how long, on average, it takes to detect a cyber breach from the time it begins. StreamWorks cuts that time significantly—to near real time—by detecting emerging patterns of sophisticated cyberattacks in massive data streams. Combining several analytic approaches, never before seen together in a cybersecurity tool, StreamWorks tells a cyber analyst when major suspicious patterns are occurring. The tool also provides a description of the potential threat and a rationale for why the threat was selected—so the analyst does not have to guess but, instead, can act swiftly.



SECURE OPERATIONS SOLUTIONS

to Make Your OT System More Robust and Resilient

Operations Technology Cybersecurity Visualization Tool | 17126, 31612, 32286

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.

CENTS: Cyber Economic Network Transaction Security | 30790

Provides a currency-based transactional economy model

Today's cybersecurity professionals need to understand and secure complex, fast-moving, and changing environments. CENTS provides a currency-based method for securing a network where scarcity serves as a limiting factor to access and engagement within the system. The network is modeled on various economic principles and establishes macro, meso, and micro economies where transactions between users (individuals, groups of people, networks, or functions within the environment) and elements (other users, activities, access, locations, or capabilities) require the tendering and receipt of a circulating currency. A network defender can view the transactions at all levels and manipulate the purchasing power of the currency for various transactions to prevent unwanted access or activity.

Hypergames | 31816

Analyzes cyber-physical security for control systems

The 2010 Stuxnet worm provided a highly publicized example of a cyberattack causing physical damage to an industrial control system. Hypergames present a tool to analyze how adversarial perturbations, like those used by Stuxnet, can manipulate a system that employs optimal control. Hypergames form an extension of game theory to model strategic interactions where the players may have significantly different perceptions of the game(s) they are playing. In the face of information asymmetries and player misperceptions, this approach can be applied to control systems subject to deception-based attacks.

CLIQUE: Correlation Layers for Information Query and Exploration | 30553

Identifies and analyzes cyber threats in real time

CLIQUE is a visual analytic tool that uses data-intensive architectures to provide analysts unprecedented visibility and command of their data. It provides situational awareness of network activity, resulting in efficient investigation to support prevention, response, and mitigation of harmful attacks. CLIQUE is built on a computationally low-cost statistical model, scalable data storage solution, and engaging visual analytics environment.

FLOWER: Network Flow AnalyzER | 14448, 17042

Stems cyberattacks through network flow analysis

Enterprise networks, including those in the cloud, are under constant attack. FLOWER is a software application that uses a passive network tap anywhere in the enterprise to inspect network flows or conversations between computers and help mitigate cyberattacks. FLOWER is a simple but powerful algorithm that parses and aggregates up to one million packet headers per second. FLOWER does not look inside every packet but has ways of determining if it is suspicious and needs further analysis.

