LevelBlue

CASE STUDY

How LevelBlue helped a leading energy company remain secure 24×7 with Microsoft E5 Solutions

A major player in the energy industry recently adopted a proactive approach to reducing its cybersecurity risk and exposure to known and unknown cyber threats and sophisticated adversaries.

The client sought a comprehensive cybersecurity solution to support its transformation initiatives, which included refreshing its cyber technology stack, provisioning local Security Operations Centers (SOCs) and staffing, maturing SOC procedures and policies, and ensuring 24×7 threat detection, investigation, and response coverage.

The challenge

The client faced several key challenges in its cybersecurity transformation journey. First, there was a pressing need to update and enhance its existing cybersecurity infrastructure, necessitating a comprehensive refresh of its cyber technology stack.

This activity included integrating advanced security tools and technologies to bolster its defense mechanisms. Additionally, the client intended to establish and staff local SOCs to improve its monitoring and response capabilities. This involved not only setting up the physical infrastructure but also recruiting and training skilled personnel to manage and operate these centers effectively.

The client also recognized the importance of improving its SOC procedures and policies to ensure efficient and effective operations. This desire required developing and refining protocols to standardize responses and improve its overall security posture.

Next, to address the ever-evolving threat landscape, the client sought to implement continuous 24×7 threat detection, investigation, and response mechanisms to safeguard against cyber threats.

Finally, the client expressed its intention to enhance its advanced threat hunting, and effective breach response was crucial.

The solution

After in-depth conversations with the client, LevelBlue recommended a suite of tailored cybersecurity solutions to address the client's needs, including two tools created through its partnership with Microsoft. The client agreed to LevelBlue's proposal and opted to adopt LevelBlue:

1. **Managed Detection & Response (MDR) for Microsoft Defender:** Provides continuous monitoring, threat detection, and response using Microsoft Defender.
2. **Co-Managed SOC for Microsoft Sentinel:** Collaborating with the client to manage their SOC using Microsoft Sentinel, ensuring seamless integration and operation.
3. **Advanced Continual Threat Hunting (ACTH):** ACTH is a Tactics, Techniques and Procedures (TTPs) focused threat-hunting platform and methodology based on the NIST MITRE ATT&CK framework.
4. **Digital Forensics & Incident Response (DFIR):** Offering expert digital forensics and incident response services to handle and investigate security incidents.
5. **Cyber Advisory Services:** Providing strategic cybersecurity advice to help the Client navigate complex security challenges and regulatory requirements.

Results

By partnering with LevelBlue, the client significantly improved its cybersecurity posture.

Continuous monitoring and ACTH significantly improved the client's ability to detect and respond to threats in real-time, ensuring LevelBlue and the client identified and mitigated potential threats and mitigated swiftly.

The co-managed SOC approach, combined with LevelBlue's mature procedures and policies, further enhanced the efficiency and effectiveness of the client's SOC operations. This collaboration allowed for seamless integration of resources and expertise, optimizing the overall security posture.

LevelBlue's DFIR services are crucial in ensuring rapid and thorough investigation and mitigation if a security incident occurs, minimizing impact, and allowing the client to quickly return to business as usual.

Additionally, LevelBlue's advisory services provide the client with valuable insights and strategies, helping the client stay secure.

Why LevelBlue

LevelBlue won the client's business despite facing stiff competition from several respected vendors. The client was impressed with several aspects of LevelBlue's operation. This included:

1. **Federated Organizational Structure:** LevelBlue's ability to support the client's federated organizational structure with a solution and partnering approach that spanned the entire group of companies.
2. **Best of Breed Technology Strategy:** LevelBlue's flexibility to integrate with the client's preferred technologies, unlike SecureWorks, which required the use of its proprietary platform.
3. **Co-Managed SOC Approach:** LevelBlue's co-managed SOC approach allowed the Client to maintain an onsite SOC component while leveraging international resources off-site, providing a balanced and effective solution.
4. **Industry Recognition:** LevelBlue's recognition as an industry leader and a Gartner-recognized Managed Security Service Provider (MSSP) instilled confidence in the Client's decision.