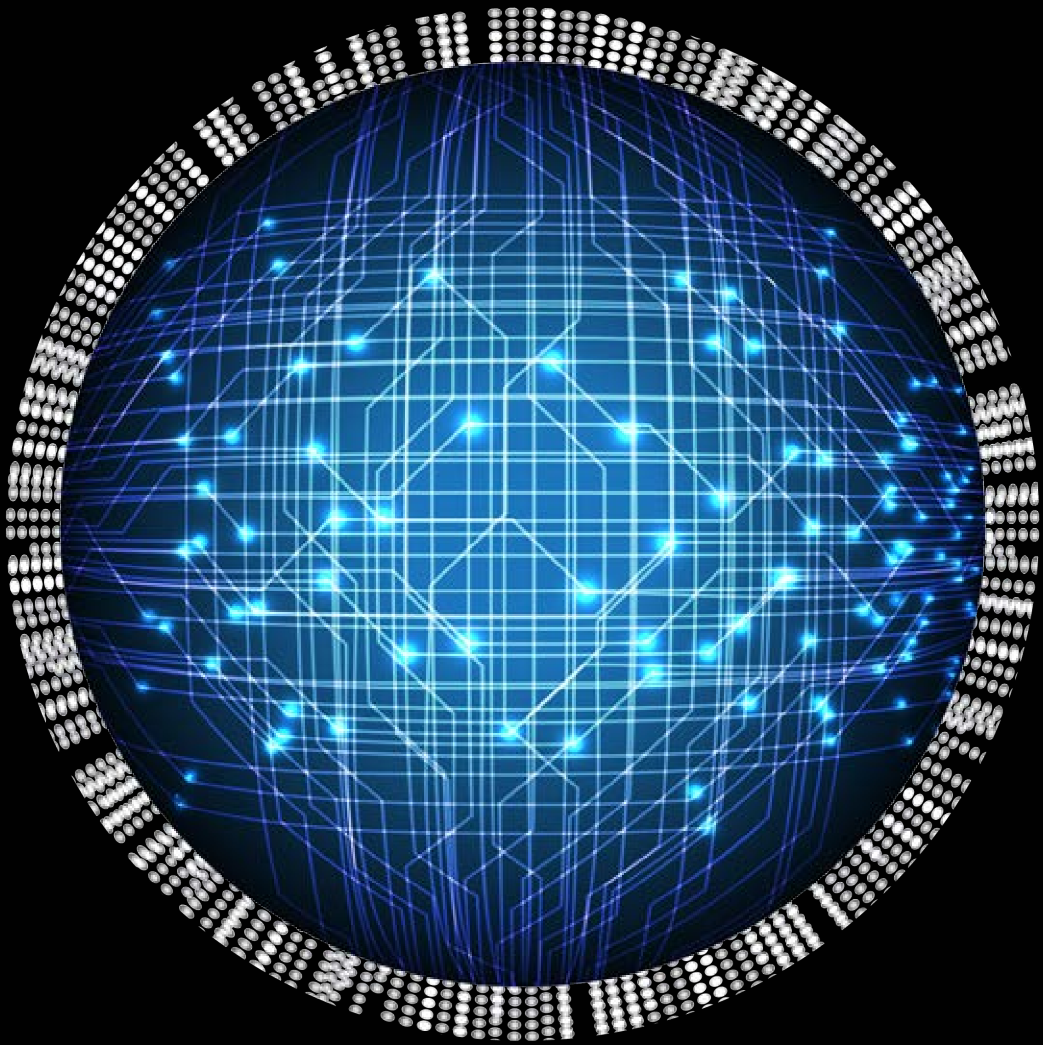
Deloitte.

