Contents

A Better Way To Manage Vulnerabilities 4
Business Challenge 6
Vulnerability Management as a Service 7
Robust Service Architecture 8
Our Differentiators 9
Vulnerability Management Services Catalog 10
Contacts Us 14
A Better Way To Manage Vulnerabilities

More Business. New Challenges.

The digital revolution is driving business innovation and growth but it’s also exposing us to new and emerging threats. Exciting technological innovations bring fantastic opportunities to:

• Increase integration of business elements in the environment;
• Drive efficiencies and optimum ways of conducting business; and
• Initiate cost effective technological implementations.

Together with opportunity, it also brings the following risks:

• Increase in size and complexity of environment
• More exposure to cyber attacks than ever before
• Data pilferage and security breach leading to loss of sensitive information

Vulnerability Management is a matured outcome of an early day practice of vulnerability assessment. Today’s threat landscape is unimaginably different, with thousands of new vulnerabilities reported annually and the growing complexity of the organization’s environment. Verizon’s Data Breach Incident Report of 2016 shows an increasing trend in the number of vulnerabilities identified and its exploits. The sheer volume of launched attacks demands best-in-class vulnerability management solutions that deliver comprehensive discovery to support the entire vulnerability management lifecycle.
It is imperative for any organization to implement an effective Vulnerability Management to safeguard against attacks and threats in the environment. An effective way of handling such a requirement is to go with a Managed Service methodology, which provides the most comprehensive solution.

**Business Challenge**

- **Do you have critical business applications?**
- **Is the company environment getting complex day by day?**
- **Is it a regulated market bound by compliance requirements?**
- **Do you store or process sensitive data?**
- **Is your organisation routinely targeted and face attempts of attack?**
- **Are there multiple platforms and technologies used?**

**Solution**

Deloitte's Cyber Risk Managed Services for Vulnerability Management is the key to this business challenge. It offers the following advantages:

- Effective management of vulnerabilities associated with critical Infrastructure components.
- Ability to manage increase in scale and complexity of the environment.
- Meet regulatory compliance requirements such as HIPAA, and SOX etc.
- Integration of Vulnerability Management with other security services such as SIEM and Threat Intelligence.
- Deep dive analysis of vulnerabilities along with correlation of threats and events.
Deloitte leverage its Cyber Intelligence Centre (CIC) platform to deliver differentiated vulnerability management services. It integrates advanced security capability with industry insight to provide application and infrastructure security and offers a broad approach to vulnerability management that goes well beyond security testing.

**End to End Support**
Unlike traditional vulnerability management programs, we offer end-to-end support right from the initiation of scan till remediation. This effectively addresses the vulnerabilities through a managed approach.

**False Positive Analysis**
False positives play an important role to remedy the vulnerabilities. A thorough analysis eliminates false positives which in turn greatly reduce the time and energy spent on applying patches.

**Remediation Tracking**
Vulnerability management doesn’t end with performing a scan. An effective program is substantiated by quality of remediation and takes corrective action from reoccurring. We track every vulnerability till it is brought to closure.

**24 x 7 Coverage**
Deloitte’s CIC provides round-the-clock support for our customers. This is critical while handling major vulnerability outbreaks such as POODLE and Shellshock. A swift response is imminent in such a scenario.

**Proof of Concept**
Every major vulnerability will be supported by a Proof of Concept which helps in understanding the business impact of the vulnerabilities and the need to remediate Critical and High vulnerabilities in the environment.
Robust Service Architecture

Deloitte's managed Vulnerability Management service offers a complete vulnerability management life cycle for finding and remediating security weaknesses before they are exploited and helps with improved visibility to security posture. Our Solution is integrated with our Managed Threat Services (MTS) and Threat Intelligence and Analytics (TIA) Services to deliver true vulnerability intelligence to manage threats effectively.

**Vulnerability Management**

### Presentation Layer - Customer Access

<table>
<thead>
<tr>
<th>Asset Inventory</th>
<th>Host specific Vulnerability Data</th>
<th>Vulnerability Tracking status</th>
<th>Remediation Trend Analysis</th>
<th>On demand Scan</th>
<th>Reporting and Dashboard</th>
</tr>
</thead>
</table>

#### Service Integrations

- Threat Intelligence
- Managed Threat Services
- Vulnerability Intelligence
- Cyber Incident Response
- Software Asset Management

**VM Lifecycle**

1. Pre Requisites
2. Scan Execution
3. Analysis of output
4. Remove false Positives
5. Public Customize Report

Data feed to Deloitte Portal
Our Differentiators

Robust Infrastructure
CIC is the backbone of Managed Vulnerability Service. It offers state of art facility that enable smooth functioning of Vulnerability Management service.

Swift Response to incidents
Vulnerabilities are likely to have catastrophic impact if not dealt properly. CIC enables organisation to provide precise and swift response to such incidents.

Structured approach
There are well defined and matured process and standards that govern the overall vulnerability management program.

Integration and correlation
Vulnerabilities are interlinked entities in relation to Threat Intelligence, SIEM, and other security components that provide additional information about the threat in the environment.

Dashboard view
Deloitte provides unique access to its customers to view their Vulnerability Management status. This gives a complete view of the threat landscape.
Deloitte CIC offers Managed Vulnerability Services in below mentioned options

- **Basic Vulnerability Management**
  Standard mode of service offering with complete lifecycle of Vulnerability Management to meet your compliance needs

- **Premium Vulnerability Management**
  Offers integration with SIEM tool and Incident Management which are Customer or Deloitte owned.

- **Advance Vulnerability Management**
  Correlation with SIEM, Threat Intelligence tool, and Asset Management. Provides fully integrated view of threat landscape.
Deloitte leverages its Cyber Intelligence Centre to deliver managed vulnerability management 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 an improved visibility of threats and assets, based on highly relevant intelligence that reflects their specific business, market, and industry context.

Related Services:

• Managed Threat Services
  Integrates all your security logs and event information for advanced correlation and analytics and provides actionable insight. Solution integrates vulnerability management services for true vulnerability intelligence and on-demand actions for effective monitoring.

• Managed Application Security
  Provides full life-cycle application security services ranging from on-demand assessment to real-time application security of client’s web presence.

• Threat Intelligence and Analytics
  Provides ability to leverage world’s leading threat intelligence capabilities, including dark web monitoring, to help you with relevant threat intelligence to secure your business critical assets. Integrated with managed services to provides contextualized threat information for your environment.

• Cyber Attack Simulation
  Improve resiliency of environment through on-demand cyber-attack simulation and validate protection mechanism for enterprise IT systems. Simulation could range from a simple Phishing attempt to a complex DDoS on your environment.

• Software Asset Management
  Integrate the software asset information with Vulnerability Management capabilities to build real time vulnerability intelligence. This significantly improves visibility for potential vulnerabilities in software assets which are not part of scanned assets or are missing from asset information.
Key Contacts:

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

**Shree Parthasarathy**  
Partner - Risk Advisory  
sparthasarathy@deloitte.com  
Delhi

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

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