SECHARD

Case Study

TREDAS's Approach to Securing Distributed Energy Infrastructure

Achieving Centralized Visibility and Compliance with SecHard

TREDAS Boosts Infrastructure Security and Monitoring with SecHard Cyber Hygiene Platform

IN BRIEF

Customer

TREDAS
(Trakya Electricity Distribution Inc.)

Industry

Energy Distribution

Location

Türkiye
Thrace Region
(60+ operational sites)

Organization Size

Regional electricity provider serving all of Thrace

Challenges

- *Aligning with national security guidelines from the Presidential Digital Transformation Office*
- *Monitoring and managing a distributed infrastructure in real time*
- *Achieving high hardening and security levels across servers and network devices*

Solution

- SecHard Cyber Hygiene Platform

Featured Modules

- Device Manager
- Hardening Module
- TACACS+ Server
- Vulnerability Manager
- Performance Monitor
- Privileged Access Manager (PAM)
- Syslog Collector

Benefits

- Hardening levels increased to 95% on network devices and 80%+ on servers
- Real-time visibility and centralized monitoring of all operational assets
- Streamlined privileged access with secure session recording
- Full compliance with national cybersecurity regulations

CHALLENGES

TREDAS, the regional electricity distribution company of Thrace, operates over 60 sites and is responsible for ensuring uninterrupted power across the region. To maintain such critical infrastructure, they needed:

- Strict alignment with the Turkish Presidential Digital Transformation Office's Information and Communication Security Guide
- Unified oversight and configuration management for all IT and OT assets
- Scalable security tools to monitor vulnerabilities and enforce hardening standards

TREDAS required a platform that could centralize operations, standardize security actions, and ensure real-time monitoring — without disrupting core electricity distribution services.

SOLUTION

After evaluating SecHard and seeing strong references from other energy distribution companies, TREDAS launched a successful POC and deployed the SecHard Cyber Hygiene Platform, actively using 6 of its 10 modules. Key implementations include:

- Hardening Module: Increased hardening levels to 95% for network devices and over 80% for Windows systems.
- Performance Monitor: Enabled real-time monitoring of ports, systems, and resource usage from a central dashboard.
- TACACS+ Server: Delivered secure, unified access control for switches of all brands and models — with full AAA log tracking.
- Vulnerability Manager: Provided continuous monitoring of network-wide vulnerability exposure.
- Device Manager: Applied hardening actions across devices in minutes.
- Privileged Access Module: Facilitated secure RDP and VNC access — with complete session recording.
- Syslog Module: Consolidated network logs to generate alert mechanisms and proactive response workflows.

BENEFITS

By implementing SecHard Cyber Hygiene Platform, TREDAS gained:

1. **Compliance Assurance:** Full alignment with national cybersecurity guidelines.
2. **Real-Time Operational Oversight:** Continuous monitoring and proactive issue detection.
3. **Security Standardization:** Automated hardening and centralized policy enforcement.
4. **Privileged Access Control:** Seamless management of external and internal system access with accountability.

Ugur Bora Gure, *TREDAS*

"SecHard has empowered us to apply advanced security configurations quickly, monitor vulnerabilities continuously, and maintain a compliant, secure, and observable infrastructure. The value it has brought is tangible, and we recommend SecHard to all energy sector organizations."

CONCLUSION

TREDAS's use of SecHard demonstrates how critical infrastructure providers can achieve security maturity at scale. By leveraging modular architecture and real-time intelligence, the organization now operates with increased resilience, visibility, and control.

To learn more about SecHard and how it can benefit your organization, visit www.sechard.com.