PARSONS

Domain6

Critical Infrastructure Protection: Defending against physical and cyber threats while ensuring safety, reliability and resiliency

Parsons PLUS envision more SM

Domain6

Parsons offers Critical Infrastructure Persistence: defense from physical or cyber vulnerabilities at the IT layer coupled with analysis of the control systems environment to ensure resilience and redundancy

With more than 20 billion devices worldwide connected to internal and external networks – and the Internet – threats in cyberspace today are now threats to countless systems in the physical world. Among these are a vast array of devices that control industrial systems powering vital components of our nation's critical infrastructure. Today, operational technology (OT) devices are vulnerable to cyberattack through the Information Technology (IT) that connects them to external networks – connections that too often serve as threat vectors for hackers and others who wish to cause harm and disruption to vital assets, organizations and the communities they serve.

Unlike the most common IT disruptions, attacks against converged OT/IT systems pose real and immediate threats to health and safety. To defend your vital networks, systems and equipment at the OT/IT convergence, Parsons Domain6 protects your critical people, infrastructure and assets against emerging threats.

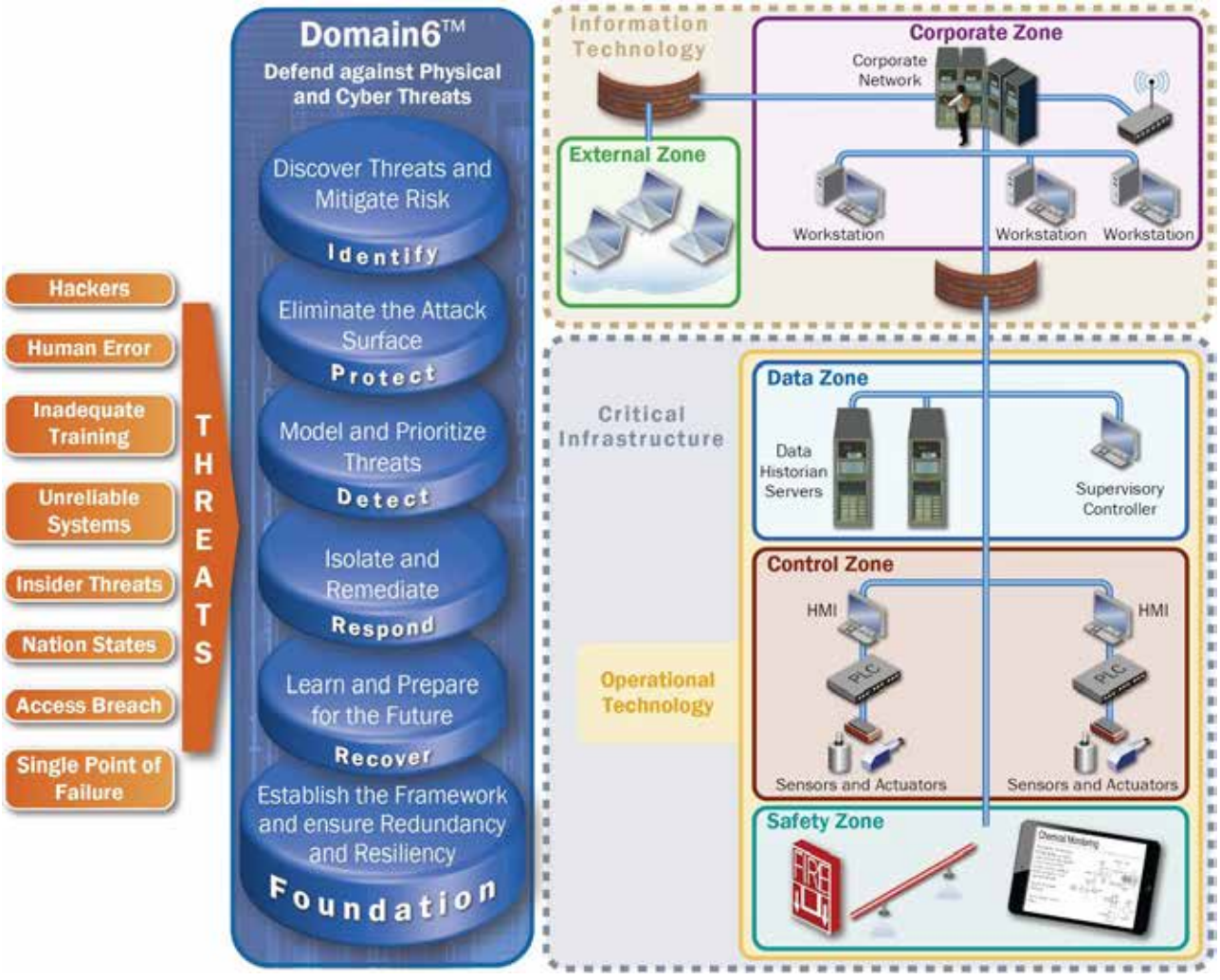
A Comprehensive OT Cyber Solution for Critical Infrastructure

