ENGINEERING

SECURING THE NATION'S CRITICAL INFRASTRUCTURE

Practicing the Art and Advancing the Science of Protecting Utility Networks

As utility communications environments become smarter and more connected, they also become more susceptible to cyberattacks. These environments are highly interconnected, interdependent systems with a variety of remote access capabilities. Accelerated smart grid deployments have dramatically increased the presence and role of intelligent endpoints, controls, and sensors. The ongoing pace of technology innovation and complexity means that critical infrastructure networks, applications, data, processes, and people are always changing.

At the same time, the physical and cybersecurity vulnerabilities grow as the threat landscape rapidly evolves and attack surfaces expand. As a result, utility networks are increasingly targeted by adversaries. A substantial disruption to these networks would have a profound impact on the confidentiality, integrity, and availability of mission-critical services on which businesses and their consumers rely.

With decades of cybersecurity experience in public and commercial sectors spanning defense, communications, energy, transportation, health care, finance, and entertainment, Peraton Labs offers superior security services from comprehensive security program and risk assessments to the development of new methods and tools to effectively address changing utility smart grid needs and mitigate emerging risks.

Peraton Labs is continually called upon to help industry and U.S. government agencies advance the science to protect and secure utility critical infrastructure from cyberattacks. Peraton Labs' successful track record in creating and commercializing revolutionary technologies yields novel solutions and services to support utilities in fortifying their cybersecurity posture and running their business more efficiently.

Leveraging our invaluable knowledge and deep research insight, Peraton Labs employs a systematic end-to-end approach to focus assessment activities on business, policy, process and critical infrastructure priorities. By utilizing our innovative 4-Quadrant Security Assessment Methodology we are able to provide a holistic, integrated evaluation of security posture across each of the quadrants of a customer's environment—wireless communications, network infrastructure, embedded hardware, and service and management applications—to expose and mitigate critical risks not apparent when looking at just one quadrant at a time.

Peraton Labs delivers generation-after-next-solutions in cybersecurity, mobility, networking, electronic warfare, analytics, and machine learning to government and commercial customers worldwide.

OUR INNOVATIVE TECHNOLOGIES INCLUDE:

- SecureSmart™ Continuous Monitoring as a Service (CMaaS), an industry-leading, field monitoring solution
- EnergyDefender, a multi-axis ICS cyber integrity solution, providing threat monitoring and cyber defense
- Jolt, a pioneering grid state consistency analysis system that protects against sophisticated and deceptive attacks using intelligent telemetry
- ProtocolPatroller, an ICS protocol cyber analysis, session mapping, and visualization system, for anomaly detection and response
- Cyber Emissions Monitor, a SCADA cyber integrity solution, based on RF emission modeling with deep analysis on SCADA equipment vulnerabilities
- CyberVAN, a flexible cyber range with high-fidelity network representations for conducting realistic cyber exercises
- WILEE, a large-scale cyber event reasoning, correlation, and prioritization solution with real-time, data-driven, cyber-hunting tools

GROUND-BREAKING APPLIED RESEARCH

We have an extensive track record of high-impact research and a long legacy of creativity and innovation. Our scientists and engineers have made pioneering contributions to packet communications, mobile ad-hoc networking, and policy-based network and systems management. With more than two dozen patents granted in recent years, we continue to advance the science from cybersecurity and analytics to quantum, autonomy, and the Internet of Things.

Department of Energy (DoE) Cybersecurity for Energy Delivery Systems (CEDS) program	**Response to cyberattack in progress:** groundbreaking, agent-based, distributed, extensible cybersecurity for hardening synchrophasor to phasor management unit (PMU) network intrusion detection and protection. **Detect adversarial manipulation of energy delivery systems components:** CMaaS and intrusion detection for wireless advanced metering infrastructure, distribution automation, and SCADA networks; detecting and analyzing traffic operations and security anomalies, characterizing network behavior for troubleshooting.
Defense Advanced Research Programs Agency (DARPA) Rapid Attack Detection, Isolation and Characterization Systems (RADICS) program DoE Liberty Eclipse regional energy assurance preparedness and resilience exercise	**Machine intelligence for advance notification of threats and energy grid survivable situational awareness:** 1) early warning and persistent situational awareness for large-scale attacks and accelerated recovery, 2) grid analytics for trust establishment and situational awareness during black start and recovery in absence of energy management system and limited operations technology capability, 3) large-scale anomaly detection and interconnections via novel graph theoretic, linear algebraic, and power balance algorithms. **Scalable and holistic energy attack and malware localization and characterization:** malware-hunting system to enable black start and power restoration by: 1) rapidly identifying misbehaving devices, the nature of the attack and Integrated Computer Solutions (ICS) malware; 2) guiding cyber restoration; 3) detecting advanced persistent threats during restoration; and 4) providing first responders with a three-axis, malware-hunting system to analyze traffic, power, and code behavior.
Air Force Research Laboratory (AFRL) Distributed, Assured and Dynamic Configuration (DADC)	**Efficient, secure, and accurate design for cyber infrastructure, cloud, and cyber physical systems:** 1) eliminate network configuration errors, 2) reduce ability of adversaries to gain knowledge of configurations, 3) precisely specify requirements with an intuitive language, 4) transform requirements into configurations; and 5) implement a configuration-space randomization technique to confuse adversaries.
Defense Advanced Research Programs Agency (DARPA) Cyber-Hunting at Scale (CHASE) Program	**Data-driven platform to detect and characterize cyberattacks:** cyber hunting system leverages innovative, adaptive data collection techniques to find and characterize attacks in real-time, at-scale, and across multiple enterprise networks with a 99% reduction in the amount of data that needs to be stored and a speed-up in incident reporting from days to minutes.
National Insitiute of Standards and Technology (NIST) Critical Infrastructure Protection Grants Program	**Advanced security profiles and enforcement for the next generation networks:** develops cybersecurity solutions for information protection in emerging networking systems and technologies.
Advanced Research Projects Agency (ARPA) Robust Adaptive Topology Control (RATC) Program	**Energy system management and operations under the robust adaptive topology control initiative:** use wide area monitoring protection and control data and dynamic topology control to improve grid operations, manage grid disruptions, and optimize asset utilization in transmission and distribution.
National Institute of Standards and Technology (NIST) Measurement Science and Engineering Research Grants Program	**Methodology for smart grid modeling:** teqchniques to model smart grid distributed energy resources and dynamic electric loads in micro-grid and building management applications, support simulation, and emulation work, and optimize energy management systems.
Defense Advanced Research Programs Agency (DARPA) Leveraging the Analog Domain (LADS) Program	**Cyber emissions monitor:** applies advanced signaling processing and machine learning to assess the real-time cyber integrity and operational health of controls equipment via non-intrusive monitoring of unintended radio frequency (RF) emissions.

SUMMARY

With decades of ground-breaking applied research and unparalleled cybersecurity experience in public and commercial sectors, Peraton Labs not only practices the art, but advances the science of protecting utility networks to help keep them secure in the increasingly challenging environment of today. Contact us at info@peratonlabs.com.

Peraton