NuSummit Cybersecurity

cybersecurity.nusummit.com

SOLUTION BRIEF

Integrated Security Assurance Program (iSAP)

Applications and their underlying technology stack serve as the foundation of digital transformation for modern businesses, but as they evolve ensuring their security presents a significant challenge. This is where the Integrated Security Assurance Program (iSAP) plays a critical role. iSAP is a comprehensive approach designed to secure applications and infrastructure in development, deployment & operation phases. By embedding security practices, tools, and processes at different stages of system lifecycle, iSAP provides a unified view of threats and vulnerabilities, ensuring proactive risk management and enhanced security

Why Do Organizations Need iSAP?

Organizations often face several critical challenges when it comes to managing Information Security, including:

Fragmented Visibility

Security data spread across multiple tools and platforms causes a lack of unified visibility, making it challenging to track vulnerabilities effectively across applications and infrastructure.

Lack Of Collaboration

Limited communication and coordination between development, security, and operations teams resulting in slower remediation and prolonged risk exposure.

Manual Processes

Dependency on manual processes for identification, prioritization, and remediation of vulnerabilities slows down the time to market.

Inefficient Prioritization

Inability to effectively correlate and prioritize vulnerabilities reported across the technology stack, increases the risk of exposure.

How Does iSAP Solve These Challenges?

iSAP tackles key security challenges by integrating people, processes, and technology, including:

Ensure Compliance

Meet industry standards and regulatory requirements, minimizing compliance risks.

Accelerate Time-to-Market

Automate security in CI/CD pipelines to deliver secure applications faster.

Standardize Security Practices

Ensure consistency by adopting industry-leading security protocols across all teams.

Safeguard Application Integrity

Safeguard applications from emerging threats, ensuring data integrity and preventing breaches.

Strengthen Security Posture

Embed security at every phase of the application lifecycle, from design to deployment, to continuously improve defense mechanisms.

Minimize Risk Exposure

Identify and remediate vulnerabilities across IT environment, reducing the attack surface and improving risk mitigation efficiency.

Increase Visibility and Transparency

Integrate dashboards to provide real-time, centralized views of vulnerabilities generated from various sources across IT landscape.

Prioritize Critical Risks

Leverage advanced threat intelligence and risk assessment frameworks to identify, rank, and address the most critical vulnerabilities first, ensuring optimal resource allocation.

NuSummit Cybersecurity's Three-Dimensional iSAP Approach

NuSummit Cybersecurity implements security by design using a three-dimensional approach to people, processes, and technology.

People	Process	Technology
Governance: Define KPIs and metrics to measure the effectiveness of security controls and processes.	**Secure SDLC** : Assessing security requirements at each stage of the SDLC and shifting security activities to the left.	**Advanced Tools:** Use tools for Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and Software Composition Analysis (SCA).
Collaboration: Enhance communication across teams to ensure shared security goals.	**Secure Development:** Integrate secure coding practices and automated vulnerability scans into the CI/CD pipeline.	**Automation:** Quicken vulnerability detection and remediation through integrated, automated testing tools.
Learning and Development: Run training programs to update teams on the latest security threats and best practices.	**Security Testing**: Utilize a combination of static and dynamic testing methods to identify risks from applications.	**Analytics and Reporting**: Centralized dashboards provide detailed, real-time security insights, helping teams make informed decisions.
	Continuous Improvement: Conduct regular audits and feedback loops to refine security processes over time.	

Key Benefits

By augmenting ISAP with a vulnerability management platform, organizations gain the following key benefits:

Unified Visibility

Gain a single, unified view of security risks across applications, infrastructure, and cloud environments.

Accurate Prioritization

Leverage AI-powered insights to prioritize and address critical vulnerabilities.

Efficient Remediation

Automate workflows and streamline remediation processes, significantly reducing manual overhead.

Real-Time Insights

Utilize role-based reports and dashboards to track security performance and Service Level Agreements (SLAs) adherence.

Faster Time to Market

Automated security processes help accelerate development cycles while maintaining high levels of security and compliance.

Cost Savings

By automating manual security processes and reducing vulnerabilities earlier in the SDLC, organizations can save costs related to remediation and compliance issues.

Success Stories

Application and Infrastructure Security Program
For **A Global Healthcare Corporation**

Business Challenge

The client required security assessments for healthcare applications, including web apps, APIs, and cloud components, while adhering to healthcare protocols like DICOM and HL7.

Solution

NuSummit Cybersecurity experts performed end-to-end security testing for web applications and APIs. Our cloud security experts focused on ensuring the security of underlying cloud infrastructure and its components.

Business Impact

The extensive security testing performed by NuSummit Cybersecurity's security experts during each phase of the product lifecycle identified critical security gaps in applications and cloud components. By implementing the security measures recommended by NuSummit Cybersecurity, the client could elevate the security of clinical applications and diagnostic solutions before delivering them to their end users. Likewise, the comprehensive risk assessments conducted aided the client in complying with the regional privacy regulations of the healthcare sector.

Application and Cloud Security Program for **An American Technology Corporation**

Business Challenge

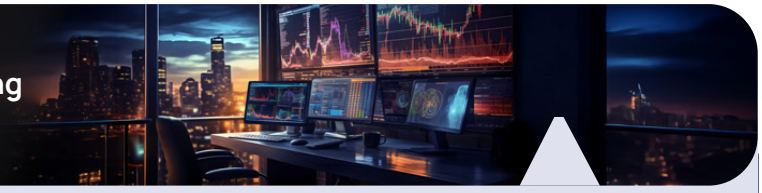
The client needed to manage dynamic security analysis and cloud security operations for applications distributed across multiple geographies.

Solution

We established a team of 18 certified professionals to conduct security assessments, guide stakeholders through identified vulnerabilities using a vulnerability management platform and manage cloud security incidents across AWS and Azure environments. NuSummit Cybersecurity .

Business Impact

The client achieved enhanced security for applications globally, maintained regulatory compliance, faster time to market and accelerated remediation, and improved their ability to respond to security incidents.



Appsec Program For **A Large Trading Finance Corporation**

Business Challenge

The client required a comprehensive security program to manage an ecosystem of over 200 applications, with 75-100 sprint releases each month. Ensuring security testing, vulnerability management, and adherence to regulatory requirements at scale was a significant challenge.

Solution

We set up a hybrid delivery model with a program lead in the USA, supported by a team of 30 AppSec professionals from onsite and offshore centres. The team tested applications, conducted security code reviews, and automated security for audit and regulatory compliance.

Business Impact

Automation implemented by NuSummit Cybersecurity's security engineers across various platforms improved security testing efficiency and ensured compliance with sprint releases for the client. The automated metrics measurement developed by NuSummit Cybersecurity enabled efficient remediation implementation.

About NuSummit Cybersecurity

NuSummit Cybersecurity helps build and transform cybersecurity postures to enable businesses to mitigate risks. We are a pure-play cybersecurity services company with deep expertise in Identity and Access Management, Risk Advisory, Security Verification, Managed Detection and Response, and Security Engineering services.

Our unique products and services help businesses build and transform security postures while mitigating risks. Our focus is to strengthen security resilience by minimizing the occurrence of attacks, threats, and risks so that you can drive change, innovate, and accelerate growth.

For more information, visit us at **cybersecurity.nusummit.com** or write to us at **cybersales@nusummit.com**

Dallas I Jersey City I Cupertino I Ottawa I Riyadh I Dubai Mumbai I New Delhi I Bangalore

Follow us at: