DER SECURITY

Defending Distributed Energy Resources

Cyber Threats, Real-World Attacks, and the DERSec Sentry Solution

Security White Paper
DERSEC-DEFENSE-1.0

Defending Distributed Energy Resources

Cyber Threats, Real-World Attacks, and the DERSec Sentry Solution

Table of Contents

1. Executive Summary

The rapid adoption of Distributed Energy Resources (DER) such as solar photovoltaics, battery energy storage systems, wind generation, and electric vehicle charging infrastructure is transforming modern power grids worldwide. While these technologies increase grid resilience and sustainability, they also introduce significant cyber-physical security challenges that threaten the reliability of energy infrastructure from local distribution networks to international grid operations.

DER Security (DERSec) has cataloged 129 unique Common Vulnerabilities and Exposures (CVEs) in solar-based DER systems alone, exposing approximately 45% of worldwide solar generation capacity (over 1 TW) to potential cyber exploitation. Meanwhile, real-world attacks on energy infrastructure continue to escalate, from botnet compromises of solar monitoring equipment to the sophisticated 2024 cyberattack on Poland’s power grid.

This whitepaper examines the growing threat landscape facing distributed energy systems, details specific vulnerability categories and attack vectors, presents real-world case studies, and introduces DERSec Sentry—the world’s first energy-aware cybersecurity platform purpose-built for DER environments. DERSec Sentry combines patented, physics-informed analytics with deep packet inspection across native DER protocols to detect dangerous commands, falsified telemetry, firmware changes, and insider threats in real time.

2. The Expanding DER Attack Surface

Traditional power systems were designed around centralized generation plants and hierarchical distribution networks with limited digital connectivity. Modern energy infrastructure is increasingly decentralized, integrating millions of DER devices across residential, commercial, and industrial environments. These systems rely on digital connectivity through DER management platforms, industrial control systems (ICS), smart meters, and cloud-based analytics, significantly expanding the attack surface for cyber adversaries.

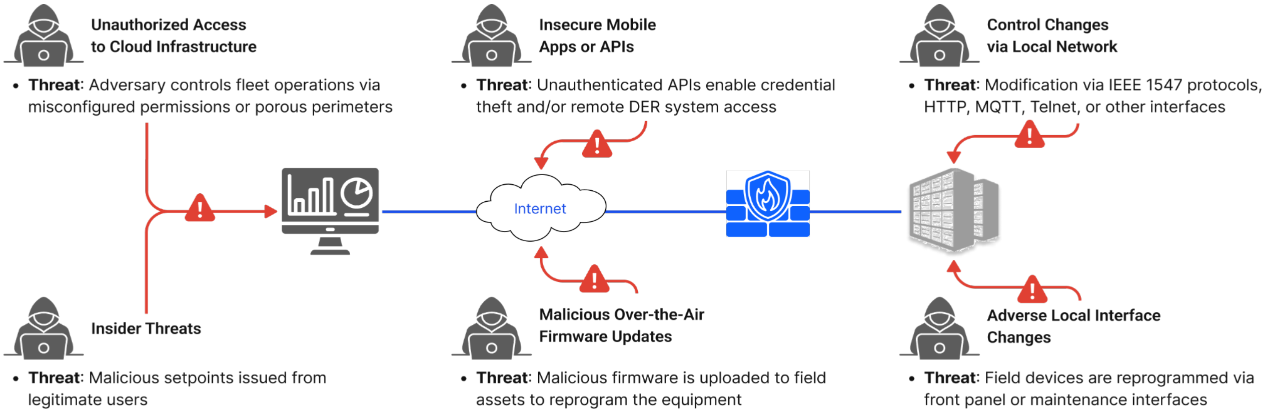
DER Technologies at Risk

DER Technology	Primary Attack Vectors
Solar Inverters	Inverter firmware manipulation, cloud platform compromise, measurement falsification, unauthorized control of power output, grid-support function modification, unauthorized parameter changes via local or remote interfaces
Battery Energy Storage Systems	Charge/discharge manipulation, thermal management override, bidirectional power flow exploitation to exceed line ratings
EV Charging Infrastructure	Charging station firmware exploits, fleet management system compromise, grid destabilization through coordinated load manipulation
Wind Generation	Turbine control system compromise, SCADA manipulation, false telemetry injection to mask operational anomalies
Microgrids	Islanding control manipulation, protection relay tampering, coordinated multi-asset attacks on campus or military installations

Because modern inverters combine computing devices with power conversion equipment, large-scale grid impacts are possible if vendor, operator, or aggregator cloud systems are compromised—or if malicious firmware updates are deployed that disable equipment at scale. Researchers have demonstrated the ability to gain unauthorized access to multiple inverter types, modify firmware, and arbitrarily control transistor switching operations, making scenarios involving simultaneous disconnection of hundreds of gigawatts of solar generation entirely plausible.

