Enhanced Cyber Services for Energy

MITIGATE MALICIOUS ATTACKS WITH AI

Enhanced Cyber Services (ECS) for Energy is an integrated cyber offering tailored to improve data and system security for energy companies by providing real-time threat detection, network visualization, and advanced investigative capabilities.

RigNet's ECS enables customers to work with a single vendor to augment their existing cybersecurity personnel, which can substantially reduce their OPEX when compared with the cost of hiring cybersecurity professionals. Working in conjunction with RigNet's security operation center (SOC), ECS will employ advanced intrusion-prevention tools to continuously monitor cyber threats.

Among the tools ECS will be using is a platform from artificial intelligence (AI) pioneer Darktrace, the world leader in cyber AI for cyber-threat detection and cyber-attack defense. The capabilities Darktrace offers along with Cyphre, our advanced data-encryption technology, enables RigNet to provide energy customers the most complete suite of cyber-security services for the protection of their data and networks.

Darktrace's partnership with RigNet is coming at a critical time. The increasing convergence of IT and OT environments is dramatically expanding the threat surface of industrial control systems, while threats to SCADA are increasingly advanced. Organizations will now be able to benefit jointly from RigNet's expertise in the energy industries and Darktrace's world-leading cyber AI.

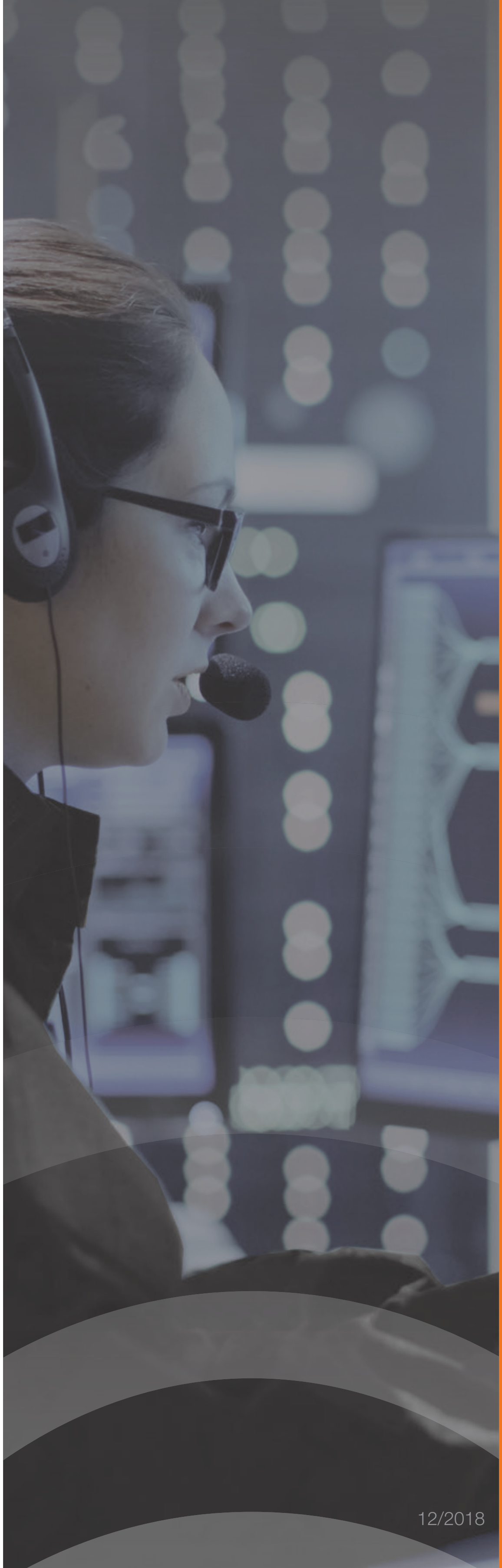
Not only will this partnership help companies support and augment existing security teams, but by detecting and combating cyber-threats in real time, attacks can be stopped before they do damage.

Visibility
Seeing on-net traffic, devices, and threat patterns enhances network security by mitigating threats in real-time.

