LTIMindtree

Whitepaper

Achieving Applications Security Maturity

Bring resiliency and Speed to software applications without losing an edge, plus lessons from an industry leader.

Authored by:

Sanjay Bhutada

Principal Director – Cybersecurity

Table of Contents

A digital-first approach moves application security to the top CISO/CSO priority 3

The new imperatives 3

Challenges of a modern-day CISO 4

Application security landscape 5

Case in point- journey of an American manufacturer 5

Objective 6

How it started? 6

Customer's application security testing roadmap 7

Benefits delivered 7

The 4 levers that contributed to the customer's successful program 8

Tools and technology 8

People 8

Processes 8

Culture 8

Application security CMM alignment mapped to NIST- illustration 9

8 ways to inch your company closer to app sec resiliency 10

CISO imperatives for outsourcing 11

Partnering in your transformation journey 13

What sets LTIMindtree apart? 13

About the Author 14

References 15

A digital-first approach moves application security to the top CISO/CSO priority

For most applications, security is now at the top of the agenda. Applications are the lifeline of the modern-digital enterprises. Application security touches many aspects of the enterprise and across all layers. Effective planning is critical to aligning the application security architecture with the new age cloud and digital strategy and the risk landscapes.

Applications have been a prime target for cyberattacks. Unfortunately, many organizations have a software development lifecycle (SDLC) that lacks rigor and discipline. It is imperative to incorporate security into the SDLC with proper policies, skills, activities, and controls. Many organizations still struggle to adapt and improve their application security to keep pace with development cycles.

App Sec must be integrated into every stage of the development pipeline to succeed and incorporate industry standards such as National Institute of Standards and Technology (NIST). This point of view outlines how to plan for and implement an effective Application Security program.

The new imperatives

- Application security approaches need to keep up with dynamic multi-cloud and hybrid environments.
- The new approaches need to be aligned with the new ways of working, keeping in mind risk prioritization given the limited budgets available.
- Automation and cultural change are essential to DevSecOps and vulnerability management
- Focused approach to manage the regulatory and compliance requirements such as SOX, PCI DSS, and HIPAA.

Challenges of a modern-day CISO

Setting up security best practices, ensuring compliance, and protecting enterprise data with minimum budget and high ROI.

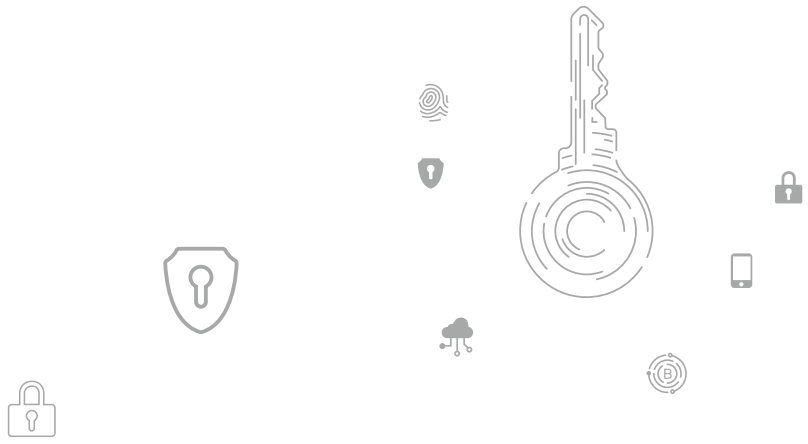
A modern-day Chief Information Security Officer (CISO) is no longer just the custodian of enterprise security. They are more a strategist than a technologist. Their job is not just to ensure that the enterprise is secure but also to make sure that the enterprise can save costs, ensure compliance, and use security as a strategic differentiator. All this requires a lot of planning and investments. There are countless challenges that make a CISO's job challenging. Some of the most prominent challenges that a CISO faces are:

Low budgets: Budgetary constraints act as a huge roadblock when setting up a modern security landscape, hiring the right team, and finding the best possible tools and technologies.

Justifying ROI: Not only are CISOs facing the issue of lower budgets, but they are often finding it hard to explain the ROI for security programs. Organizations need to understand that cybersecurity is not a direct profit center, but if you ignore it, you are simply putting your business in jeopardy.

