IOT SECURITY AS A MANAGED SERVICE

Continuous compliance monitoring for new threats and corrective action:

- L1 and L2 Technical Support
- Cloud Application Hosting Management
- IOT Application and Network Monitoring
- GDPR Compliance
- Security Configuration Management
- Threat and Vulnerability Management
- Security Incident Management
- Storage and Backup
- Disaster Recovery
- OS Hardening and Security Upgrades
- Apply Security Patches and Updates
- Regular Audits and Compliance
- Maintenance Releases Support
- Castanet SaaS

- Offered in partnership with Deutsche Telekom IoT

CASE STUDY - CONTINUOUS VULNERABILITY ASSESSMENT AND REMEDIATION OF POS DEVICES

THE CHALLENGE

Dicks Sporting goods were facing challenges when it comes to protecting their businesses and their customers—from securing online accounts and point-of-sale (POS) systems, to eliminating malware and other vulnerabilities. The security was limited to POS patching - Applications and Operating System. In-house security staff assumed the implementation was solid and that they would be alerted to issues requiring further triage. But when the industry experienced serious security breaches around data and devices, they realized its SIEM was not very useful in detecting and exposing what was occurring inside of the company's IT environment. The company had a bloated security operations center (SOC), yet it lacked a strategic solution for security. Moreover, it was very cumbersome to get data into the outdated SIEM or extract data out of it, and it was impossible to search the data.

THE SOLUTION

Dicks Sporting Goods implemented HARMAN's Castanet their environment. Soon after adopting the platform, the company cleaned up its legacy data and application misconfigurations. The continuous assessment gives them insights into security compliance, gaps, and threats.

HARMAN's Castanet gathers sensitive information about data, devices, and activities and helps them fix the gaps through automated workflow. Dicks are able to maintain 100% security compliance and gain visibility into areas that needs attention. The POS devices get the required patches, and configurations in a well-defined window that ensures no impact on usual business.

The solution works to push important information for analysis. Data is then used to detect patterns, and trends that leads to vulnerabilities. Once detected, the required action is triggered using the automated engine. This is a continuous process, that ensures full compliance of their POS devices.

- Offered in partnership with Deutsche Telekom IoT