Resilient Energy Infrastructure

The energy industry is working to leverage new technologies to complement and expand legacy infrastructure while facing an expanding landscape of cybersecurity threats. CyberRes energy solutions deliver availability, security, and efficiency to help them meet these demands.

To reduce costs while providing reliable and guaranteed power to customers within region or a country, the energy sector must leverage new technologies that complement and expand existing legacy infrastructure. The expansion of the cyber-physical landscape includes IIoT, cloud-based infrastructure, and smart devices. This increased digital footprint drives new insights into customer habits and preferences while increasing efficiencies in operations.It also opens the door to additional risks that can impact the cyber-physical value chain. Energy providers need to embed protective and detective security technology throughout the value chain to achieve desired outcomes.

Guaranteed Service Delivery

Availability of energy is critical to guarantee the continuous operations of end customers. This requirement is even more applicable to renewable energy because of its reliance on IIoT, OT, and analytics to monitor the operations of the value chain. Energy infrastructure and connected devices are subject to advanced attacks that bypass traditional protective controls. Energy providers need to rapidly detect, remediate, and prevent attacks, and visualize risk so they can ensure service availability. Traditionally hard-to-secure devices, programmable logic controllers, remote terminal units, safety information systems, or phasor measurement units should be protected and monitored through next-generation technologies. This can help minimize the impact of attacks or unintentional service interruptions. The adoption of a zero trust philosophy will also reduce the likelihood of compromise. CyberRes Security Operations and Identity and Access Management portfolios provide the most mature and flexible models for protecting and monitoring for IT, OT, and IIoT risk.

Efficient Operations

Smart devices, the smart grid, IIoT, and cloud-based systems can be leveraged by energy providers to not only enhance the customer experience, but to also increase the efficiency of operations and self-assessment capabilities. Economic load dispatch is a prime use case whereby smart devices and analytics can be leveraged to quickly identify increased energy demand and determine whether the available energy supply is sufficient or whether additional power needs to be generated/acquired. The same approach can be taken with renewable energy for real-time equipment monitoring to ensure plant uptime. Having this near real-time capability to monitor for increased or decreased energy needs enables energy suppliers to avoid over/under generating power and optimize costs. Protecting and monitoring IIoT devices, cloud systems, and the supporting network is necessary to secure such efficient operations.

CyberRes Intelligence monitors for lateral movement and privilege escalation, as

well as most of the tactics, techniques, and procedures of the MITRE ATT&CK framework.

Big Data Intelligence

Actionable intelligence requires large amounts of data in order to provide a view into customer preferences and habits, achieve efficient operations, and reduce costs. Customer data can be collected through numerous sources, such as smart meters, mobile/web applications, call centers, or in-person visits. It will likely include sensitive data sets such as sleeping habits, number of people in the home, presence or lack of security systems, banking details, and home addresses. The data required for efficient operations and grid management, if compromised, would be valuable information to competitors and nation states. The collection and centralization of this data introduces a new area of risk to energy entities. Building a data governance framework and securing sensitive data throughout its lifecycle is necessary to reduce the risk of a breach.

CyberRes Data Security portfolio can provide governance and secure IT and OT data in its original format to enable downstream analytics applications.

Securing the Application Landscape

The energy sector includes thousands of applications that are found in distributed energy resource management systems, virtual power plants, and SCADA systems. These applications generate and share data, which could result in a critical power outage if the application were breached. Securing applications within both the IT and OT environment must be included in a vulnerability management program to reduce the risk of an outage. As mentioned above, customers leverage mobile and web applications to communicate with energy organizations. If these applications were to be compromised, the customer data and accounts would be open to data theft.

CyberRes Application Security portfolio can secure mobile, web, and cloud-based apps through static, dynamic, and mobile application testing.

CyberRes Capabilities for Energy

CyberRes is a Micro Focus line of business.

> "With ArcSight we have a platform to monitor security events and manage incidents. We have seamless data integration and are compliant with relevant security standards and controls. Improved asset visibility ensures 99 percent availability."
>
> MR. JACOB JACOB
> Specialist Cyber Security
> Dubai Electricity and Water Authority

We bring the expertise of one of the world's largest security portfolios to help our customers navigate the changing threat landscape by driving both cyber and business resiliency within their teams and organizations. We are here to help enterprises accelerate trust, reliability, and survivability through times of adversity, crisis, and business volatility. We can provide solutions that drive resilience in the energy sector and enable desired business outcomes.

Guaranteed Service Delivery

CyberRes Security Operations and Identity and Access Management portfolios are designed to provide the most mature and flexible models for protecting and monitoring risk across the energy value chain. Petabytes of data are produced by IIoT devices, resulting in a limitation of the logs that can be collected and monitored. However, CyberRes Security Operations solutions have the big data-ready capabilities to collect data from many devices within the energy value chain. Additionally, CyberRes can augment traditional detection and response technology beyond an XDR and enhance the partnership between humans and machines. This enables SOC analysts to act faster and smarter and make critical decisions that will keep operations running.

Efficient Operations

CyberRes Intelligence and Security Operations portfolios monitor for lateral

movement and privilege escalation, as well as most of the tactics, techniques, and procedures of the MITRE ATT&CK framework. These solutions offer unprecedented capability to address modern and future threat actors, combining industry-based threat intelligence, adaptive behavioral profiling, adjacent adversary analytics, adaptive access control, and precision SCADA device analysis. This is combined with CyberRes' next-generation MITRE analytics and campaign-based threat models to create a comprehensive solution.

CyberRes is able to address risk across the identity landscape, enabling energy providers to:

- *Discover:* Provide a comprehensive baseline of privileged identities and their dependencies. As a first step in managing privilege, it is important to know which identities (users, services, devices, things, etc.) have elevated access and what dependencies exist so you have the insight to simplify and implement policies.
- *Monitor:* Detect changes and track privilege activity to support governance and compliance. Monitor changes and privileged activity throughout the entire identity lifecycle to identify potential threats and ensure governance and compliance.
- *Control:* Implement identity-powered privilege management to reduce risk. This allow you to apply policies that adjust privileges to reflect access requirements based on attributes in real time. It employs the principle of "least privilege" so everyone and everything has just enough access to do the job.

Extending this ability into the CyberRes Identity and Access Management portfolio, the Adaptive Access solution goes beyond zero trust and provides dynamic identity context. This provides predictive, behavioral, and data-driven continuous authentication. It also provides continuous authorization, real-time response, and remediation to prevent lateral movement across the energy value chain.

Big Data Intelligence

CyberRes Data Security portfolio can enable big data intelligence by securing sensitive data sets using field-level AWS-256 format-preserving encryption. This keeps data in its original format for usability. The data also retains its referential integrity, allowing it to be connected across all sources. Additionally, CyberRes Data Security Structured Data Manager provides a mature data governance solution. This structured data can be automatically classified at collection and monitored throughout its lifecycle. The approach removes the need for in-transit and at-rest data security solutions, lowering the risk of a data breach, saving costs, and ensuring the usability of data for analytics, applications, and business processes.

Securing the Application Landscape

With the thousands of applications used within IT and OT environments, a strong application security process needs to be built into the application development lifecycle. CyberRes Application Security solutions can detect vulnerable code through mobile, static, dynamic, or open source analysis. Detected vulnerabilities can be output into existing bug tracking tools such as Jira and Micro Focus ALM for seamless remediation. Leveraging either the on-premises instance or our SaaS offering, developers have a range of options to match their in-house security expertise.

Contact us at **CyberRes.com**

Like what you read? Share it.

CyberRes

A Micro Focus line of business