Enhance OT Cyber Risk Quantification with Vulnerability Insights

SOLUTION OVERVIEW

Business Challenge

ICS/OT cybersecurity professionals often struggle to effectively communicate cybersecurity weaknesses and cyber risk to their executive leadership.

Cybersecurity teams focus on technologies and indicators such as the number of obsolete platforms, critical vulnerabilities, and potentially malicious events inside the ICS/OT system while executives want to hear about the probability of an event and the dollar impact of cyber incidents on the business.

Solution

DeNexus' DeRISK™ platform regularly pulls data from Tenable Security Center to provide leadership teams with key indicators that show how their cybersecurity projects impact the cyber risks faced by the company across sites or in comparison with industry peers.

Value

CISOs and cybersecurity teams use DeNexus to:

- Enrich the dataset used for risk modeling by combining Tenable's and DeNexus' data
- Deliver accurate analysis on where the business faces the greatest risks in OT environments
- Collaborate effectively with CFOs and executives on cybersecurity investment decisions

Outputs from DeNexus include financially oriented information such as:

- Indicators of industrial OT cyber risk exposure
- Annual Expected Loss
- Value at Risk
- Probability of loss
- ROI of suggested risk mitigation strategies

Technology Components

- Tenable Security Center version 6.2 and above
- DeNexus's DeRISK platform 5.x

Key Benefits

- Automatic re-use of Tenable's data
- Quantification of cyber risks
- Financial impact of potential cyber events
- Translation of CVE metrics into business metrics:
  - Annual Expected Loss
  - Value at Risk
  - Probability of Loss
- Automatic data feed through APIs
- Continuous cyber risk updates
- ROI-based comparison of risk mitigation options
- Tracking of cyber risk improvement trends
- Cyber risk reduction
- Turnkey cyber risk executive reports

About DeNexus

DeNexus is the leading provider in cyber risk modeling for industrial networks.

Employing advanced simulation, AI, and inside-out data, DeNexus forecasts incident probabilities, translating them into quantifiable financial risks.

Trusted by Global 1000 companies in power generation, energy transportation and distribution (T&D), manufacturing, hyper scale data center operations and transportation, DeNexus provides an evidence-based approach to enhance cybersecurity investment decisions and risk reduction.
www.denexus.io

About Tenable

Tenable® is the Exposure Management company. Approximately 40,000 organizations around the globe rely on Tenable to understand and reduce cyber risk.

As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies.
www.tenable.com

More Information

For demo and support, please contact us:
https://www.denexus.io/contact

Features

Leveraging critical inside data from telemetry sources like Tenable Security Center enables DeNexus to provide detailed, bottom-up, portfolio-level cyber risk modeling and quantification. Specific capabilities include:

- Quantification of cyber risk in the OT environment,
- Comparison of the cyber risk posture across sites and with industry peers,
- Identification of sites or system that could potentially lead to the greatest financial loss when a cyber incident occurs,
- Prioritization of CVEs at each site, based on exploitability and severity,
- Suggestions of most effective mitigation strategies,
- Prioritization of mitigation strategies based on expected ROI and risk reduction,
- Executive level reporting to support evidence-based cybersecurity resource allocation,
- Justification of cybersecurity investments

Examples of Outputs

Main Drivers of Potential Loss

Initial Access Vector (IAV)	Annual Expected Loss ($)	Loss (in Days of Revenue)	Event Contribution (%)	Event Revenue Loss Contribution (%)
Exploitation Of Remote Services	$1,059,624	1.4	26.7%	0.4%
Remote Services	$907,051	1.2	22.9%	0.3%
Drive-By Compromise	$532,713	0.7	13.4%	0.2%
Phishing				
Spear Phishing				

Main Types of Potential Loss

Loss Event	Annual Expected Loss ($)	Loss (in Days of Revenue)	Event Contribution (%)	Event Revenue Loss Contribution (%)
Loss Of Productivity	$2,479,248	3.3	62.6%	0.9%
Downtime	$907,630	1.2	22.9%	0.3%
Extortion	$267,845	0.4	6.8%	0.1%
Equipment Damage	$128,309	0.2	3.2%	0.0%
Forensic Investigation	$110,178	0.1	2.8%	0.0%