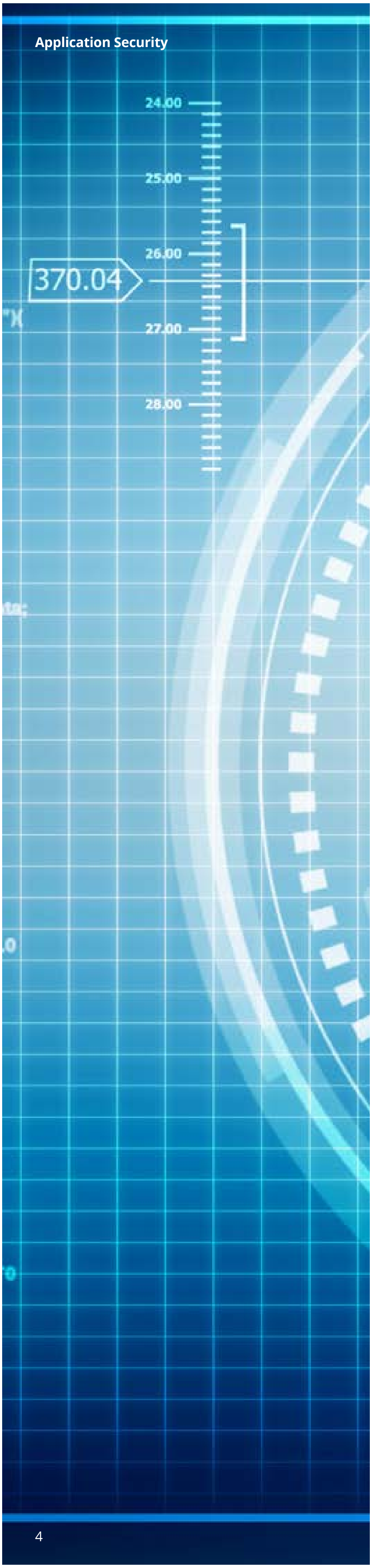


# Application Security

June 2018

Risk Advisory

# Contents



# Cyber Risk Managed Services – Application Security

Every organization reaches out to its consumers by all possible mediums. This includes Web and Mobile applications. However, most have inadequately secured their applications, leading to cyber attacks we experience every day.

## A fresh approach

Given the complexity of today's environment, the traditional approach of securing applications in silos is not an effective way of handling security. There is a need for a much more radical approach which should be robust, scalable, and able to connect with dynamics of application. Selecting the right tool sets that can effectively identify the vulnerabilities is an important component of this approach, along with skilled resources who have the expertise to interpret and provide solutions.

## Managing risk – Where to begin?

Many organizations fail to prioritize application security, leaving their entire environment at risk. With large organizations managing thousands of applications, it is prudent to adopt a risk-based application security management. To begin with, we need to adopt a framework that covers the following –

- Build an application inventory
- Identify business criticality and its impact
- Identify and prioritize vulnerabilities
- Action plan on remediation

## Today's Challenges

Applications are easy targets
"Internet facing applications are the easiest to attack; the latest trend depicts the same."

Complexity and volume of applications
"Today's business deals with large volumes in terms of size and complexity of applications."

Inherent vulnerabilities and gaps
"Inherent gaps in the coding standards adopted coupled with volume of applications create a huge challenge."

Risk Identification and Prioritization
"These are dependent on the tools used, skill set of resources, and maturity of managing application vulnerabilities."

Regulatory and Compliance requirements
"Every business is bound by regulatory compliance requirements such as SOX, PCI DSS, and HIPAA."

# A Comprehensive Security Solution for Applications

Securing applications is a multi-faceted activity that needs a thorough understanding of the application behavior and its various functionalities. More than half of all breaches involve web applications—yet less than 10% of organizations ensure all critical applications are reviewed for security before and during production.

## Stage 1: Protection during design and development

### Static Code Analysis (SAST)

- Apart from protecting the applications from external attacks, it is essential to look at the application's software build to detect errors and defects.
- Static code analysis should be done early in the development lifecycle and also continuously used throughout the life of the application.

## Stage 2: Protection during pre-production

### Interactive Application Security Testing (IAST)

- Interactive Application Security Testing combines the strengths of SAST and DAST and performs a behavioral assessment.
- It leverages information from inside the running application, including runtime requests, data / control flow to find vulnerabilities accurately.

## Stage 3: Protection at production environment

### Dynamic Application Security Testing (DAST)

- Dynamic application security testing (DAST) helps identify security vulnerability in an application in its running state.
- It mimics real-world hacking techniques and attacks and provides comprehensive dynamic analysis of complex web applications and services.

