INNOSEC
CASE STUDY

One of the World's Largest Pharmaceutical Companies Meets the Challenges of GDPR through an Integrated Approach

Copyright InnoSec Ltd. 888-311-8650 info@innosec.com

innoSec
INNOVATING SECURITY

OVERVIEW

The client is a multinational pharmaceutical company that has operations in Europe and America. In light of the recent Global Data Protection Regulation (GDPR), they had to identify which systems had GDPR data and determine how to do a Privacy Impact Assessment (PIA) on these systems. Instead of manually gathering system and vulnerability data from various sources, InnoSec's STORM Cyber Risk Management product offered them an automated solution to scope the GDPR PIA and demonstrate the level of confidentiality and integrity of the 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 GDPR compliance across the global organization.

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, PCI, ISO and HIPAA. The far-reaching consequences include fines of $500K for PCI and 20M+ Euros for GDPR.

The GDPR is a new regulation. Companies are unprepared to meet the challenges. Many of the steps that are required are currently largely manual and siloed. Systems must be inventoried and EU personal data identified between various stakeholders. Security assessments are painful and are done manually.

Making matters more challenging, the integrity and confidentially of the system must be demonstrated. Additionally, 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.

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 GDPR 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 GRPR assessments, 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 its offering.

InnoSec's STORM Cyber Risk Management Application has inventoried approximately 5000 systems in the client organization to measure the confidentiality and integrity of the systems to ensure they meet article 5 and 32 of the regulation across the global enterprise. The application streamlines and automates the assessment process and cyber security management lifecycle – right from system identification and classification, privacy impact assessment, vulnerability impact, notification, remediation plan management, and resolution.

All cybersecurity team members, including compliance manager, business owners, remediators, and the cyber security team are mapped to their specific roles and processes in

innoSec
INNOVATING SECURITY

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 SIEM tools such as IBM QRadar, Qualys, Rapid7 and BMC Remedy Software, capturing critical information, including 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 other cyber security risk and assessment information in a centralized database. This has made it easier for the client to track and manage compliance. 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 GDPR Assessment capabilities at the client organization:

GDPR ASSESSMENT INITIATION

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. The confidentiality and the integrity of the system is measured using STORM's powerful risk engine. 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.

FINDINGS

Each finding impacts the residual risk of the system. 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 3 days, while a low severity case can take up to 30 days.

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 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.

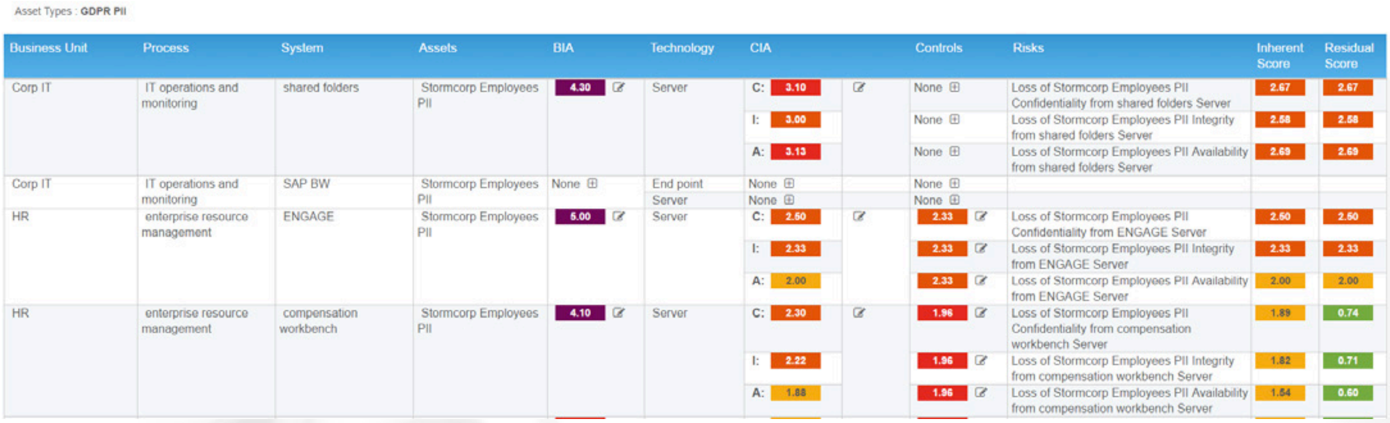
PRIVACY IMPACT ASSESSMENT AND REPORTING

At each stage of the PIA assessment, STORM tracks the progress/ status of the assessment against pre-defined timelines (i.e. 5 days for analysis, 2 days for validation, 14 days for remediation).

STORM automatically populates the privacy impact assessment report with data. Therefore, at the click of a button, auditors get access to key reports such as a list of all findings across the organization, as well as a remediation work plan and an audit trail report. Powerful dashboards provide in-depth visibility into findings data and statistics such as % compliant, confidentiality scores, integrity scores, risk ratings, 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 CHANGE MANAGEMENT DATABASES, SECURITY INFORMATION AND EVENT MANAGEMENT SYSTEMS AND VULNERABILITY MANAGEMENT SYSTEMS

STORM has API connectors that link to Change managements systems like ServiceNow and BMC, SIEM tools such as IBM QRadar and vulnerability scanners like Qualys and Rapid7 that capture and import system information, security incidents and vulnerabilities.



Asset Types : **GDPR PII**

Business Unit	Process	System	Assets	BIA	Technology	CIA	Controls	Risks	Inherent Score	Residual Score
Corp IT	IT operations and monitoring	shared folders	Stormcorp Employees PII	4.30	Server	C: 3.10	None ⊞	Loss of Stormcorp Employees PII Confidentiality from shared folders Server	2.67	2.67
						I: 3.00	None ⊞	Loss of Stormcorp Employees PII Integrity from shared folders Server	2.58	2.58
						A: 3.13	None ⊞	Loss of Stormcorp Employees PII Availability from shared folders Server	2.69	2.69
Corp IT	IT operations and monitoring	SAP BW	Stormcorp Employees PII	None ⊞	End point	None ⊞	None ⊞			
					Server	None ⊞	None ⊞			
HR	enterprise resource management	ENGAGE	Stormcorp Employees PII	5.00	Server	C: 2.50	2.33	Loss of Stormcorp Employees PII Confidentiality from ENGAGE Server	2.50	2.50
						I: 2.33	2.33	Loss of Stormcorp Employees PII Integrity from ENGAGE Server	2.33	2.33
						A: 2.00	2.33	Loss of Stormcorp Employees PII Availability from ENGAGE Server	2.00	2.00
HR	enterprise resource management	compensation workbench	Stormcorp Employees PII	4.10	Server	C: 2.30	1.96	Loss of Stormcorp Employees PII Confidentiality from compensation workbench Server	1.89	0.74
						I: 2.22	1.96	Loss of Stormcorp Employees PII Integrity from compensation workbench Server	1.82	0.71
						A: 1.88	1.96	Loss of Stormcorp Employees PII Availability from compensation workbench Server	1.54	0.60

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 PIA

Instead of sifting through multiple cumbersome emails, spreadsheets, and applications, the client now has an automated way to scope and access the confidentiality and integrity of the system. This single source is used to manage and track all the 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 and compliance, 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 and compliance program providing a significant ROI.

Clients 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

Copyright InnoSec Ltd. 888-311-8650 info@innosec.com