Limited team: Organizations often don't have a large in-house security team to support the CISO. This lack of support makes it challenging for a CISO to implement security measures on many occasions.

Dynamic environment: There are numerous apps, countless systems, legacy infrastructures, and an ever-evolving threat landscape.



Application security landscape

Every day, hackers hack an average of **30,000** websites[1]

There is an attack somewhere on the Internet every **39** seconds[2]

Malware is spread via email about **94%** of the time[3]

The Internet blocks an average of **24,000** malicious mobile apps every day[4]

According to FireEye, a cybersecurity company, around **18,000** organizations had malicious code in their networks, of which **50** suffered major breaches[5]

As of today, there are **19000+** vulnerabilities listed in the Common Vulnerabilities and Exposures (CVE) database [6]

Application development security and cloud security is a fast-growing skills area projected to grow **164%,** and **115%** respectively between 2020-2025 [7]

Case in point- journey of an American manufacturer

Our customer is a global leader in manufacturing. Their business has market strength from cost to safety, recyclability, and proven reliability. They have multiple external web-facing SOX-compliant applications that support critical business functions across sales and marketing, product distribution, HR and finance. The mobile application allows their fleet drivers to perform customer deliveries, capture proof of delivery, receive core returns and capture proof of pickup. Further, they also have a distributor portal system where distributors (customers) can create orders, check status, pay invoices, etc.

They wanted to build a robust application security ecosystem for their enterprise applications (web and mobile) and address them holistically across people, processes, and technology throughout the software development life cycle. Also, it was crucial to ensure that the app development did not stall or even slow down systems.

Objective

- Identification of critical vulnerabilities in the source code. Build a structured application security program.
- Gain in-depth analysis related to the security of critical applications.
- Reduce risk from both internal and third-party sources.
- Keeping customer data secure and building customer confidence.

How it started?

- External facing applications were an immediate area of concern, therefore outside-in application attack surface areas were identified as a vital area of testing.
- Risk-based identification of custom apps, which included multiple parameters for deciding the risk score for every application. These included :
    - Type of applications – Web, mobile, commercial-off-the-shelf (COTS) , thick client, etc.
    - Internal/External facing, PII Data, business critical data, enhancement/change frequency, client risk rating, etc.
    - Based on the above, from a large inventory of applications, approx. 100 applications were identified as application with critical risks.
    - Standardized Software Development Lifecycle (SDLC)Framework – Starting with tool Selection, DAST, and then SAST
- "Security" and "Compliance" mapping and visibility
- Control mapping derived from NIST cyber security Framework

Customer's application security testing roadmap

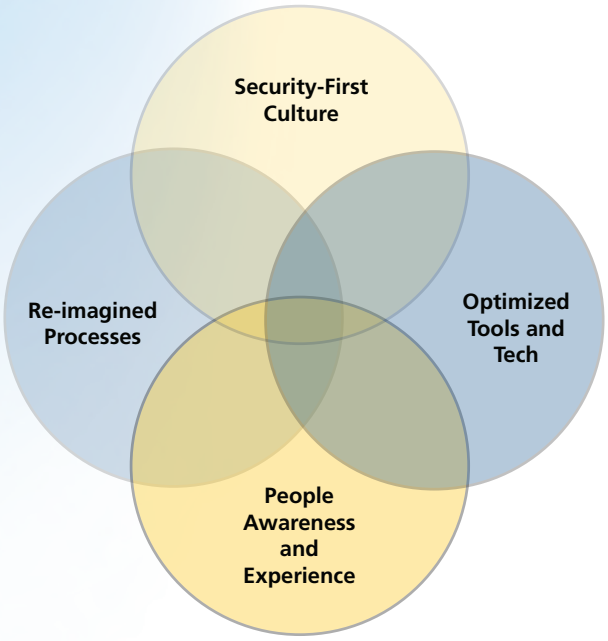
Below are the 8 key focus areas in the AppSec posture improvement and embedding security across the lifecycle of application security.