## Stage 4: Protection on-the-go

### Runtime Application Self-Protection (RASP)

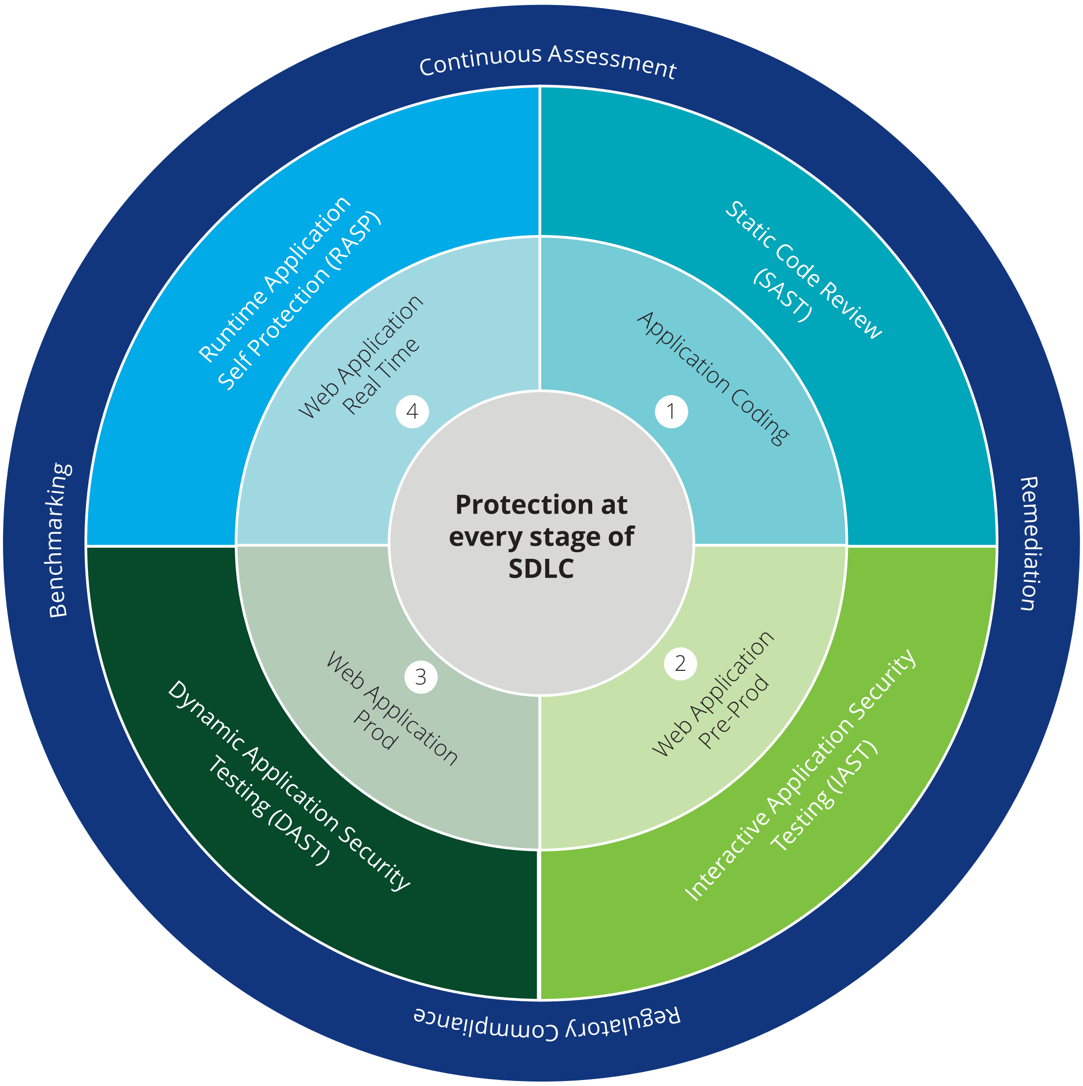
- RASP enables applications to protect themselves against attack in run-time
- It overcomes the shortcomings of legacy protection systems such as Web Application Firewalls (WAF), Intrusion Protection, and Detection Systems (IPS/IDS).

