INNOSEC CASE STUDY

One of the World's E-Commerce Companies Meets the Challenges of Cyber Risk Management through an Integrated Approach

888-311-8650 info@innosec.com

innoSec
INNOVATING SECURITY

OVERVIEW

The client is a multinational retail company that has operations in Europe and the United States. In light of the recent firings and financial impacts to Target, Home Depot and other global retailers, they had report to the board their cyber security strategy and its effectiveness. To provide this information they needed an approach that quantified the cyber risk of their business assets, aligned them to compliance initiatives and their cyber budget. Instead of manually gathering system and vulnerability data from various sources, InnoSec's STORM Cyber Risk Management product offered them an automated solution to demonstrate the level of effectiveness and compliance of their system using dashboards, reports and workflows, while integrating system and vulnerability data from various sources, and consolidating all of it in a centralized database. This has helped the client get a better, quicker, and more real-time view of their cyber security program and how well it worked.

INTRODUCTION

The client's cybersecurity team, headquartered in North America, has the important role of investigating and resolving all cybersecurity issues across the organization's global operations. The team helps ensure that the company is in compliance with regulation and guidelines including GDPR and PCI. The far-reaching consequences include fines of $500K for PCI and 20M+ Euros for GDPR.

Cyber Risk Management is an approach that aligns risk tolerance, cyber insurance needs and the business asset risk. Companies are unprepared to meet the challenges of the dynamic nature of cyber-attacks and stay ahead of attackers. Before, InnoSec's STORM many clients attempted to do this manually and siloed. Systems must be inventoried and data identified between various stakeholders. Security assessments are painful and are done manually. Making matters more challenging, data had to be aggregated from various Security Information and Event Management (SIEM) applications such as IBM QRadar and Vulnerability scanners like Qualys and Rapid7 in a near real time manner.

Keeping track of all this information at a global level is increasingly challenging for the cybersecurity team. At any given point, it was difficult for them to get a complete, real-time view of cyber risk and compliance across the enterprise. The team spent considerable time and effort manually gathering system data from various sources, and doing manual assessments. It quickly became evident that this approach was neither cost-efficient nor scalable. The client needed a new system that would automate risk assessments and management, while also integrating vulnerabilities from across global operations and applications into a central database for complete visibility.

SOLUTION

Among all the cyber security solutions providers evaluated by the client, InnoSec was chosen based on the advanced capabilities and configurability of their offering.

InnoSec's STORM Cyber Risk Management Application has inventoried approximately 1200 systems in the client organization, preformed a business impact analysis (BIA) and confidentiality, integrity and accessibility analysis (CIA) to measure the inherent risk of the systems and align it to risk tolerance and cyber insurance needs. The application streamlines and automates the assessment process and cyber security management lifecycle – right from system identification

innoSec
INNOVATING SECURITY

and classification, risk assessment, vulnerability impact, notification, action plan management, and resolution.

All cybersecurity team members, including compliance manager, business owners, remediators, cyber security team are mapped to their specific roles and processes in STORM, thereby enhancing accountability and transparency. Each user has a dashboard, reports and workflows that allows them to seamlessly work together.

STORM also integrates with change management databases like ServiceNow or BMC, Vulnerability scanners like Qualys or Rapid7, and SIEM tools such as IBM QRadar and BMC Remedy Software, capturing critical information, including systems, vulnerabilities potential breaches and SIEM artifacts (affected system logs, incident reports, vulnerability information of affected assets, threat advisories/ zero day alerts). STORM then consolidates this data along with the cyber security risk assessment information in a centralized database demonstrating residual risk. This has made it easier for the client to track and manage compliance, risk and remediation work. In addition, a range of advanced reports provide complete, real-time visibility into the status of each system.

Below is a glimpse into the InnoSec's STORM Cyber Risk Management capabilities at the client organization:

CYBER RISK ASSESSMENT

Whenever a new assessment is started, STORM identifies all the systems in scope for the assessment by taking data from change management data bases like ServiceNow or BMC and categorizing the data in the systems. STORM allows the location and classification to be logged in the system, and assigns a business and system owner who monitors the system through the assessment.

STORM captures detailed information about the organization, business unit, processes, systems and devices including the purpose of use and demonstrates the relationships in a system tree.

This demonstrates multiple levels of information in a parent/child manner. Controls are inherited from lowest to highest allowing a complete assessment down to the device level.

As the assessment is completed, components escalate severity rating, and impact. It also helps categorize the information into various types based on pre-defined criteria, and can do multiple assessments simultaneously.

Users can also add business context to the data (i.e. remediation plan, budget, and business impact). STORM also helps in qualitative and quantitative impact analysis, and supports correlation of the assessment with past data to enable quick analysis, and to support decision-making on the need for remedial action.

RISK ALGORITHMS

STORM's risk engine is a set of algorithms that are used to calculate inherent and residual risk based on the business impact and confidentiality, integrity and accessibility impact to each system.

REMEDIATION AND BUDGETING

STORM routes each incident/event for review and analysis to authorized users based on pre- configured rules for review, approval, and disposition. The application's decision-tree functionality helps identify reportable events, as well as the type of report that needs to be filed. Remediation data is captured from external sources via STORM's interfaces to third-party products.

