Detection and Analysis of Threats to the Energy Sector (DATES)

A groundbreaking integrated capability in intrusion detection, security event management, and sector-wide threat analysis

Detecting cyber attacks against digital control systems quickly and accurately is essential to energy sector security. Current intrusion detection systems (IDS) continuously scan control system communication paths and alert operators of suspicious network traffic. But existing IDS, often not tailored to the control environment, typically offer limited attack response capability and frequently produce false alarms or fail to alert. Without carefully deployed monitoring, these devices can produce an overwhelming number of alarms that become difficult to correlate. This introduces system communication latency and slows incident response time.

The two-year DATES project is a groundbreaking effort to develop the first integrated intrusion detection, security incident/event management (SIEM), and large-scale threat analysis capability for the energy sector. DATES will provide control system operators with enhanced incident detection and alerting tools through rigorous monitoring of threats at the network, host, and device levels. Integrating SIEM capabilities, the system will use attack models and information from prior events to automatically correlate alarms, distinguishing malicious cyber incidents from minor disruptions.

Additionally, utilities can lack an anonymous method to share threat information across the sector, which limits owner/operator threat visibility to what they can record on their own systems. DATES will create an anonymous global threat database, allowing utilities to securely report their threat data. System owner/operators can then view other sector security events in real time to obtain an accurate, high-level view of their security posture. Improving and integrating these security features will create an unprecedented defense system against increasingly sophisticated cyber attacks.

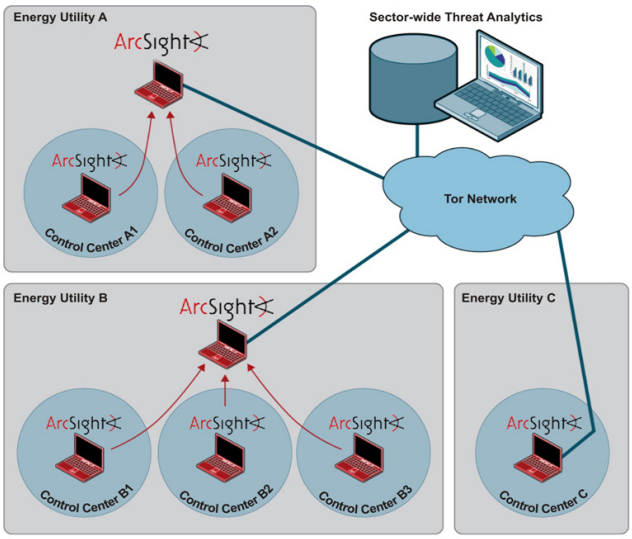
National SCADA Test Bed

Benefits

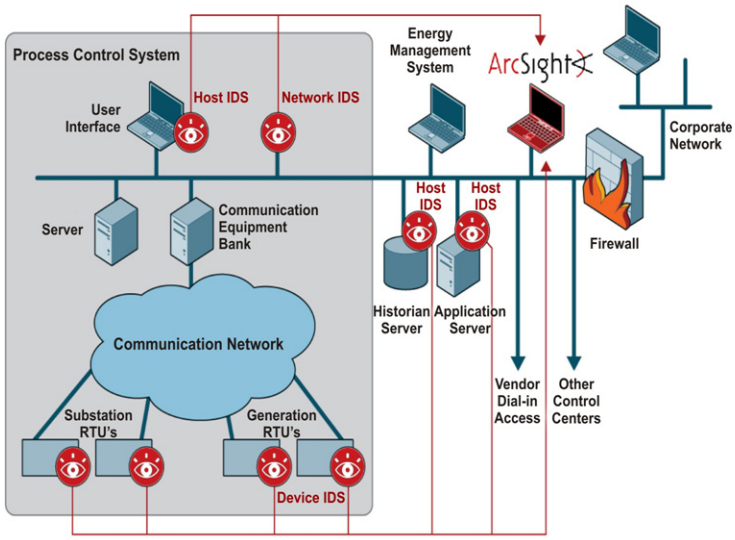
- Creates a multi-level comprehensive monitoring system complementary to perimeter defenses
- Provides customized attack detection capabilities at the network, host, and device levels
- Correlates security alerts using enhanced security incident/event management technology to accurately identify security attacks and potential threats
- Improves situational awareness to enable more timely response to a cyber attack
- Mitigates current reluctance among private sector utilities to share security event data
- Provides operators with a sector-wide view of cyber attack activity and the details needed to determine what attack methods are being used

Partners

- SRI International
- ArcSight
- Sandia National Laboratories



The DATES framework will provide industry with a secure sector-wide monitoring, information sharing, and threat analysis capability.



The red eye graphics indicate the possible placement of DATES IDS sensors at the network, host, and device levels in a typical control system.

Technical Objectives

The DATES project team seeks to accomplish the following tasks over the project's three planned phases:

Phase 1:

- Develop a comprehensive suite of vulnerability scenarios to determine optimal IDS sensor placement and design
- Link IDS components and enterprise security management tool to create comprehensive SIEM capability
- Develop correlation models for IDS alarms
- Enhance cyber threat analytics tool to create a secure, anonymous channel for contributing attack data to the global repository

Phase 2:

- Select appropriate IDS components and create correlation rule sets
- Build out attack scenarios to validate the correlation system and demonstrate ability to form utility-level situational awareness picture
- Develop methods for using the threat data repository to formulate sector-specific defense strategies

Phase 3:

- Analyze and finalize system configuration to maximize leading-edge attack detection capability
- Conduct red team testing to validate DATES solution suite

End Results

Project results will include:

- IDS software and software connectors
- Correlation and configuration rules for SIEM software
- Fully integrated prototype DATES software suite

As the DATES solution suite matures, the project team will:

- Seek to include its monitoring and situational awareness configuration as part of the functional requirements for factory acceptance tests with one or more industry partners
- Leverage the factory acceptance test mechanism to assure DATES effectively addresses critical control system IDS/SIEM needs
- Seek a close cooperative role with one or more industry partners to stimulate interest in pilot deployment

May 2008

DOE National SCADA Test Bed (NSTB)

NSTB is a multi-laboratory resource that partners with industry and other government programs to test, research, and help design cyber security solutions to enhance control systems security in the energy sector and reduce the risk of energy disruption due to cyber attack.

For More Information:

Hank Kenchington
Program Manager
DOE NSTB
202-586-1878
henry.kenchington@hq.doe.gov

Alfonso Valdes
SRI International
650-859-4976
Alfonso.valdes@sri.com

Visit Our Websites:

www.csl.sri.com/projects/dates
www.oe.energy.gov/controlsecurity.htm