# Application Security – Lifecycle Approach

With applications and software development getting complex by the day, we can no longer look at securing it by utilizing a single solution. We need to look at different phases of lifecycle that an application undergoes to build a solution that covers the entire gamut of application security.

### Advantage of lifecyle approach

- Covers end-to-end phases of an application build that includes design, development, production, and run-time
- Provides an integrated solution thereby creating multiple layers of defence for application protection
- Helps in performing in-depth analysis of threats and vulnerabilities which are being exploited at an application level
- Enables early identification of vulnerabilities and thereby reduces the attack vector of an application
- Reduces overall cost of securing applications by effectively leveraging protection mechanisms during the entire application development process


Continuous Assessment
Remediation
Regulatory Compliance
Benchmarking
Static Code Review (SAST)
Interactive Application Security Testing (IAST)
Dynamic Application Security Testing (DAST)
Runtime Application Self Protection (RASP)
1 Application Coding
2 Web Application Pre-Prod
3 Web Application Prod
4 Web Application Real Time
Protection at every stage of SDLC

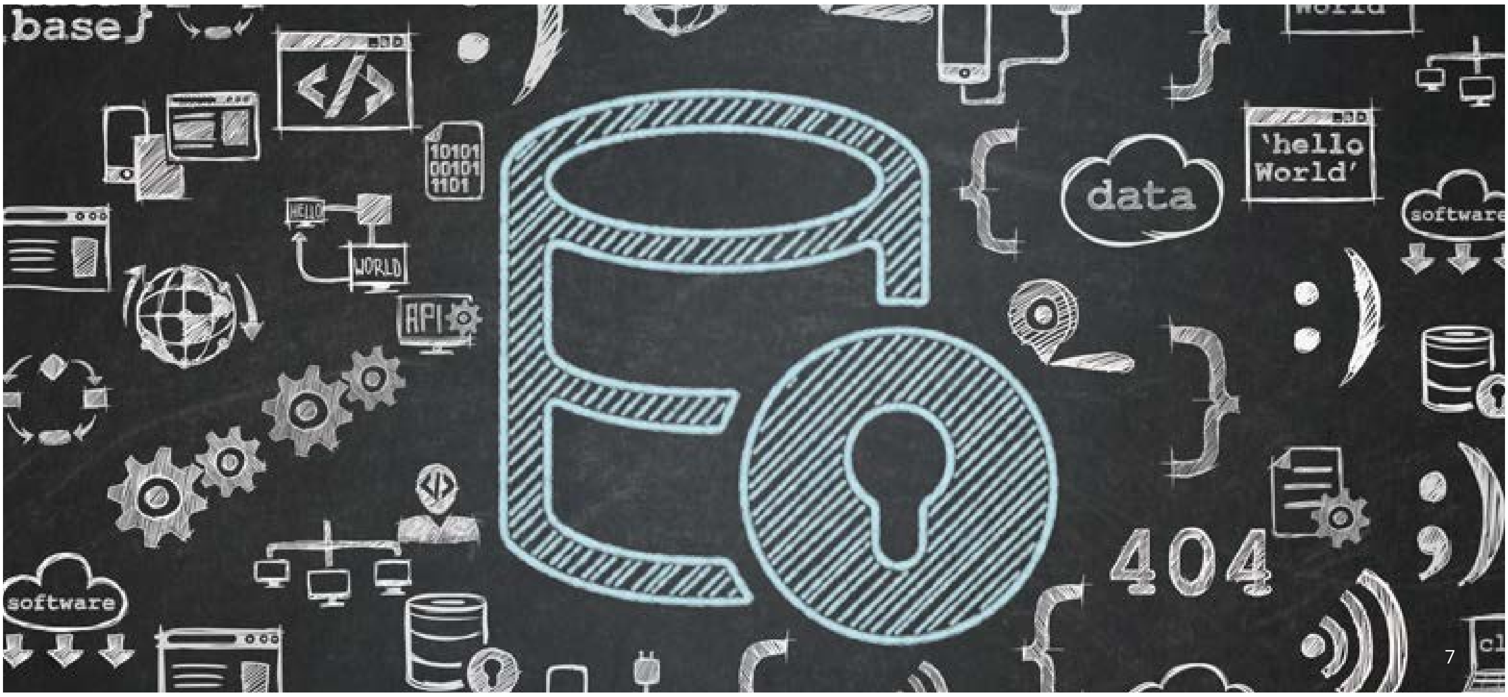
# Securing Applications – At Every Stage