1. Build a risk-based Application Security Program
2. Standardized SDLC framework, best practices, structured testing plan and workflows, etc.
3. Dynamic Application Security Testing (DAST)
4. Static Application Security Testing (SAST)
5. Implementing and integrating the right security tools in line with their requirement
6. "Security" and "Compliance" Mapping and Visibility
7. Vulnerability Lifecycle Management
8. Shift-left the Security Testing Process thru Next Gen automated transformational services

Benefits delivered

- 40% + improvement in Appsec posture in first 6 months
- Application mapping against NIST and internal compliance guidelines
- On-prem Security testing solutions
- Customized and advanced reports with a call to action
- Established SDLC framework for DevSecOps
- Culture change initiative across various teams

The 4 levers that contributed to the customer's successful program



Tools and technology

- Right choice of on-prem scanning tools in alignment with customer requirement
- A mix of automated and manual scanning
- Parallel scanning tools
- Right tool configurations
- Contextualized and Developer friendly reports

People

- Training and awareness programs
- Situational risk awareness and actionable remediation insights
- Effective communication channels

Processes

- Secure SDLC activities for development teams at each phase
- Third-party security reviews and remediation advisory
- Control mapping derived from NIST Cyber Security Framework
- Red Teams
- DevSecOps integration

Culture

- Structured testing workflow led to seamless assessment and minimal conflicts
- Embed Secure by design principles and controls

Application security CMM alignment mapped to NIST- illustration

NIST CSF Functions	**Level 1:** Initial	**Level 2:** Managed	**Level 3:** Defined	**Level 4:** Quantitatively Managed	**Level 5:** Optimized
Identify	Little to no application security risk identification	Process for application security risk identification exists, but it is immature	Risks to applications are identified and managed in a standard, well-defined process	Threats to the application environment are identified and proactively monitored periodically	Application security risks are continuously monitored and incorporated into business decisions
Protect	Application protection is reactive and ad-hoc	Application protection mechanisms are implemented across the environment	Application is protected in accordance with its classification for business criticality	The application environment is proactively monitored via protective technologies	Protection standards are operationalized through automation and advanced technologies
Detect	Application anomalies or events are not detected in a timely manner	Application anomaly detection is established through detection tools and monitoring procedures	A baseline of "normal" application activity is established and applied against tools/procedures to better identify malicious activity	Continuous monitoring program is established to detect application threats in real-time	Detection and monitoring solutions are continuously learning application patterns and adjusting detection capabilities
Respond	The process for responding to application incidents is reactive or non-existent	Analysis capabilities are applied consistently to application incidents by Incident Response (IR) roles	An IR plan defines steps for application incident preparation, analysis, containment, eradication, and post- incident	Response times and impacts of application incidents are monitored and minimized	The capabilities of all IT application personnel, procedures, technologies are regularly tested and updated
Recover	The process for recovering from application incidents is reactive or non-existent	Resiliency and recovery capabilities are applied consistently to application incidents impacting business operations	A Continuity and Disaster Recovery Plan defines steps to continue critical applications and recover to normal operations	Recovery times and impacts of application incidents are monitored and minimized	The capabilities of all IT application personnel, procedures, technologies are regularly tested and updated

8 ways to inch your company closer to app sec resiliency

1 Evaluate security maturity: Organizations can uncover their current maturity level and then understand the most effective course of action to increase this level quickly and pragmatically while introducing as little disruption as possible to their current development process and in-production application management.

2 Build an application inventory: Create a list of applications, application upgrades, and all identified vulnerabilities for each application to help better prepare against cyber threats.

3 Identify and prioritize vulnerabilities: Identify all vulnerabilities and prioritize them based on the risk level they possess.

4 Identify business criticality and its impact: Organizations must define the most critical business applications and create a robust security program around those. Although it is essential to safeguard business-critical applications, organizations should not leave the other applications alone as they can be a gateway for attackers.

5 Action plan on remediation: A well-documented action plan on countering application vulnerabilities and remediation should be in place and well communicated to everyone in the organization.

6 Massive scanning capabilities: App Sec solutions must have massive scanning capabilities. These solutions should be capable of scanning hundreds and thousands of applications at once, and they should be robust enough to make these scans frequently.

7 Agile method of scanning and eliminating vulnerabilities: App Sec solutions should define what it needs to scan in the next hour, not what it needs to review in the next month. It should be capable of running behind the scenes to find application vulnerabilities and be fast enough to report and eradicate vulnerabilities as soon as they are found.

