opentext™ | Cybersecurity

Product Flyer

ArcSight cyDNA for Energy and Utilities

Protect critical infrastructure with a FarSpace view of adversary activities directed at your organization.

ArcSight cyDNA Benefits

Protect Operational Control Systems

Adversary Signal Analytics
Suspicious Remote Access
FarSpace Coverage

Fortify Critical Infrastructure

Zero-Touch Global Deployment
Single-Platform Visibility
Adversarial Scanning Activity

Guard Financial Data

Data Exfiltration
Devices Impacted

Defend Intellectual Property

Deconfliction Threat Analysis
Threat Actor Attribution

Today, the energy and utilities industries have become increasingly digital, enabling more efficient operations and improved service delivery. This digital transformation has been steadily revolutionizing the sector, enabling real-time monitoring and control of energy generation, distribution, and consumption. However, this connectivity also presents inherent risks. As the number of data points and devices continues to grow, energy and utilities organizations face challenges in providing sufficient security coverage to safeguard their critical infrastructure against cybersecurity threats.

What if there was a way to see cyberattacks on energy and utility infrastructure as they occur, and see who's behind them?

ArcSight cyDNA by OpenText is an Adversarial Signal Analytics solution that can provide a holistic view of threat actors attempting to infiltrate operational control systems, subvert financial systems, and steal confidential intellectual property. While traditional intelligence could tell you what MIGHT happen, based on what HAS happened to others, ArcSight cyDNA can tell you what IS happening, based on malicious traffic to YOUR organization.

Cybersecurity Challenges

The energy sector faces an ongoing struggle with a large and expanding digital attack surface, posing significant cybersecurity challenges. With the adoption of more advanced industrial control systems,

the energy industry has witnessed a proliferation of interconnected systems, devices, and networks. This expanded attack surface encompasses a wide range of critical infrastructure, including power generation plants, smart grids, energy and water distribution networks, and IoT devices. As the sector embraces advancements like renewable energy integration, decentralized energy systems, and electric vehicle charging infrastructure, the complexity and diversity of potential entry points for cyber threats multiply.

Oil and gas, energy generation and public utility sectors in particular struggle to achieve cybersecurity objectives for the following reasons:

- OT systems converging with IT
- Public and private ownership models
- Complex vendor relationships
- Interdependent infrastructure
- Legacy systems and equipment

ArcSight cyDNA Benefits for Energy and Utilities

Protect Operational Control Systems
ArcSight cyDNA utilizes **Adversary Signal Analytics**, letting you quickly identify adversarial activity directed at your organization. You'll be able to discover and contextualize cybercriminals attempting to disrupt or manipulate operational control systems via internet connection, pinpointing devices experiencing **suspicious remote access** activity, and identifying those responsible. ArcSight cyDNA's **FarSpace coverage**, the ability to see beyond traditional security boundaries and firewalls, gives you a bird's eye view of adversarial activity against your organization and helps fill the security gaps created by the convergence of IT and OT systems.

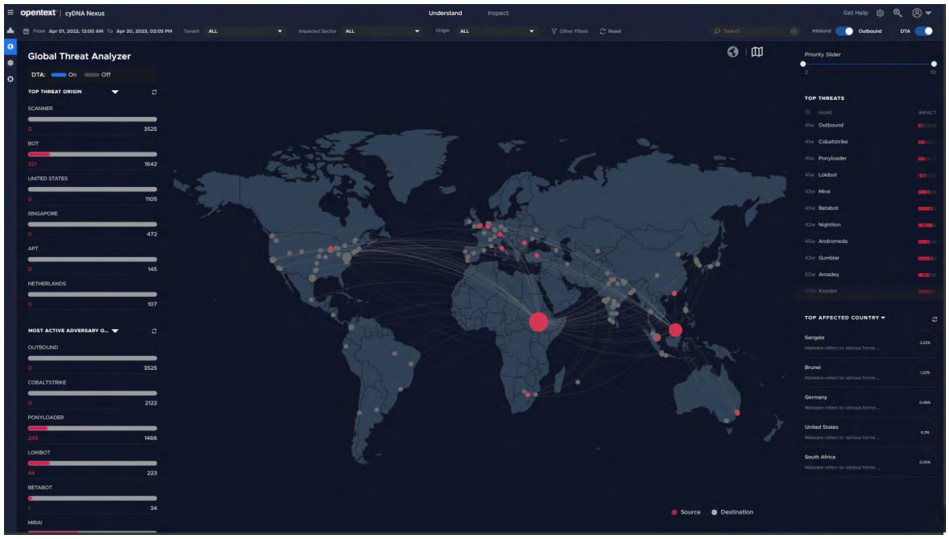

Figure 1. ArcSight cyDNA showing organization's (red) outbound data sent to adversarial (grey) destinations

Fortify Critical Infrastructure
ArcSight cyDNA can help fortify oil and gas production and supply chains, energy generation, and public utility services with its **zero-touch global deployment**. It is deployed without the need for additional hardware, and can cover your desired digital spaces with ease, whether public or privately owned (with owner permission, of course). Formerly siloed operating environments can be incorporated into cyDNA's covered space with **single-platform visibility**.

Threat actors love exploiting vulnerabilities in legacy systems and equipment. In their attempts to do so, they conduct scanning activity to find targets to be exploited. Fortunately, cyDNA allows you to detect **adversarial scanning activity** of your extensive infrastructure, letting you identify cyber threats, all without collecting a single event log.

Guard Financial Data
Public utility companies have a wealth of sensitive customer information needed for billing and service delivery. This includes credit card information, bank account numbers, social security numbers, driver's licenses, and other personally identifiable information. Threat actors are highly motivated to access this information as it can be exploited for identity theft, financial fraud, or sold on the black market. ArcSight cyDNA can alert you to **data exfiltration** from your organization, informing you of the locations and **devices impacted**, and the threat actors responsible.

Defend Intellectual Property
Energy companies invest significant resources in R&D to enhance efficiency, discover energy solutions, or improve sustainability. Cybercriminals target intellectual property, technology patents, proprietary processes, and research

“Traditional threat intelligence platforms tell you, in general, there are threats in an industry or in a country. cyDNA tells you explicitly what threats it is seeing—as they are happening; this is an important distinction.”

Muhi Majzoub
Executive Vice President, Chief Product Officer
OpenText

Connect with Us
www.opentext.com

data to exploit or to gain a competitive advantage. ArcSight cyDNA provides the ability to see targeted attacks on your organization and remove the baseline noise that broadly dispersed threats represent. With **Deconfliction Threat Analysis**, cyDNA shows you a more precise view of attacks specifically targeting you, and **threat actor attribution** to reveal adversaries that have taken a special interest in your organization’s capabilities.

Learn more at
www.arcsight.com

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.