Security should be embedded in every phase of application development to provide protection in its true sense. To accomplish this, we need to understand the complete lifecycle of application development and incorporate security best practices that connects with its individual stages.

### Multi-faceted Approach

Any application development starts by gathering the requirement and perform analysis followed by design, code, testing, and deployment into production environment and finally provides ongoing maintenance support. To look at this lifecycle holistically, we need to incorporate security at strategic phases that will help identify gaps and vulnerabilities early on and also provide layered protection.

- **Application design and development** is where it all begins to materialize and provide shape to an application. It is important to adopt secure coding practice to build a secure application. Static code review will help achieve the objective of identifying and mitigating the vulnerabilities at code level.
- **Application Testing** phase needs adequate protection to the application. Interactive Application Security Testing (IAST) provides the necessary information that helps the developer to make the security-related modifications while the application is being built.
- **Application in production** environment is what the world sees. Adding security at this phase is a must as it provides insight to the visibility that the attacker is likely to have.
- **Run-time protection** is the ongoing mechanism to safeguard the application from external attacks. It is imperative as any leakage of sensitive data leads to financial loss and negatively impacts brand value.



# Application Security – A New Horizon

## Protection on-the-go

The protection capabilities of the traditional perimeter devices such as Web Application Firewall (WAF), Intrusion Prevention/Detection Systems (IPS/IDS) can be insufficient, because they lack insight into application logic and configuration. Run-time Application Self Protection (RASP) operates within the application, developing application context and using that to provide accurate attack visibility and blocking without accidentally stopping legitimate request that looks similar to an attack.

## How does RASP work?

- RASP embeds security into the running application where it resides on the server. It then intercepts all calls to the system to ensure they are secure.
- RASP can be applied to Web and non-web applications and doesn't affect the application design.
- Safeguards applications by effectively leveraging protection mechanisms during the entire application development process

## Prevention of attacks

- **Blocks Zero Day attacks** such as Shellshock
- **Major OWASP top 10** vulnerabilities such as SQL Injection, Cross Site Scripting (XSS), Path Traversal
- **Block automated attacks** with bot blocker technology that automatically blocks malicious bots
- **Virtual patching** prevents vulnerabilities from being exploited until they can be permanently remediated

## Key Benefits

- Out-of-the-box protection via preconfigured vulnerability detection rules
- Continuous security monitoring of actual attacks and protection against vulnerabilities
- Real-time analysis of application logic and data flows to see threats invisible to network security
- Accurately distinguish between an actual attack and a legitimate request
- Integrated monitoring capabilities with Deloitte’s Managed Threat and Vulnerability Management Services

# RASP Betters Traditional WAF Protection

## Limitations of Web Application Firewall (WAF)

Web Application Firewall were once touted to be the most intelligent defence layer sitting at the perimeter. It has become irrelevant in the current scenario as WAF has a major drawback – the inablility to understand application behavior. This leads to easy bypass of WAF protection and the attackers are able to exploit the application residing behind the WAF layer with ease. Organizations have understood this serious limitation of WAF and are now beginning to migrate to RASP which offers application intelligence and thereby does a better job.