3. Solar Energy Cyber Threats and Vulnerabilities

DERSec's comprehensive vulnerability research has identified dozens of solar energy vulnerabilities and six publicly reported cybersecurity attacks on solar systems. The CVEs span solar monitoring systems, gateways, cloud infrastructure, and inverters. From a risk perspective, cloud vulnerabilities pose the most significant threat because they allow attackers to control gigawatts of generation from a single point of compromise.



Unauthorized Access to Cloud Infrastructure

- **Threat**: Adversary controls fleet operations via misconfigured permissions or porous perimeters

Insecure Mobile Apps or APIs

- **Threat**: Unauthenticated APIs enable credential theft and/or remote DER system access

Control Changes via Local Network

- **Threat**: Modification via IEEE 1547 protocols, HTTP, MQTT, Telnet, or other interfaces

Insider Threats

- **Threat**: Malicious setpoints issued from legitimate users

Malicious Over-the-Air Firmware Updates

- **Threat**: Malicious firmware is uploaded to field assets to reprogram the equipment

Adverse Local Interface Changes

- **Threat**: Field devices are reprogrammed via front panel or maintenance interfaces

Figure 1: Solar DER cybersecurity threat vectors and attack surfaces.

Notable Attack History

Year	Attack	Description
2019	**Denial-of-Service on sPower**	Unpatched Cisco firewall exploited, causing 12-hour loss of visibility to 500 MW of solar and wind assets.
2023	**Mirai Botnet and Romanian Grid Exploit**	Solar gateways incorporated into Mirai botnets. Romanian customers modified mandatory inverter grid-support settings using installer codes, jeopardizing grid integrity.
2024	**Japanese SolarView Compromise**	Remote code execution on Contec SolarView devices; 800 devices hijacked for bank theft while attackers retained capability to disable equipment or falsify solar measurements.
2024	**Lithuanian Ignitis Group Attack**	Pro-Russian hacktivist group Just Evil targeted state-owned energy company's solar monitoring via leaked credentials without MFA, accessing cloud management for 22 sites including schools and emergency stations.
2024	**PRC-Linked Botnet Operation**	Chinese state-sponsored actors compromised solar monitors for a botnet positioned for malicious activity, per FBI/NSA/CNMF joint advisory.
2025	**Poland Grid Attack**	Coordinated cyberattacks targeted 30 renewable energy sites (wind/solar) and a combined heat and power plant. The attacks used wiper malware to damage operational technology (OT) equipment but failed to create a major grid blackout.

U.S. CISA, NSA, and FBI have assessed that PRC state-sponsored cyber actors are pre-positioning on IT networks for disruptive cyberattacks against U.S. critical infrastructure. The Volt Typhoon threat actor has compromised multiple critical infrastructure organizations, underscoring the urgency of protecting DER assets against nation-state adversaries.

4. Case Study: The 2025 Poland Grid Attack

CRITICAL INFRASTRUCTURE ATTACK

In late December 2025, there was a sophisticated cyberattack targeting Poland's power grid, representing one of the most significant OT-focused energy attacks in recent European history. The attack demonstrated advanced persistent threat (APT) capabilities and highlighted the vulnerability of energy infrastructure to state-sponsored cyber operations.

Attack Overview

According to a Dragos report on the Poland attack, adversaries conducted a multi-stage operation against Polish energy infrastructure that combined IT network intrusion with operational technology (OT) targeting. The attack leveraged spear-phishing campaigns to gain initial access to corporate networks, then pivoted laterally to reach OT environments controlling power distribution and generation assets.