Cymbiote | 31551, 31560

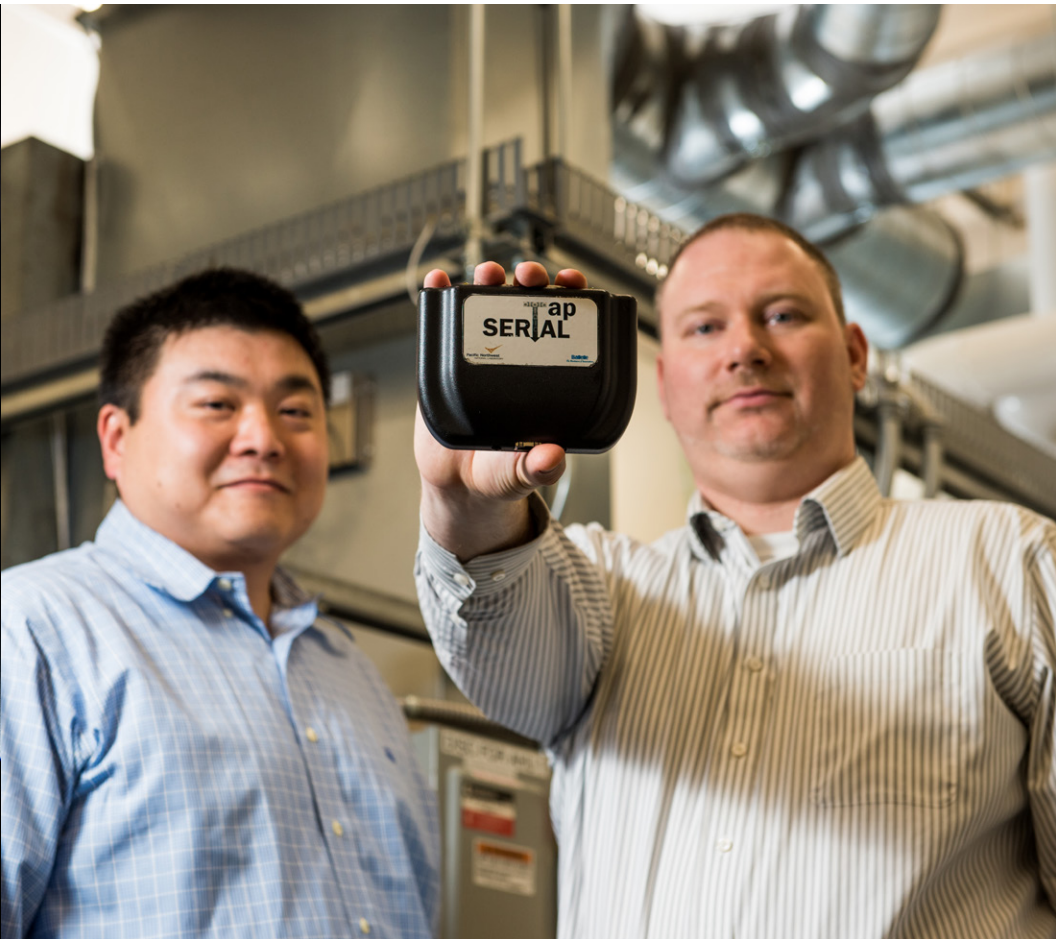
Detects cyberattacks in embedded field devices for real-time event recovery

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, 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.

SerialTap | 16338

Taps into industrial control system cybersecurity

Computer-driven industrial control systems, such as those for power systems, manufacturing, oil, and gas, need cybersecurity solutions for monitoring network traffic and defining against an increasing number of threats. SerialTap does just that by bridging the gap between older, serial-based devices and modern networks in industrial control systems. This low-cost, small device connects to both a control system and the computer network without interrupting system operations. SerialTap translates the data from the control system so that the network cybersecurity software can analyze it, improving a company's situational awareness and response time.



Serebrus/Scalable Reasoning Systems | 17126, 32179, 32286

Provides an analytic framework for web-based visualization

Cyber defenders need a single, consistent, and reliable collection and analysis strategy for information—a system that automatically extracts topics, themes, and trends in the data and visually presents the relevant and emerging threats. Serebrus Scalable Reasoning System is an analytic framework for developing web-based visualization applications. Using a growing library of both visual and analytic components, custom applications can be created for any domain, from any data source. Its modular architecture helps connect data to analytics and visualizations—helping users make sense of data. This technology has been used to create solutions for a wide range of domains, including health care and cybersecurity, incorporating either large or streaming data sets.

DISTRIBUTED LEDGER TECHNOLOGIES

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 5 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.

Threat-Detection Company Licenses Cybersecurity Decoy Technology | 31305

Lures hackers into artificial world

Shadow Figment is designed to lure hackers into an an artifical world, then stop them from doing damage by feeding them illusory tidbits of success. The aim is to sequester bad actors by captivating them with an attractive but imaginary world. Shadow Figment is designed to protect physical targets, such as buildings, the electric grid, water and sewage systems, and even pipelines.

Using artifical intelligence, the PNNL-developed technology engages attackers in an elaborate deception, providing defenders with extra time to respond.

The technology was further developed in partnership with Attivo Networks, a provider of cybersecurity defense products. The California-based company eventually licensed Shadow Figment and bundled it into the Attivo ThreatDefend™ Platform for use in electric grid environments.

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.

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 5,000 staff and has an annual budget of $1.1 billion. PNNL is managed by Battelle for the 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 *pnnl.gov/available-technologies*.

CONTACT

If you would like more information about any technologies featured in our brochure, send inquiries to:

inventions@pnnl.gov

Pacific Northwest
NATIONAL LABORATORY

U.S. DEPARTMENT OF
ENERGY

PNNL-SA-149987