To help you understand more, here is the comparative study between RASP and WAF Services -

| Criteria | Deloitte's Runtime Application Self Protection (RASP) Service | Web Application Firewall (WAF) Deployments |
|---|---|---|
| **Accuracy** | Detection of malicious input only when passed to library calls where exploitation would occur. Monitors inbound and outbound data and logic flows | Detection is based on naïve pattern matching, without considering whether the input data would be passed to vulnerable code |
| **Time to Value** | No need to know locations of existing vulnerabilities in application code; can act as a virtual patch against a vulnerability | Requires extensive testing and configration to adequately cover the application. It also involves fine tuning |
| **Reliability** | Will not fail open under high load–code is always instrumented, regardless of servers load | Single point of failure; likely to fail open under high load, leaving the web application vulnerable |
| **Platforms** | Any instrumented application | All types of Web applicattion |
| **Visibility** | Provides detailed feedback to developers to show how to remediate code vulnerabilities | Offers no detailed insight into the application |
| **Network Protocols** | Protocol agnostic; handles HTTP, HTTPS, AJAX, SQL and SOAP with equal ease | Must be able to understand the application's netwotk language type |
| **Maintenance** | Automatically understands changes to the application | Can gain application context through training only |

# What does a Managed Security Program bring to the table?

Deloitte leverages its Cyber Intelligence Centre to deliver the above mentioned services to its clients across the globe. The Deloitte Cyber Intelligence Centre (CIC) combines deep cyber intelligence with broad business intelligence to deliver relevant, tailored, and actionable insights to inform business decision-making. The CIC fuses a number of services together to provide our clients with a truly tailored service that enables them to fully understand their cyber risks and adopt proportionate responses in an increasingly digital and interconnected business environment. We do this by providing them with improved visibility of threats and assets, based on highly relevant intelligence that reflects their specific business, market, and industry context.

| Service Offering | Basic | Advance | Premium |
|---|---|---|---|
| Static Code Review (SAST) | ✓ | ✓ | ✓ |
| Interactive Application Security Testing (IAST) | ✓ | ✓ | ✓ |
| Dynamic Application Security Testing (DAST) | ✓ | ✓ | ✓ |
| Run-Time Application Self Protection(RASP) | ✓ | ✓ | ✓ |
| Integration with Incident Management (SIEM) |  | ✓ | ✓ |
| Integration with Vulnerability Management |  | ✓ | ✓ |
| Integration with Threat Intelligence |  |  | ✓ |

