DEEP FOREST

SECURITY

- Digital forensics
- Cyber incident response
- Information security risk consulting
- AI-powered detection & automated response
- Security event logging, analysis, alerting
- Cyber vulnerability management

Threat Landscape Increased

2023 Highlights

- **Port of Los Angeles**:
  - Cyber-attacks doubled compared to 2022.
- **NoName Group's Canadian Port Campaign**:
  - A notorious group attacked several Canadian port authorities.
  - Impacted: Ports of Nanaimo, Saguenay, Trois-Rivières, and Belledune.
- **Pro-Russian Cyber Campaigns**:
  - Multiple cyber-attacks affected key Canadian ports, including Halifax, Montreal, and Québec.

Threat Landscape Increased

2024 Highlights

- **USCG expresses grave concern**
  - Ports and Harbors are still assigning cybersecurity to IT, stating that it needs to be assigned to the CFO, because it falls under Risk Management, and impacts entire organization.
- **Ivanti Breach**:
  - Advanced evasion techniques led to persistent access.
  - Significant impact: 412 hosts compromised via credential theft.
- **CISA's Ivanti Vulnerability**:
  - Internal Ivanti tools were exploited, compromising security.
- **Chinese State-Sponsored Cyber Operations**:
  - US Government identified targeted surveillance at North American Ports.

Deep Forest Security Enhanced Front Line Tools to Meet New Threats Head-on:

- **Advanced Security Assessment**: Increased robustness, Includes C Suite Exec Summary.
- **Powerful AI anomaly detection:** Network monitoring and response
- **Enhanced Vulnerability Scanning**: Detects new and emerging security loopholes.
- **AI-Driven Log Monitoring**: Features metadata analysis and anomaly detection.
- **Refined Incident Response Strategies:** Better suited for todays threatscape.
- **Elevated Simulation Exercises**: Improved Tabletop and Red Team exercises simulate current threat scenarios to test cyber resilience.

Deep Forest Security's Strategic Tool Deployment

Responding to the 2023/2024 threat landscape

Key Insights from Over 50-Client Deployment:

- Security handed off to IT rather than CFO
- No annual risk assessments.
- No regular vulnerability scans.
- No security management plans.
- No Incident Response Capabilities.
- Insufficient security policies.
- Poor Network Monitoring.
- No Log Monitoring.
- No incident response capabilities.
- Subpar Training.
- No comprehensive system stress tests.