INDUSTRIAL DEFENDER®

RAND McNALLY



CASE STUDY

Rand McNally

Assessing Cyber Risk and Applying Additional Security Controls

INDUSTRIALDEFENDER.COM

COMPANY PROFILE

Rand McNally is an American technology and publishing company that provides innovative fleet management and commercial transportation solutions, connected vehicle technology, consumer travel, and education products.

The company is a leader in the fleet management software market, and its cloud-based telematics platform helps fleets manage increasing regulatory compliance requirements and improve profitability through advanced driver and vehicle analytics as well as market-leading truck navigation and asset tracking. Rand McNally's Fleet platform and in-vehicle hardware includes an electronic logging device (ELD), which is used to electronically record truck drivers' Hours of Service (HOS).

"With the sharp rise in ransomware attacks, Rand McNally wanted to evaluate its cyber risk levels and increase security controls."

THE SITUATION

With the sharp rise in ransomware attacks, Rand McNally wanted to evaluate its cyber risk levels and increase cybersecurity controls to ensure the company was doing everything possible to be proactive about keeping systems and data secure.

Customer Requirements

- Assess and mitigate current risk levels in the company's IT and OT environments.
- Ensure that cybersecurity best practices based on the CIS Controls and the NIST Cybersecurity Framework are in place to protect from cyberattacks like ransomware.

THE SOLUTION: INDUSTRIAL DEFENDER

Industrial Defender engineers and analysts consulted with Rand McNally with a goal to layer security mechanisms and to ensure the company had in place the five foundational security controls from the Center for Internet Security® (CIS) and the NIST Cybersecurity Framework (CSF), including:

- Asset Management (CIS Controls 1-2 and NIST ID.AM)
- Configuration Control (CIS Control 4 and NIST PR.ID 1 & 3)
- Access Control (CIS Control 5-6 and NIST PR.AC)
- Software and Vulnerability Management (CIS Controls 2 & 7 and NIST ID.RA & ID.RM)
- Security Event Monitoring (CIS Controls 8 & 13 and NIST DE.AE, DE.CM & RS.AN)

After planning out the company's cyber risk reduction strategy, Rand McNally engaged Industrial Defender to:

- Create a complete inventory and baseline of hardware and software assets.
- Detect configuration changes from the inventory of assets such as software installations or changes, user accounts added or modified, listening ports and services, firewall rules, computer security settings, etc.
- Collect installed software application inventory and identify common vulnerability exposures (CVEs).
- Capture user account information from assets and provide policy checks such as password complexity and age.
- Monitor server and workstation assets, capturing events from audit logs (system logs and antivirus/malware applications). The events are normalized, consolidated, processed for trends and thresholds, and prioritized. Automatic notifications are produced for critical events to alert the customer for real-time awareness.

THE RESULT

Key risks and vulnerabilities that were identified and mitigated included:

Asset Management

- Computers that were no longer in use were removed from the network

Configuration Control

- Detection of audit policy changes

Access Control

- Access control settings on workstations and laptops were modified
- Password credentials were strengthened for some user accounts
- Removed some service accounts

Software and Vulnerability Management

- Guaranteed the absence of critical CVEs found within the software inventory
- Ensured there was no "personal use" application software, unused software, and software and operating systems no longer supported by vendors

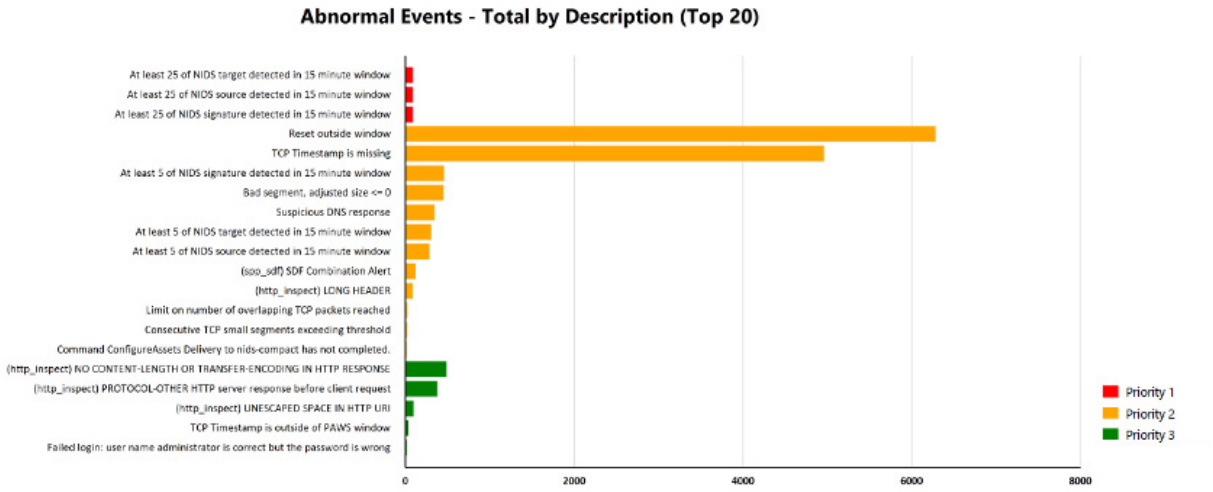
"Industrial Defender provided very useful information about our cyber risk posture that we were able to use to harden our environment further and feel reassured that we are protected against future threats."

– Director of IT

Security Event Monitoring

- Excessive failed logon attempts from users and service accounts
- Virtual Host Servers used for operations (for example domain controller) with substantial CPU/memory resource constraints
- Virtual Servers with time drift requiring resync often

A series of reports and dashboards were created to provide insights into key risk indicators (KRIs) for Rand McNally. IT managers can now quickly identify if there are risks that require further investigation or mitigation actions.



An Example Report from Industrial Defender

Future expansion plans for Rand McNally include using Industrial Defender's CopilOT Service™ to reduce internal workloads and focus more on strategic cybersecurity initiatives.

THE INDUSTRIAL DEFENDER DIFFERENCE

Since 2006, Industrial Defender has been solving the challenge of safely collecting, monitoring, and managing OT asset data at scale, while providing cross-functional teams with a unified view of security. Their specialized solution is tailored to complex industrial control system environments by engineers with decades of hands-on OT experience. Easy integrations into the broader security and enterprise ecosystem empower IT teams with the same visibility, access, and situational awareness that they're accustomed to on corporate networks. Learn more at **www.industrialdefender.com**.

Planning an OT Security Project?

SCHEDULE A DEMO

FOR MORE INFORMATION

1 (877) 943-3363 • (617) 675-4206 • info@industrialdefender.com
225 Foxborough Blvd, Foxborough, MA 02035
industrialdefender.com

© 2021 iDefender, LLC

INDUSTRIAL DEFENDER®