Parsons Domain6 offers a comprehensive solution that identifies and mitigates risk to organizations across the U.S. Department of Homeland Security's 16 designated infrastructure sectors. Cyber and physical risks include those to SCADA architecture, programmable logic controllers, remote terminal units – and machinery, equipment, field devices and controls once considered immune to cyber-borne intrusion, disruption and attack.

The Domain6 Approach

- Fully converged OT/IT defensive capabilities.
- Security-by-design vs. bolt-on solutions.
- OT/IT expertise based on decades of experience in physical, cyber, and critical infrastructure domains.
- Available as a subscription service, allowing OT professionals to remain mission-focused.

Defense against Cyber/Physical Threats and Vulnerable Architectures



Nations, economies, communities and the security organizations serving them share a common dependence on resilient critical infrastructure assets – from the military base, to the electric grid, oil refinery and beyond. Domain6 protects critical infrastructure against cyber and physical threats and facilitates performance optimization. With Domain6, Parsons offers the tools, expertise and capabilities to defend what matters most to you.

FOUNDATION:
Establish the Framework and Ensure Resilliency

- Deployment of Camelot, Parsons' defensive cyber operations toolkit
- Use of multiple sources of information and advanced analytics to prioritize threats
- Monitoring and defense through secure SOC locations
- 24/7 or 8/5 operations-based on client requirements
- Diverse, tailored, mission-ready platforms

IDENTIFICATION:
Discover Threats & Mitigate Risk

- ICS inventory threat and vulnerability assessment
- Risk reduction strategy
- Vulnerability and modeling
- Table top exercises
- Collaborative OT/IT training
- RMF and compliance
- Priority vulnerability remediation

PROTECTION:
Eliminate the Attack Surface

- Definition of new OT topology
- Design of new OT topology enclaves
- Replacement of IP addresses
- Definition and management of closed networks
- Secure communications
- Cloaked OT Systems
- Monitoring from the inside

DETECTION:
Model and Prioritize Threats

- ICS threat modeling
- Anomaly and pattern detection through machine learning and advanced user behavior intelligence
- Detection of credential theft, anomalous data aggregation, privilege escalation and data exfiltration
- Privacy compliant and non-intrusive data collection

RESPONSE:
Isolate and Remediate

- Triage: Identify and mitigate single points of failure
- Impact assessment and quantification
- Root cause analyses
- Stakeholder/Regulator communications

RECOVERY:
Learn from the Threat and Prepare for the Future

- Future proof for a resilient infrastructure
- Generate efficiency by fine tuning systems and optimize performance
- After-action analysis for future learning, training and exercises

Safeguard Operations with Domain6

- Understand your cyber and physical vulnerabilities
- Address safety and security
- Ensure resiliency
- Deploy the latest cybersecurity technology
- Optimize performance

Parsons Domain6 Security Operations Center – Citadel

Secure SOC Located in Columbia, MD. Hub for Domain6 security as a service solution. Tailored cyber operations in all Domain6 services: converged cyber (IT/OT) and Physical Security OT Expertise in design, implementation and operations. Provides an advanced analytics platform, to include Zero Day net defense protection and diverse tailored mission-ready capabilities that maximize system resiliency. End-to-end full spectrum solution driving operations optimization through systems performance analysis.

Count on Parsons

For more than 30 years, Parsons has delivered cybersecurity and physical defense services that have protected our nation's most sensitive information and critical infrastructure. This experience is enhanced by more than 70 years of experience in the design, construction and management of vital assets around the globe. As a trusted partner to commercial organizations, and federal, state and local governments, Parsons and its team of OT/IT experts stand by to deploy leading professionals, processes and technologies to address the full spectrum of risks to your business.

Contact Us

Parsons is a leader in technical solutions, continuity of operations, critical infrastructure, and classified facility protection. Together, we create a safer, more secure world. Contact Parsons today to find out how Domain6 can be deployed to protect your OT/IT systems.

PARSONS

100 West Walnut Street
Pasadena, CA 91124

www.parsons.com

Please email us at: Domain6@Parsons.com