AUJAS CYBERSECURITY

NSE NSEIT

CASE STUDY - RISK ADVISORY SERVICES

Automated threat and security incident response solution by using RSA Archer for a telecom major

CHALLENGE

A global telecom major with best in class technology assets did not have the appropriate security governance and testing framework to secure its business. The company lacked the tools, processes, and methodologies to manage threats and vulnerabilities. They wanted Aujas to create a comprehensive, automated threat and incident management framework to manage threats.

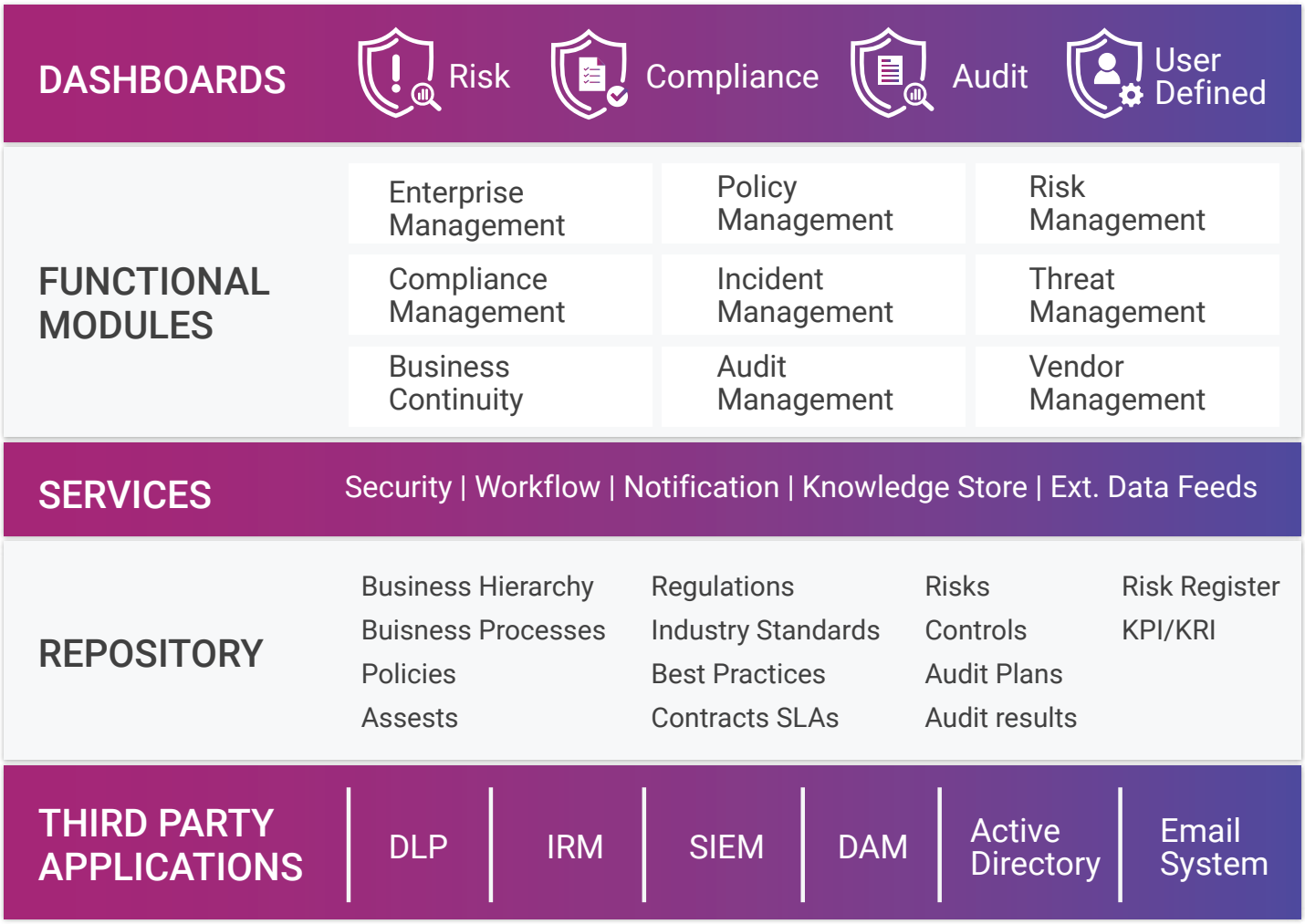
SOLUTION

Aujas created a threat management framework which comprised of security governance, asset and vulnerability management processes, threat analysis, and integrated with the security incident management procedures.

The framework was automated using RSA Archer eGRC solution to focus on proactive threat analysis. Archer threat management module was leveraged to consolidate threat feeds, security and vendor advisories, analysis of SIEM feeds, vulnerabilities, and configuration weaknesses. This consolidation helped in predicting the most likely exploitable vulnerability in critical assets and enabled in prioritizing remediation tasks. Reactive incident management ensured the appropriate handling of unforeseen security incidents.

Three RSA Archer modules were leveraged to design the threat and security incident response framework.

Three RSA Archer modules were leveraged to design the threat and security incident response framework.



RSA ARCHER OVERVIEW

ENTERPRISE MANAGEMENT: To build an asset repository and link it with business processes, “contacts” to build workflows for escalation, reporting, and notifications.

THREAT MANAGEMENT: To integrate proactive threat intelligence with tools to analyze the probability of exploitation and complement with professional security advisories and integrated threat feeds.

INCIDENT MANAGEMENT: To integrate proactive threat intelligence with tools to analyze the probability of exploitation and complement with professional security advisories and integrated threat feeds.

APPROACH

Plan	Design	Implement & Operate	Sustain & Enhance
Engagement kickoff meeting with the key stakeholders to finalize scope & requirements Establish project management rules (detailed project plan, resource plan, communication & escalation plan, status report templates, quality checklists, etc) Identify key stakeholders, develop interview questionnaires and schedule interviews to understand status quo	**Governance & Processes** • Identify the asset register with details such as owners and custodians, and freeze on the classification • Develop a classification policy • Define processes for information threat escalation & closure • Create an IT security threat assessment methodology • Design IT security threat management solution **Business & Technical Requirements** • Identify and document business & technical requirements for automation an integration	**Technology Selection** • Evaluate available GRC tools and technology solutions based business and technology needs • Select the technology solution **Archer eGRC Implementation** • Manage the implementation and integration of Archer eGRC solution • Develop test plans and conduct user acceptance testing	**Archer eGRC Operations Management** • Perform administration activities (access grant & revokes) • Track assessments • Validate assessments • Generate reports

OUTCOMES

- Enhanced security posture
- Improved return on investments
- Centralized and automated threat management
- Improved visibility on the enterprise-wide security status
- On-demand reports for decision support, leadership teams, and auditors

ABOUT AUJAS

Aujas cybersecurity is an enterprise security service provider for organizations across North America, Asia Pacific, and EMEA regions. Aujas has deep expertise and capabilities in Identity and Access Management, Risk Advisory, Security Verification, Security Engineering & Managed Detection and Response services. By leveraging innovative products and services, Aujas helps businesses build and transform security postures to mitigate risks. The service focus is to strengthen security resilience by minimizing the occurrence of sophisticated attacks and threats while offering 360-degree visibility and protection across enterprise infrastructure.

For more information, do visit us at www.aujas.com

You can also write to us at contact@aujas.com