Strengthening Automobile and Manufacturing Cyber Security

For a World leading Automobile company based in North America
Project Overview
Implementing Cyber Security and IT Transformation for a Leading Automobile Company in North America

About The Client
World leading Automobile company based in North America

Case Survey
InterraIT’s comprehensive cyber security solution enabled the customer to address security challenges, establish centralized governance, and achieve regulatory compliance while driving business innovation in car manufacturing.

Business Challenges
1. Application, Email, and Endpoint security incidents, network traffic monitoring, and reporting.
   Security Information and Event Management of the payload in its network while managing the varying types of structured and unstructured content
2. Inconsistencies in its cyber security control framework specifically for the control function of Identifying, Protect, Detecting, Responding, and recover
3. Vulnerability scanning and penetration testing to mitigate the application and IT security gaps in Business Continuity planning and system resilience under the Dos and DDos of Cyberattack
4. Need for centralized Governance and monitoring system of their digital assets to maintain regulatory compliances.
5. Lack of integrated Identity and Access Management Policy using Multi-factor Authentication with threshold values of Type I error (FRR), Type II error (FAR), and Cross Over Error Rate (CER)

Our Solutions
1. Set up a team of cyber security professionals of different roles and responsibilities for 24x7 SOC services to manage, monitor, report, advise, and fix real-time threats and malicious traffics.
2. Establish a Business process for Asset and Data classification, Data Life Cycle, Data Remanence, Asset Retention, Data Security controls, and Data Loss Prevention maintaining compliance with NIST SP 800-53, ISO 20000, ISO 20043
3. Set up a centralized authentication model to avert Dictionary attacks, Brute force attacks, and Trojan horse login program attacks.
4. The tool-based implementation governance model, Threat, and vulnerability analysis maintain Compliance with ISO 27001, ISO 27002.
5. Implementation and support of SIEM-based LOG management and reporting as a countermeasure to address various attack surfaces analyzing through STRIDE and DREAD model and setting up Managerial, Operational, and Technical Security control.
6. Implementation and support for tool-based Compliance Governance policy of E-mail to mitigate using Cyber Kill Chain Attack Framework
7. Organize training and awareness programs for Social Engineering threats in addition to Hoax, Pharming, Phishing, Spear Phishing, and Whaling attack

Tools adoption for our solution

Azure Sentinel, AD, O365, Microsoft Cloud App Security, Microsoft Defender ATP, Symantec, PAM Solution CyberArk, IPS/ IDS, Proof Point

InterraIT support model for this engagement

The following diagram will describe overall objectives and corresponding the boundary of InterraIT’s activities in this engagement.