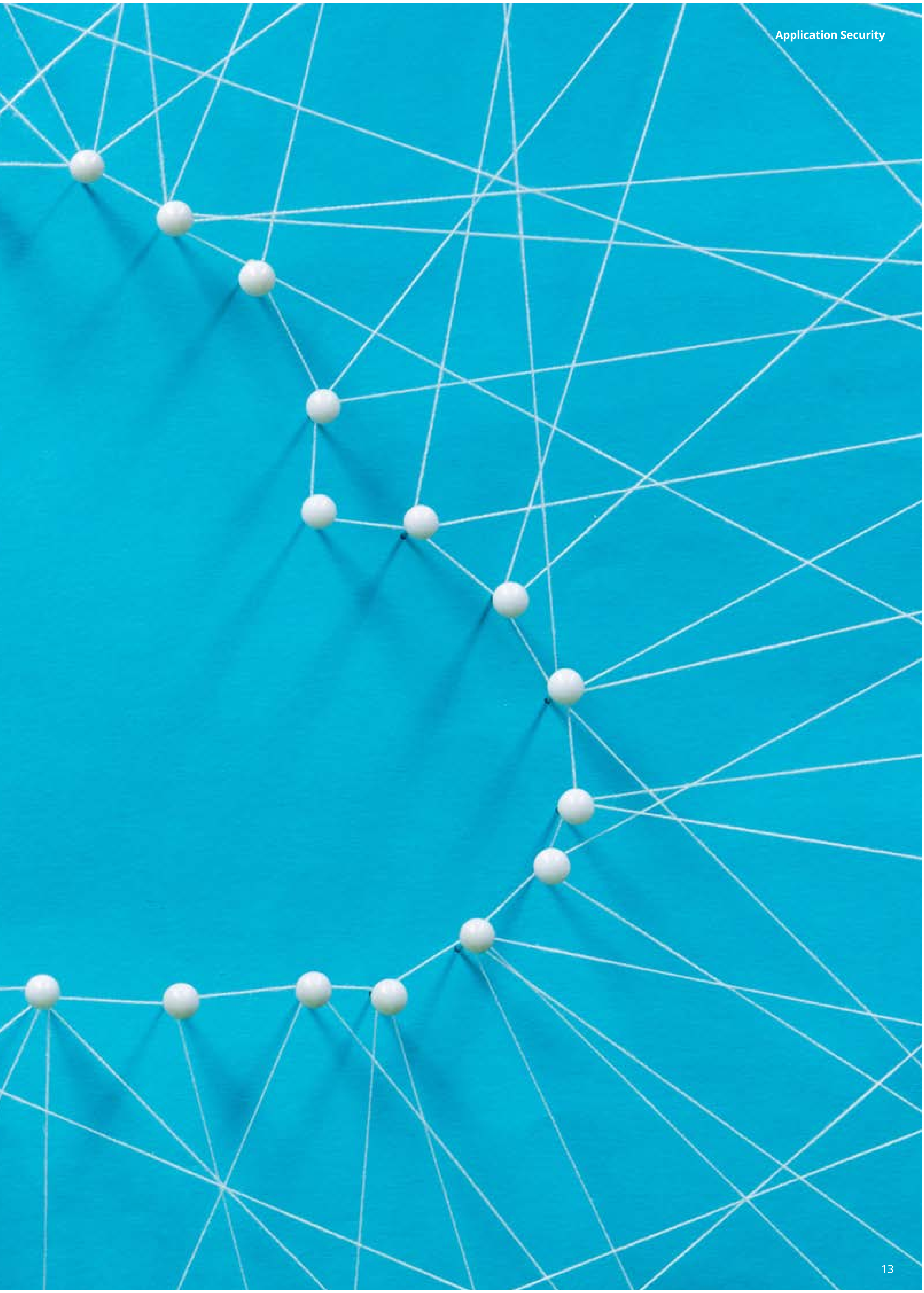
# Managed Security Service Capabilities

- **Robust Capability:** Cyber Intelligence Center (CIC) is the backbone of Managed Application Security Service. It offers state-of-the-art facility that has advanced security tools to run the service effectively.
- **Deep Expertise:** Deloitte has a team of highly skilled application security experts with the merit of holding international certifications. They are equipped with security incident handing capabilities along with niche skillset in managing adverse attacks and breaches.
- **Swift response:** Threat and vulnerabilities don't wait for us to respond. They are likely to have a catastrophic impact if not dealt properly. CIC has the rich blend resources and technology that facilitates quick response coupled with corrective measure to mitigate the incident at the earliest.
- **Dashboard view:** Deloitte provides unique access to its customers to view their application security status via its highly intuitive and customizable dashboard.
- **Service Integration and Advance Analytics:** Threats and vulnerabilities are no longer isolated incidents. They must be considered interlinked entities with reference to Threat Intelligence and SIEM. Deloitte can help you in providing Managed Threat Service and Incident Response with advance analytics capability.

# Related Services

Deloitte provides additional services that are related to Application Security that deliver immense value in managing threats and vulnerabilities effectively.

- **Managed Threat Intelligence Service:** Deloitte provides industry-specific threat information using its commercial feeds which is a vital component of application security risk mitigation. This proactive information can help the organization address its application vulnerabilities before it gets exploited.
- **Managed Vulnerability Service:** Deloitte's Managed Vulnerability Service provides comprehensive solution to its customers in identifying and managing vulnerabilities in their environment. This service, when coupled with Application Security Management, provides complete coverage to all vital infrastructure components of an organization.
- **Managed Threat Services:** Deloitte offers extensive Incident Management capabilities with security analytics capability or managed SIEM solution. When this is integrated with Application Security Service, it provides a structured mechanism to handle security incidents and helps the organization in mitigating it effectively.



# Key Contacts:

**Rohit Mahajan**
President - Risk Advisory
rmahajan@deloitte.com

**Gaurav Shukla**
Partner - Risk Advisory
shuklagaurav@deloitte.com

**Anand Tiwari**
Partner - Risk Advisory
anandtiwari@deloitte.com

**Sandeep Kumar**
Partner - Risk Advisory
kumarsandeep@deloitte.com

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP). This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.