Through STORM, remediation project and task owners can add more details about the work, edit its description, and attach further evidence/ files. STORM allows for thresholds that map the findings to the severity level of the findings -- Critical, High, Medium, or Low, supported by a color-coded chart (e.g. Red = Critical, Amber = Medium, Green = Low). These severity levels indicate how soon the findings needs to be resolved. For instance, a critical finding would need to be resolved in 10 days, while a low severity case can take up to 30 days. Each remediation can be documented with the capital and operational expenditures needed to lower the risk to acceptable levels providing a cyber budget.

STORM captures the remediation plan for investigating or resolving the finding. For instance, if a virus has infected a system, the remediation plan might be to test the system controls, and determine what went wrong, what was impacted, and whether or not additional controls are required. All these steps are outlined in STORM, and assigned to a task owner along with predefined timelines. Once the action items have been performed, the task owner enters the results in STORM, and routes it to a task approver for final review, approval, and closure.

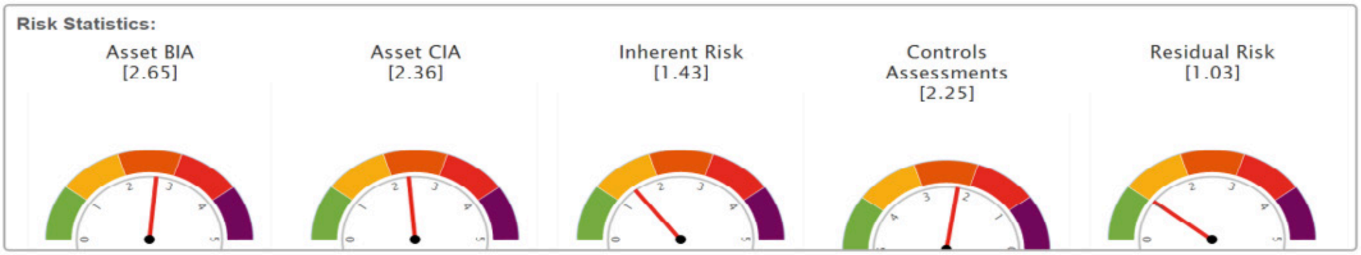
RISK ASSESSMENT MONITORING AND REPORTING

STORM's Cyber Risk Management product provides a window into the effectiveness of the cyber security program demonstrating the inherent and residual risk of each system, defines the amount of cyber insurance needed based on the strategy and risk tolerance and aligns this data to cyber budgeting needs. It also tracks the progress/ status of the risk assessment against pre-defined thresholds triggering alerts when thresholds are exceeded.

STORM automatically populates the risk impact report with data. Therefore, at the click of a button, boards and executives (risk owners) get access to key reports such as crown jewel assets, cyber budgeting, findings across the organization, as well as the remediation work plan and an audit trail report. Powerful dashboards provide in-depth visibility into findings data and statistics such as risk metrics, compliance, severity of findings, outstanding open findings, types of findings, and sources of findings. Users can slice and dice this data from various perspectives to identify trends and areas of concern, and to make informed decisions.

INTEGRATION WITH SECURITY INFORMATION AND EVENT MANAGEMENT SYSTEMS

STORM has API connectors that link to SIEM tools such as IBM QRadar and BMC Remedy Software to capture and import security incidents. These incidents are then routed through the usual workflow of investigation and remediation plan management in STORM.



Flip to the next page to see the Benefits of STORM GDPR Solution!

BENEFITS

With the STORM GDPR Solution, the client is experiencing the following benefits:

AUTOMATED ASSESSMENTS

Instead of sifting through multiple cumbersome emails, spreadsheets, and applications, the client now has an automated way to scope and access the risk of the cyber security program. This single source of truth is used to manage and track all the risk and assessment details across the global organization. STORM cuts across business and geographic siloes, integrating all findings into a common database.

BETTER VISIBILITY INTO CYBERSECURITY INCIDENTS

At the click of a button, the client gets a comprehensive, real-time view of all assessment findings. Each finding can be efficiently analyzed from various perspectives. Plus, powerful dashboards and reports help in drawing out insights from the findings to strengthen cybersecurity measures across the organization. For each finding, STORM maintains a detailed incident history, and also tracks the resolution status and key metrics such as loss information.

MINIMAL MANUAL EFFORT

STORM has replaced time-consuming manual processes with automated workflows. This has helped the client accelerate cybersecurity remediation, right from finding identification to resolution. It has also freed up more time for the client to focus on more critical tasks such as findings analysis and cyber threat mitigation.

WHY INNOSEC

The client chose InnoSec for the following reasons:

The competition was "like cracking a walnut with a hammer", too heavy, too costly, no ability to measure risk as the organization required.

InnoSec's product integrated in all the components of a cyber security management program providing a significant ROI.

They didn't have to buy additional applications to get vulnerability, compliance, risk and asset management. It is all included in our offering.

InnoSec is the market leader in enterprise-wide Cyber Risk Management and Compliance. InnoSec solutions are used by leading global corporations in diverse industries such as Financial Services, Healthcare, Life Sciences, Energy and Utilities, Food, Retail, CPG, Government, Hi-tech and Manufacturing to manage their risk management programs, regulatory and industry-mandated compliance and other corporate governance initiatives.

Email: info@innosec.com
US: +1-888-311-8650
Israel: +972-58-412-0028

innoSec
INNOVATING SECURITY