CASE STUDY

Enhancing Cyber Security and Implementation for Business Process Management

For an American pharmaceutical and biotechnology company

Corporate Office

1731 Technology Drive, Suite 760,
San Jose, CA 95110 USA
Tel: +1 408 451 1700
Fax: +1 408 441 7495

Website: www.InterraIT.com
Project Overview

The project focuses on addressing the customer’s challenges related to cyber security incidents monitoring, access control, governance, and vulnerability assessment.

About The Client

One of the largest American pharmaceutical and biotechnology companies

Case Survey

To implement a comprehensive Cyber Security and Business Process Management solution, addressing the challenges, ensuring secure operations, and regulatory compliance.

Business Challenges

1. Lack of proper cyber security incidents monitoring, reporting, availability, Integrity mechanism, digital asset management, and data loss prevention.
2. Inconsistencies in proper Authentication, Authorisation, and Access control mechanisms in integrated IT environment.
3. Need for centralized Governance and monitoring system of their digital assets using a chain of custody to maintain regulatory compliances.
4. Need to set up a proven mechanism to ensure reconnaissance of their IT Security which includes Application, Email, and Endpoint security and vulnerability assessment to prevent cyber threats.

Our Solutions

1. Deployed a highly qualified structured team of SOC and cyber security analysts with different roles and responsibilities to perform reconnaissance of customer’s cyber security policies, tools, infrastructure, and IT assets
2. Conduct Asset and Data classification, establish and update Business processes to maintain Data Life Cycle, Data Remanence, Asset Retention, Data Security controls, Data Loss Prevention maintaining compliances with NIST SP 800- 53, ISO 20000, ISO 20043
3. Set up an Access control mechanism based on the implementation of Authorization using the Clark-Wilson model
4. Set up Major Incident Management, exercising the MIM process to reduce the downtime and restore services to normalcy in the event of any high priority or major incident, and follow through with the RCA and learnings during the post-incident review.
5. Tool-based implementation of due care, due diligence, Risk Management, Threat and vulnerability analysis maintaining Compliance with ISO 27001, ISO 27002.
Our Solutions - Continued

6. Provide 24x7 coverage on their IT security system for threat detection, risk, and vulnerability assessment.
7. Implementation and support for tool-based End Point Detection and Response (EDR) Governance policy (24*7 support), SIEM-based LOG management, and reporting as a countermeasure to address various attack surfaces using STRIDE and DREAD model
8. Implementation and support for tool-based Compliance Governance policy for E-mail security
9. Organize training and awareness programs for customers to mitigate Social Engineering threats in addition to Hoax, Pharming, Phishing, Spear Phishing, and Whaling attack

Tools adoption for our solution
Mimecast, AD, O365, Carbon Black, Firewall, IPS, Splunk, Red Canary, CyberArk, Nessus, CrowdStrike, Tenable, Ivanti, SNOW

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