8 Making security everyone's job: It is essential to ensure that security is not only the responsibility of the security teams but is part of everyone's day-to-day activities. Everyone in the organization should be trained to ensure enterprise security, and well-defined documentation, processes, and programs should be in place to ensure everyone is aware of security best practices.

Exercising more caution with open-source codes, libraries, and tools: Nowadays, it is common for developers to use open-source codes, libraries, and tools for building new applications. Although these open-source solutions have their own advantages, they also have their own vulnerabilities. It is a must for organizations to have checks in place to ensure that no security incidents happen because of open-source codes.

CISO imperatives for outsourcing

Although building a full-time in-house security team sounds like a good idea, it is a challenging task to accomplish. While establishing an in-house security team, a CISO is often faced with challenges like finding and retaining the right talent, making timely and appropriate technology investments, having the right set of advisors, etc.

To overcome these security obstacles, focus more on their core business, and gain access to security expertise, outsourcing this area may look daunting at first. Still, with the correct application security partner, organizations gain a competitive edge that can help them divert their complete attention to the crux of their business while staying completely threat-free.

Some of the key benefits of outsourcing include:

Access to a large talent pool of application security experts: Outsourcing ensures that organizations gain access to these experts without going through the tiresome recruitment and retention process.

Application Monitoring and Governance: 24/7 access to best-in-class solutions with no vendor lock-ins, and the ability to analyze threats and provide engineering solutions.

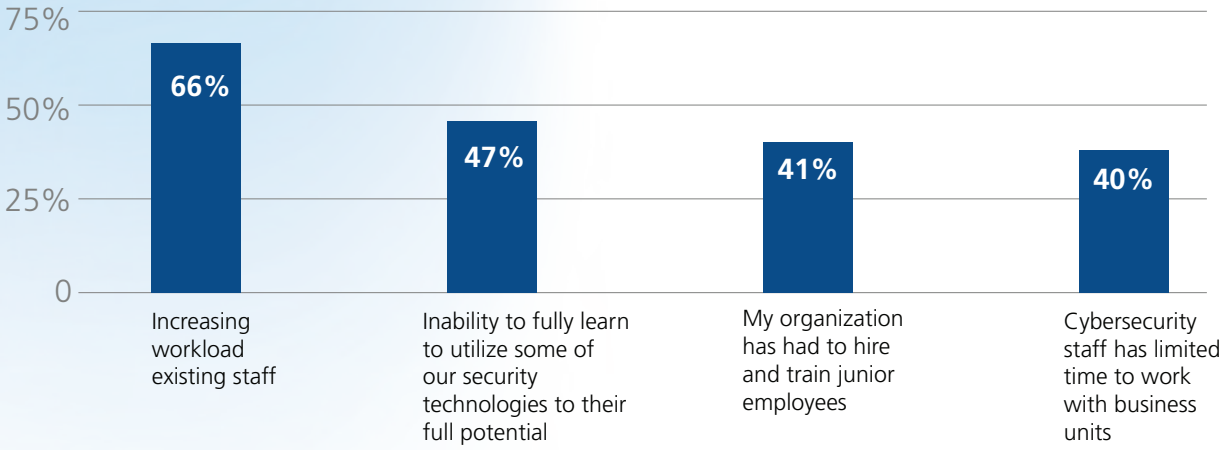
Flexibility and scalability: Organizations are always looking to launch new apps every day and sometimes even every hour. To ensure that these apps are well protected, they need cloud-agnostic security solutions with the flexibility to cover on-premises and SaaS environments. Service Providers are always flexible and provide options to scale up or ramp down operations without many additional investments.

Compliance with the updated regulations and guidelines: Security service providers are up to date with the latest security regulations and policies and advise their clients in employing cybersecurity risk management best practices and implementing PCI and HIPAA security standards.

Reduce the burden of configuration, maintenance, outage, and disruptions: Configuration, maintenance, outages, etc., all such challenges will be managed by the service providers, and the organizations can focus on their expertise.

