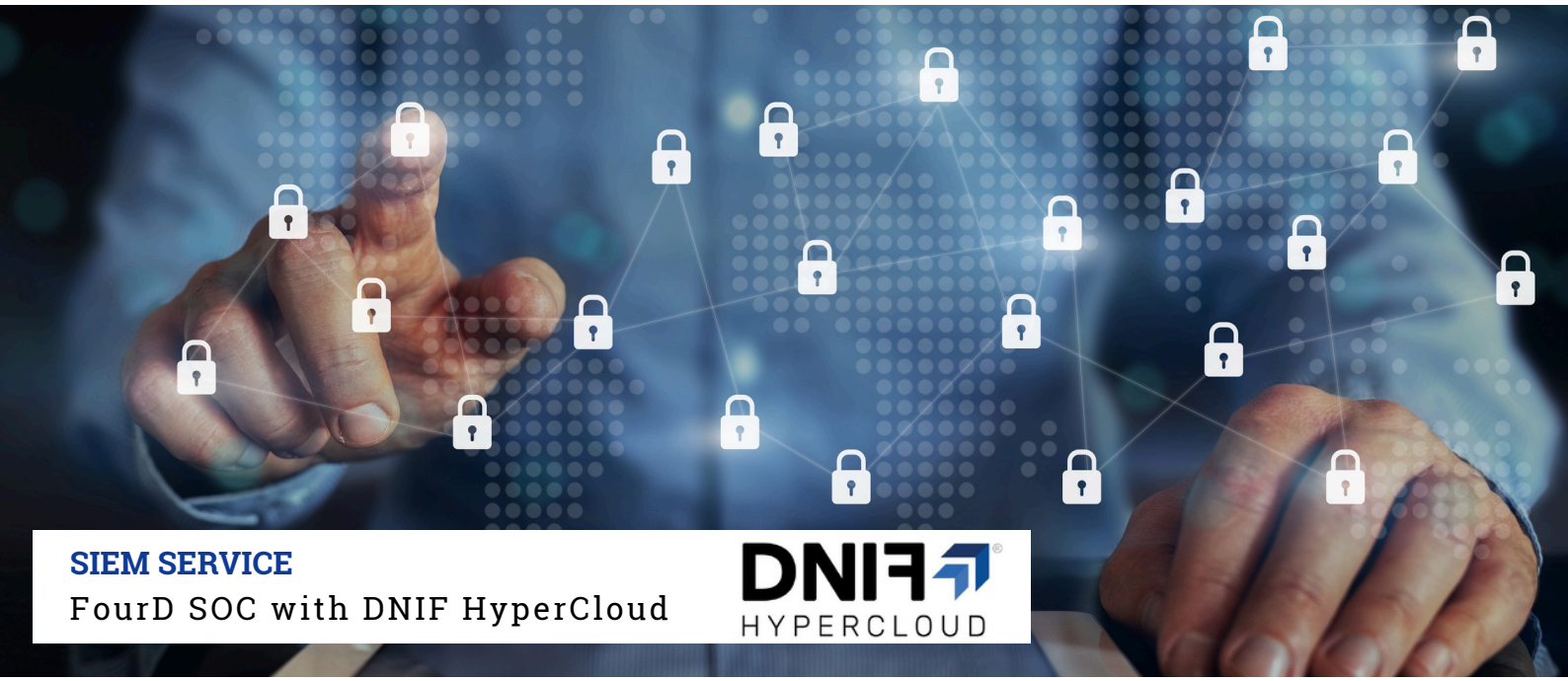

SIEM SERVICE

FourD SOC with DNIF HyperCloud

Client Overview

The client is one of India's leading tyre manufacturers, headquartered in South India, with both domestic and global markets. The organization focuses on manufacturing and technologies like industrial automation and IoT and requires robust data protection measures.

The Challenge:

- **Despite having established cybersecurity measures, the client faced significant gaps in compliance, threat visibility, and the effectiveness of their SIEM platform.**
- **Issues included limited compliance reporting, insufficient log retention, and a lack of enriched threat analytics dashboards.**
- **A device-based licensing model further restricted the integration of critical systems and applications into their SIEM platform, leaving the organization vulnerable to cyberattacks.**
- **Recognizing the urgency, the client sought to enhance their SOC platform and cybersecurity posture.**

The Solution:

Fourth Dimension Technologies implemented a Security Operations Center (SOC) service, featuring the DNIF HyperCloud SIEM solution.

Key improvements included:

- **8x6 Monitoring: Continuous defense against cyber threats.**
- **SIEM Deployment: Integration of all security devices across the organization's infrastructure, including anti-malware, antivirus, and secure web gateway applications.**
- **Volume-Based Licensing: Enabled the onboarding of additional devices for enhanced visibility.**

Sizing:

- **Average Events per Second: 1,000**
- **Total Log Sources: 160**
- **Threat Cases Created: 105**

SIEM SERVICE

FourD SOC with DNIF HyperCloud

Technologies and Tools:

- Firewall
- Load Balancers
- Directory Services
- Endpoint Security
- Linux (Ubuntu)
- IPS/IDS
- Routers & Switches
- WiFi Controllers
- Cloud Services (M365)
- Windows Servers
- Virtualization
- Email Security

Implementation Process:

- The deployment was a collaborative effort between Fourth Dimension and the client's IT team.
- Key steps included:
- Agent deployment on endpoints/servers.
- Enabling syslogs across network devices, including remote branches.
- Secure data logging to DNIF HyperCloud.
- A four-week monitoring and tuning phase to optimize detection and response capabilities.
- The ongoing engagement continues to onboard additional devices and applications for enhanced coverage.

The Results:

- **Strengthened Cybersecurity Posture**: The client's cybersecurity significantly improved with 24x7 monitoring, timely threat detection, and effective incident response. Monthly Cyber Risk and KPI reports offer valuable insights.
- **Incident Detection and Mitigation**: The simulated penetration test demonstrated the SOC's efficiency by quickly identifying and blocking unauthorized activities.
- **Continuous Monitoring and AI Insights**: DNIF HyperCloud's AI-driven analytics correlate thousands of events per second, enabling proactive threat management and ensuring emerging risks are addressed promptly.

Conclusion:

Fourth Dimension's SOC service has transformed the client's cybersecurity posture. Our monitoring, detection, and incident handling enabled the client to focus on their manufacturing operations while trusting their IT environment is secure. We remain a steadfast partner in safeguarding their IT infrastructure.

mail: info@fourdtech.com