The threat actors demonstrated deep knowledge of industrial control systems and energy sector protocols. The attack chain included reconnaissance of SCADA systems, exploitation of network segmentation weaknesses between IT and OT environments, and attempted manipulation of grid control systems. The adversaries sought to compromise systems responsible for monitoring and controlling power distribution, with the potential to cause widespread service disruptions affecting millions of consumers.

Key Threat Indicators

Attack Phase	Details
Initial Access	Targeted site VPN access points with valid credential or historical vulnerabilities
Lateral Movement	Exploitation weak network segmentation to remote access multiple OT devices
OT Targeting	Focused on protocol conversion equipment and IEDs, RTUs, and HMIs in the substations using default accounts and passwords; executed malicious firmware to wipe equipment
Impact	Loss of solar site visibility and control
Intended Impact	Disruption of power distribution; manipulation of grid control parameters; potential for cascading failures across interconnected systems
Attribution Indicators	Tactics, techniques, and procedures (TTPs) consistent with state-sponsored threat groups targeting European critical infrastructure

The Poland attack underscores the reality that energy infrastructure cyberattacks are not theoretical—they are actively occurring. As DER systems become more prevalent and interconnected, the attack surface expands to include not only centralized grid infrastructure but also the distributed generation and storage assets that increasingly support grid stability.

5. Cascading Impacts

A cyberattack on distributed energy resources does not remain confined to the energy sector. The interconnected nature of modern infrastructure means that disruptions cascade rapidly from energy providers to essential state services. SolarPower Europe has estimated that the loss of just 3 GW of photovoltaic capacity would cause significant grid implications, while the loss of 10 GW could trigger cascading outages. Several cloud-connected DER management companies control fleets that reach or exceed these critical thresholds.

Cascading Impact Chain

Affected Sector	Potential Consequences
Energy Generation	Simultaneous disconnection of GWs of DER capacity; injection of subsynchronous oscillations; power quality degradation through harmonic distortion; tripping of protection equipment via deliberate phase shorts
Grid Operations	Voltage and frequency instability; overloaded transmission and distribution lines from manipulated bidirectional power flows; loss of situational awareness from falsified telemetry data
Healthcare	Hospital backup generation failure; disruption of medical device operations; loss of cold-chain integrity for pharmaceuticals and blood supplies; communication failures affecting emergency response coordination
Water and Sanitation	Water treatment plant disruptions; pump station failures; loss of pressure in distribution systems; potential contamination from interrupted treatment processes
Transportation	Traffic signal failures; EV charging infrastructure shutdown; rail and transit system disruptions; airport operations degradation
Public Safety and Communications	Emergency services communication failures; 911 dispatch system outages; loss of surveillance and public safety systems; degraded first-responder coordination
Financial Services	Banking system disruptions; payment processing failures; data center outages affecting cloud services; market trading interruptions

The 2025 Iberian Peninsula power outage demonstrated how quickly energy disruptions cascade into societal impacts. With increasing DER penetration—solar provided 50.4% of ERCOT power generation in April 2025—the consequences of a coordinated cyberattack on distributed energy assets could be devastating and far-reaching in the U.S.

6. The DERSec Sentry Solution

DERSec Sentry delivers the world's first energy-aware cybersecurity layer purpose-built for Distributed Energy Resources. Unlike generic IT security tools retrofitted for operational technology, Sentry combines patented, physics-informed analytics with deep packet inspection across native DER protocols to detect dangerous commands, falsified telemetry, firmware changes, and insider threats in real time.

