ENGINEERING
INFOGRAPHICS

Ensuring energy continuity through security

Cyber Resilience to protect our energy infrastructure

Energy is the invisible and indispensable engine of our society. A cyberattack on the energy sector could also cause widespread blackouts, leading to severe economic, social, and national security consequences.

Ransomware attacks and supply chain breaches present significant threats to the energy sector. Effective identity and access management are crucial for mitigating these security risks.

4 Key Pillars:

- **Defining a strategy** to improve the security posture
- **Implementing a "Zero Trust" approach** to dynamically manage access to critical data and applications
- **Adopting SOC with advanced data analysis and automation** to neutralize persistent and insider threats
- **Proactively preventing attacks** to ensure rapid recovery and secure ongoing operations

To tackle cybersecurity challenges effectively, it's crucial to embrace **a holistic approach** and **a multilayered "in-depth" defense strategy**. We integrate vertical and horizontal solutions to safeguard devices, identities, data, technological infrastructures, workloads, and cloud-based application services. **By combining technologies, processes, and expertise in line with industry standards** and modern methodologies, we ensure the security and **resilience** of energy operations.

The Value of Technology's Impact

AI-Driven Value

We employ AI to detect and prevent attacks in real-time, analyze vast amounts of data to identify anomalous patterns or suspicious behaviors, and automate security processes such as incident response. An effective cybersecurity approach based on AI necessitates implementing **advanced defense systems**, ongoing personnel training to understand and utilize these technologies correctly, and continuously **evolving security strategies** to counter increasingly sophisticated threats in the evolving digital landscape.

Cybersecurity Awareness

We implement robust Identity and Access Management (IAM) to control access to critical environments and ensure regulatory compliance, optimizing operational costs and promoting a cybersecurity culture essential for sustainable business growth. This approach **strengthens internal security** and enhances energy **consumers' awareness of best cybersecurity practices**, thereby bolstering the overall security chain within the sector.

Composable Business Models

The composability of cybersecurity in the energy sector involves creating **modular security frameworks** that can be adapted and integrated into existing infrastructure. The goal is to enhance protection against evolving cyber threats while maintaining operational efficiency and reliability of energy systems. For example, the **Composable Mesh** in our SOC framework revolutionizes the traditional approach by bringing control points and security measures closer to critical assets through **a centralized, multi-layered platform**.

Our Toolbox

Our Impact

DISCOVER MORE →