Monitoring
Threats attack around the clock and your network is continuously under siege from automated attacks or cybercriminals around the world. Monitoring for attacks needs to be 24/7/365, so you need to have security experts and tools in place. It takes an average 206 days for US companies to detect a breach. The average cost of identifying a breach within that time-frame was $5.99 million.[1]

Awareness
Running on your network and devices so you can be aware of developing threats to them.

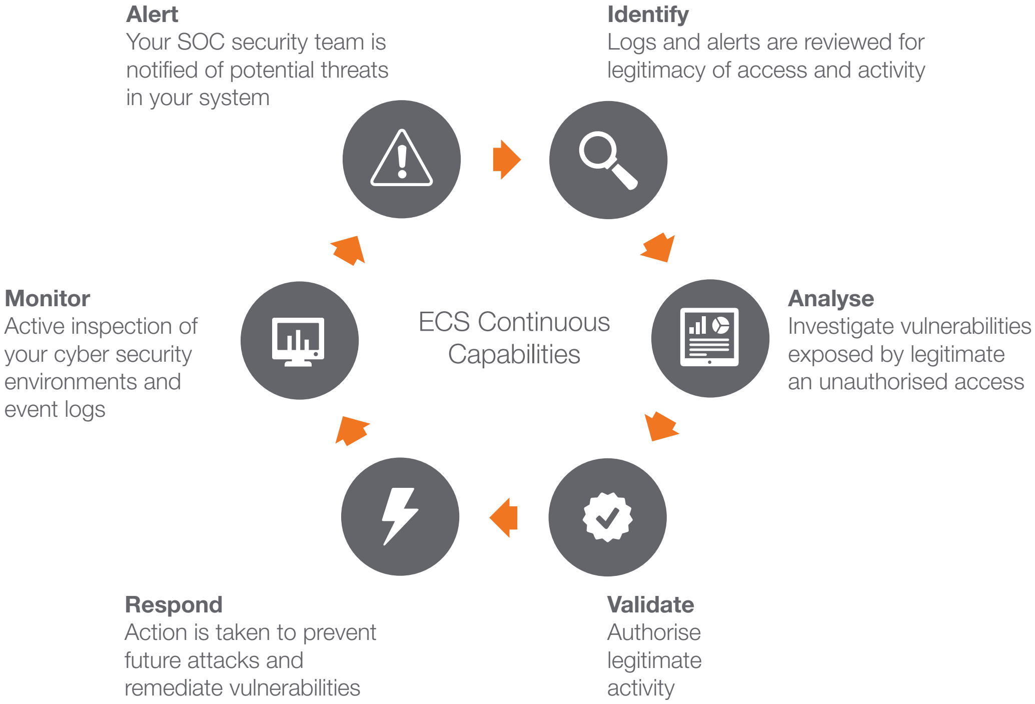
Response
Identifying threats and taking timely corrective action is paramount is reducing the impact of a cyber event to the operations of any company.



RigNet

Enhanced
Cyber Services

12/2018



ECS Continuous Capabilities

Alert
Your SOC security team is notified of potential threats in your system

Identify
Logs and alerts are reviewed for legitimacy of access and activity

Analyse
Investigate vulnerabilities exposed by legitimate an unauthorised access

Validate
Authorise legitimate activity

Respond
Action is taken to prevent future attacks and remediate vulnerabilities

Monitor
Active inspection of your cyber security environments and event logs

[1] *13th annual Cost of a Data Breach study, 2018, Ponemon Institute.*

RigNet (NASDAQ:RNET) delivers ultra-secure, intelligent technology solutions that allow the oil and gas industry to finally realize the business results of digital transformation. We empower diverse energy businesses to gain real-time insights from their remote operations and take action that drives profitable revenue growth. RigNet operates globally, with headquarters in Houston, Texas.

For more information
visit our website www.**rig.net**/contact/contact-sales
or contact us at sales@**rig.net**

Enabling Intelligence. Delivering Results.