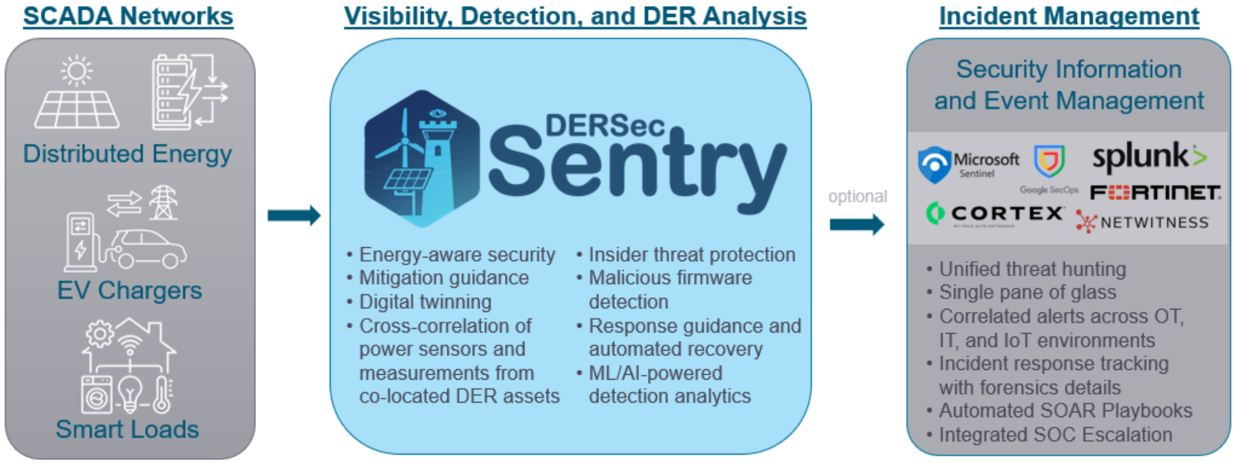

SCADA Networks
Distributed Energy
EV Chargers
Smart Loads
Visibility, Detection, and DER Analysis
DERSec Sentry
• Energy-aware security
• Mitigation guidance
• Digital twinning
• Cross-correlation of power sensors and measurements from co-located DER assets
• Insider threat protection
• Malicious firmware detection
• Response guidance and automated recovery
• ML/AI-powered detection analytics
optional
Incident Management
Security Information and Event Management
Microsoft Sentinel
Google SecOps
splunk>
FORTINET
CORTEX
NETWITNESS
• Unified threat hunting
• Single pane of glass
• Correlated alerts across OT, IT, and IoT environments
• Incident response tracking with forensics details
• Automated SOAR Playbooks
• Integrated SOC Escalation

Figure 2: DERSec Sentry integrates with SCADA, OT IDS, and SIEM tools for unified visibility.

Core Capabilities

Capability	How It Protects Against DER Attacks
Deep Packet Inspection	Parses SunSpec Modbus, OPC UA, DNP3, IEEE 2030.5, OCPP, and other DER traffic to extract and validate measurement and control signals in real time.
Digital Twin Analytics	Physics-informed simulation runs in parallel with physical systems to detect maloperations and false data injection attacks that evade traditional network monitoring.
ML/AI Cyber Detection	Inference engine trained on over 1 billion DER data points using NVIDIA Morpheus detects anomalous patterns indicative of cyber threats or operational manipulation.
Stateful Detection	Tracks operational state over time to detect slow-burn adversarial campaigns that evolve gradually to avoid triggering threshold-based alerts.
Response Playbooks	If enabled, autonomous threat response capabilities to block endpoints, revoke credentials, and reset compromised systems to known-good states.
Forensics Context	Power-aware intelligence distinguishes physical faults from cyberattacks, accelerating root cause analysis and recovery operations.

Built on patented, R&D100 Award-winning research from Sandia National Laboratories, DERSec Sentry integrates with SCADA systems (e.g., Inductive Automation Ignition), OT IDS tools (e.g., Nozomi Networks Guardian), and SIEM/SOAR tools (e.g., Splunk SOAR) to provide comprehensive, single-pane-of-glass IT/OT/IoT/DER visibility, detection, and response.

7. Deployment and Integration

DERSec Sentry deploys flexibly across all Purdue model levels—from field networks through enterprise IT. Whether in the cloud, on-premises with rackmount hardware, or containerized on existing hardware, the DERSec Sentry provides fail-safe monitoring via mirror/SPAN ports while alerting operators to threats targeting field assets or head-end systems.

