MICRO FOCUS

Case Study
Security

DNeX Technology S/B

ArcSight supports next generation SOC to reduce incident response time and improve threat detection.

Overview

DNeX (DNeX Technology S/B—"DNeX") is a leading service provider in Malaysia's trade facilitation and energy sector. Its core businesses encompass a range of specialized companies, each providing customized services, solutions and infrastructures, engineered and led by industry experts.

Challenge

FORTRESS, DNeX' core offering, addresses the constantly changing IT security threat landscape by adopting a fluid security infrastructure. As part of this, its managed security services division offers 24x7 monitoring, as well as Security Information and Event Management (SIEM), Security Operations Center (SOC) building, and security log management services.

"I have seen a lot of SIEM solutions come and go over the last 20 years. ArcSight, however, is still leading the pack. Without it, I would not be able to run our mission-critical SOC, supporting all our customers with a minimum of two staff per shift."

RODNEY LEE
CEO
DNeX

These services are key for Malaysia's financial services (FS) institutions, to comply with a regulatory mandate from the central bank that all FS institutions need to monitor traffic and transactions across their network on a 24x7 basis, in real-time. This includes data correlation between all brands of financial products.

Rodney Lee, CEO of DNeX, explains the challenge this presents for many banks: "Introducing an on-site SOC and 24x7 security monitoring is cost-prohibitive for many organizations. They simply don't have the resources to do this. Using an economy-of-scale model, DNeX helps with this. Relationships with our customers are entirely built on trust and I have personally been in the IT security business for 20 years. We understand the central bank's monitoring requirements, which gives us a running start with new customers."

He continues: "Micro Focus® ArcSight was on our radar from the early days. It was, and in my opinion still is, the number one SIEM on the market, backed by a reassuring position in Gartner's magic quadrant."

Solution

ArcSight Enterprise Security Manager (ESM) is a comprehensive real-time threat detection, analysis, workflow, and compliance management platform with increased data enrichment capabilities. Hosted in a DNeX datacenter,

DNeX

At a Glance

- **Industry**
  Software and Technology
- **Location**
  Malaysia
- **Challenge**
  Support FS and National Critical Infrastructure institutions with mandatory security monitoring in a cost-effective and efficient model
- **Products and Services**
  ArcSight Enterprise Security Manager
- **Results**
  + 50% cost savings for customers, compared with on-site SOCs
  + Full visibility and reporting supports advanced threat detection
  + Diverse source correlation directs resources to high risk areas
  + Time savings with sophisticated Connector technology

> "A government customer gave us four weeks to create 22 FlexConnectors/parsers. ArcSight enabled us to complete the project within two weeks."
>
> **RODNEY LEE**
> CEO
> DNeX

Contact us at:
www.microfocus.com

Like what you read? Share it.

ArcSight ESM processes and analyses customer security logs with a typical lag time of less than five seconds.

Fully segregated customer data ensures confidentiality and DNeX comprehensively backs up all security logs. Lee comments on how ArcSight enables DNeX to operate a lean security organization: "ArcSight processes data from a wide variety of sources and offers sophisticated event correlation to accurately escalate threats that violate the internal platform rules. We appreciate the ability to build automated use cases, so that incidents are identified automatically without anyone having to sift through security logs for the answers. This 'red-flagging' saves us huge amounts of time."

More event sources bring more enterprise visibility and the ability to develop more complex use cases specific to the security needs of a customer's organization. This very mature ArcSight implementation disseminates and correlates threat information, filtering out 80% of incoming events as noise, so the DNeX team can focus resources on high-risk areas.

Lee and his team have found huge benefit in ArcSight's use of SmartConnectors and FlexConnectors. Out-of-the-box SmartConnectors support every common event format, from native Windows events, and APIs, to direct database connectivity. Using the FlexConnector development framework, DNeX develops custom connectors/parsers to integrate with ArcSight ESM for indexing and use in its correlation engine.

Lee: "We recently encountered an example of an Open Source firewall which was totally unknown to us. Even though this was not a mainstream data source, we were able to build a FlexConnector for it within half an hour, so that we could integrate the data and give this customer complete visibility. A government customer gave us four weeks to create 22 FlexConnectors/parsers. ArcSight enabled us to complete the project within two weeks."

ArcSight reporting and dashboarding has proved very helpful to DNeX customers. Customers can log onto the DNeX SIEM and generate custom reports presenting near real-time security status. DNeX has also configured 'attack maps' for customers. These demonstrate the value of security monitoring in a very visual way and can often be prominently displayed at customer sites.

DNeX can also support Malaysia's Critical National Infrastructures, where traffic and network monitoring is mandatory too. Critical Infrastructure providers typically rely heavily on Operational Technology (OT) networks, which were often not built with security in mind. They now need to combine their OT and IT operations while ensuring full security compliance. DNeX is on hand to support this effort with its ArcSight-driven SIEM architecture. It can do this on a managed service basis, but also in a flexible hybrid model, where the organization hosts its own SOC, and hands monitoring services over to DNeX after business hours. Taking this flexible approach can halve a customer's costs of hosting their own 24x7 security operations.

Results

Focusing on ArcSight for over 10 years has given DNeX unprecedented expertise that adds value to their customers. Lee on the continuing commitment to ArcSight: "I have seen a lot of SIEM solutions come and go over the last 20 years. ArcSight, however, is still leading the pack. Without it, I would not be able to run our mission-critical SOC, supporting all our customers with a minimum of two staff per shift."

He concludes: "Even though the attack landscape is changing all the time, and becoming more challenging by the day, I feel in great hands with ArcSight."