CYWARE™

CASE STUDY

Energy Leader Shines a Light on Cyber Fusion for the U.S. Energy Sector

Executive Summary

In the wake of escalating cyber threats, the U.S. Energy Sector emerges as the most prioritized Critical Infrastructure (CI) sector and the backbone of most other CI sectors. Even well-resourced organizations struggle to outpace collaborative and evolving adversaries. This case study describes how a large energy company deployed the Cyber Fusion Platform to address significant challenges from threat intelligence to insider threats, with transformative security benefits.

Cyware Cyber Fusion Stats

30,000+	Businesses receive threat intelligence through Cyware's platform
400+	Integrations with security, IT, and DevOps tools
83%	Enterprise customers average reduction in time spent per ticket, with **2,083 hours** saved per month

Critical Infrastructure's Most Critical Function

The Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA) consider the Energy sector as the topmost CI industry. Its pivotal role is underscored by the fact that without energy, no other CI sector can function. State and non-state actors consistently and aggressively target the Energy sector, in part due to its high-profile nature. Recognizing this persistent threat, regulatory bodies have increased security regulations, requiring the sector to enhance its cyber defenses.

A large energy company, recognizes the importance of cybersecurity and invests heavily in defense-in-depth, robust threat intelligence, and ongoing cybersecurity awareness training. Even with their sophistication, they also recognize that cybersecurity challenges remain.

While the threat landscape is continuously changing, simply adding more layers to a complex security stack has diminishing returns. Similar to many other large organizations, the company has dozens of disparate tools that don't always play nicely together. Combined across multiple functions, this can create data, tech, and people silos, making collaboration and proactive security difficult. While the core components of cybersecurity were there, it was cumbersome to get the right intelligence to the right people to take the right action at the right time.

Green Light for Cyware's Cyber Fusion

Securing critical infrastructure is complex and the Energy sector is not immune from global security talent shortages. This sector also has substantial investments in legacy infrastructure and systems that lack modern security capabilities. A proliferation of interconnected devices and systems has increased the attack surface. The company decided to take a new approach with Cyware's Cyber Fusion platform, enabling them to break down silos, streamline and centralize processes, and improve efficiency and effectiveness across intelligence, analysis, investigation, response, and reporting.

Cyware's Cyber Fusion Platform not only adds key capabilities to improve an organization's defensive posture – it improves the way existing tools and teams work together, optimizing resources to support a more proactive program. Cyware addresses a variety of challenges the energy leader faces.

1 **Full Intelligence Cycle Implementation**

Allows them to collect, aggregate, correlate, and prioritize intelligence reports. This holistic approach ensures that they don't just receive raw data, but include actionable insights that are relevant to their operational needs.

2 **Incident Response**

Automated intelligence ingestion streamlines the creation of selective incidents. Moreover, the platform's ability to carry out comprehensive environmental analyses and initiate automated actions via Cyber Fusion's comprehensive integrations with their detection and actioning tools empowers them to respond to threats in real-time, mitigating potential damage.

3 **Insider Threat Management**

With compartmentalized workflows, the platform allows coordination amongst various business units like SOC teams, human resources, legal, and physical security. This collaboration means that insider threats, which often require a multi-departmental response, are handled more efficiently and effectively.

4 **Threat Investigation**

Bridging the intelligence generation gap ensures that the collected data isn't merely stored but is actively correlated to paint a more comprehensive picture of potential threats.

5 **Reporting Features**

Advanced auto-reporting and tailored intelligence dissemination complemented by manual reporting provision mean that the right intelligence reaches the right stakeholders at the right time through automated delivery mechanisms.

6 **Risk Management**

Threat exposure contextualization is provided at technical levels to proactively address vulnerabilities and improve system resiliency against evolving threats.

7 **KPI and Work Management Reporting**

Fulfilling regulatory requirements is of paramount importance and they can now more easily meet SEC 8K and 1106 reporting requirements. This not only ensured compliance but also instilled greater confidence in their stakeholders.

Cyber Fusion Brightens the Energy Sector's Security Future

For energy sector stakeholders, the challenges are ubiquitous and the threats, ever-present. It is a strategic imperative to invest in and deploy advanced solutions like cyber fusion, ensuring not just the security of the Energy sector but also the resilience of the entire nation's Critical Infrastructure.

With the Cyware platform, this energy industry leader is able to connect legacy systems, improve the effectiveness of existing security tools, while getting clarity and actionable insights into their threat landscape. They can break through data, technology, and team silos, improving efficiency and collaboration. Ultimately, they can automate connecting the dots in order to swiftly action upon contextualized threat intelligence, reducing response times and minimizing potential damage.

CYWARE™

For more information you can reach us at :

Cyware
111 Town Square Place Suite 1203 #4,
Jersey City, NJ 07310
sales@cyware.com | www.cyware.com