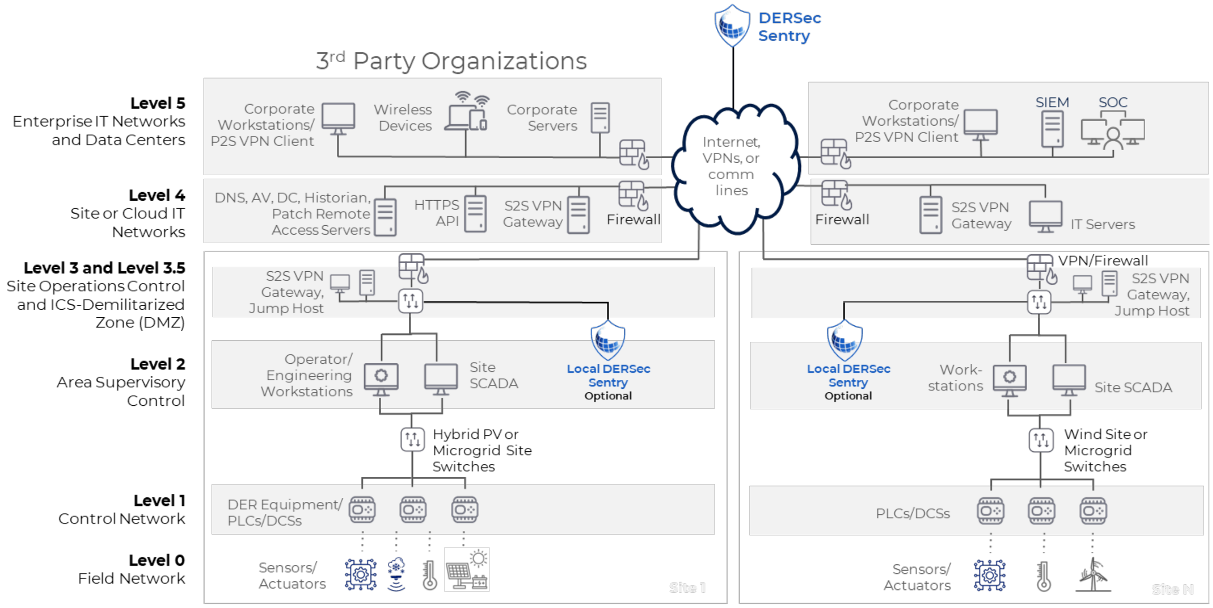

DERSec Sentry
3rd Party Organizations
Level 5
Enterprise IT Networks and Data Centers
Level 4
Site or Cloud IT Networks
Level 3 and Level 3.5
Site Operations Control and ICS-Demilitarized Zone (DMZ)
Level 2
Area Supervisory Control
Level 1
Control Network
Level 0
Field Network
Corporate Workstations/ P2S VPN Client
Wireless Devices
Corporate Servers
DNS, AV, DC, Historian, Patch Remote Access Servers
HTTPS API
S2S VPN Gateway
Firewall
Internet, VPNs, or comm lines
Corporate Workstations/ P2S VPN Client
SIEM
SOC
Firewall
S2S VPN Gateway
IT Servers
S2S VPN Gateway, Jump Host
Operator/ Engineering Workstations
Site SCADA
Local DERSec Sentry
Optional
Hybrid PV or Microgrid Site Switches
DER Equipment/ PLCs/DCSs
Sensors/ Actuators
Site 1
VPN/Firewall
S2S VPN Gateway, Jump Host
Local DERSec Sentry
Optional
Work-stations
Site SCADA
Wind Site or Microgrid Switches
PLCs/DCSs
Sensors/ Actuators
Site N

Figure 3: DERSec Sentry deployment across Purdue model levels.

Target Environments

Utility-Scale DER: Solar farms, BESS, and wind installations requiring NERC CIP compliance and advanced threat detection.

AI Data Centers: Backup generation and on-site renewable power supporting mission-critical computing infrastructure.

Microgrids: Campus, military, and community microgrids requiring autonomous cybersecurity monitoring and rapid incident response.

eMobility Fleets: EV charging infrastructure and fleet management requiring protection against coordinated load manipulation.

8. Conclusion and Call to Action

The convergence of escalating cyber threats, growing DER penetration, and the critical role of distributed energy in modern grid operations creates an urgent need for purpose-built cybersecurity solutions. With more than 100 known CVEs in solar systems alone, active nation-state targeting, and demonstrated attacks against European power grids, the question is not whether a major DER cyberattack will occur, but when. DERSec Sentry provides the critical security layer that distributed energy infrastructure demands—combining deep protocol understanding, physics-informed analytics, and machine learning to detect and respond to threats that traditional IT security tools cannot see.

> **Ready to secure your energy infrastructure?** Contact us at **info@dersec.io | dersec.io**