How organizations are being affected by the cybersecurity skills shortage

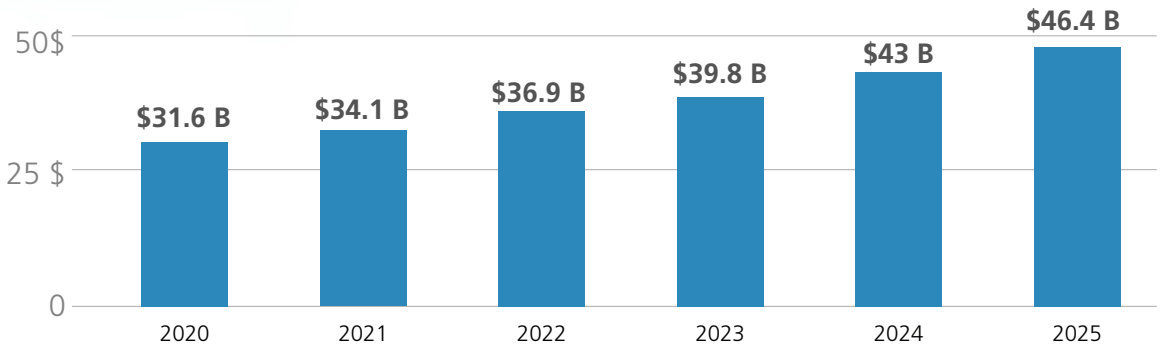
Seventy-four percent of organizations have been affected by the cybersecurity skills shortage



Source: Enterprise strategy group and information systems security association

Steadily managed growth ahead for MSSPs

Due to a combination of heightened security breaches, more sophisticated cyber attacks, more complex technologies and a dearth of talented security pros, enterprises are increasingly turning to managed security service providers.



Source- MarketsandMarkets

Partnering in your transformation journey

At LTIMindtree, we understand that the world today runs on software, and applications are one of the most critical elements of connecting with customers. It is now mandatory for organizations to ensure that their customers are provided a world-class user experience on apps and that their data is protected from cybercriminals.

As a global end-to-end managed security services provider, we understand the security needs of our customers and formulate a mature application security program to ensure their applications remain secure with the changing threat landscape.

What sets LTIMindtree apart?

- LTIMindtree has extensive experience working with multiple global enterprises, including fortune 500s, in their security programs.
- Expertise to provide end-to-end managed security services to ensure that our customers can rely on us for their complete security needs, not just application security.
- Deep technology partnerships with most of the large security software makers and, therefore, has access to all the latest tools, technologies, and early product roadmap.
- At LTIMindtree, we make extensive use of the latest technologies like AI and ML for automation led tool expertise – Nextgen solutions to address client security testing needs.
- At LTIMindtree, we follow DevSecOps and embed security into every stage of the application development cycle.
- Our resources are certified in CEH, OSCP, ECSA, ISO 27001 lead auditor, etc.
- Ready-to-use checklists and templates across domains implementing best practices such as ISO, PCI DSS, NIST, OWASP, HIPPA, SANS, etc.

To know more about our application security services, **talk to our experts today.**

About the Author

Sanjay Bhutada

Principal Director – Cybersecurity

Sanjay is an industry veteran with over 24 + years of experience in cybersecurity. He is leading the advanced threat and vulnerability management practices globally at LTIMindtree. He has been instrumental in introducing technology-enabled managed services in SecDevOps, infrastructure and application security, red teaming, breach attack simulation. Sanjay's diverse experience has led to innovative solutions and best practices in alignment with the security strategies and objectives of multiple Fortune 500 clients. Throughout his career, Sanjay has been instrumental in driving and introducing real-time visibility of Security posture and quantified risk scoring to achieve prioritized focus and better regulatory compliance adherence for clients across continents.

References

http://www.sophos.com/medialibrary/pdfs/other/sophossecuritythreatreport2012.pdf%20

https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds

https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/istr-23-cyber-security-threat-landscape

https://www.bbc.com/news/world-us-canada-55386947#:~:text=Kevin%20Mandia%2C%20CEO%20of%20FireEye,known%20to%20have%20been%20targeted.

https://cve.mitre.org/cve/

https://www.globenewswire.com/en/news-release/2022/03/21/2407041/0/en/Application-Security-Global-Market-Report-2022.html