deep (i)™

Actionable
Intelligence.
Delivered!

deep (i)
the **most advanced solution**
for managed security services

INNOVATIVE
SOLUTIONS

deep (i) suite provides **unparalleled threat intelligence** and incident response through cutting edge **Managed Security Services**

Cybersecurity is one of the biggest economic challenges countries face in the twenty-first century. The Middle East is one of the most advanced regions when it comes to the speed of technology adoption and population growth. Organizations in the Middle East are more prone to cyber threats compared to the rest of the world.

Cyber threats are growing more hostile, security skills are in shortage and imperatives like mobility and cloud computing can pose additional business risks. These factors have led to a noticeable increase in cybersecurity investment to protect critical assets and sensitive information. However, not all investments have yielded the desirable results due to isolated initiatives and lack of centralized security services. As an alternative, establishing a strategic partnership with a competent Managed Security Service Provider (MSSP) has been a well sough after solution for maintaining robust cybersecurity operations and building required capabilities.

Innovative Solutions can help address your complex cyber security challenges, through turnkey solutions, unparalleled threat intelligence and incident response and highly flexible Managed Security Services (MSS), namely deep (i), designed to get better return on investment while meeting the unique demands of your business.

deep (i) suite

- → Managed **Endpoint Protection**
- → Managed **Incident Response**
- → Managed **SOC Monitoring**
- → Managed **Web Security**

Managed **Endpoint Protection**

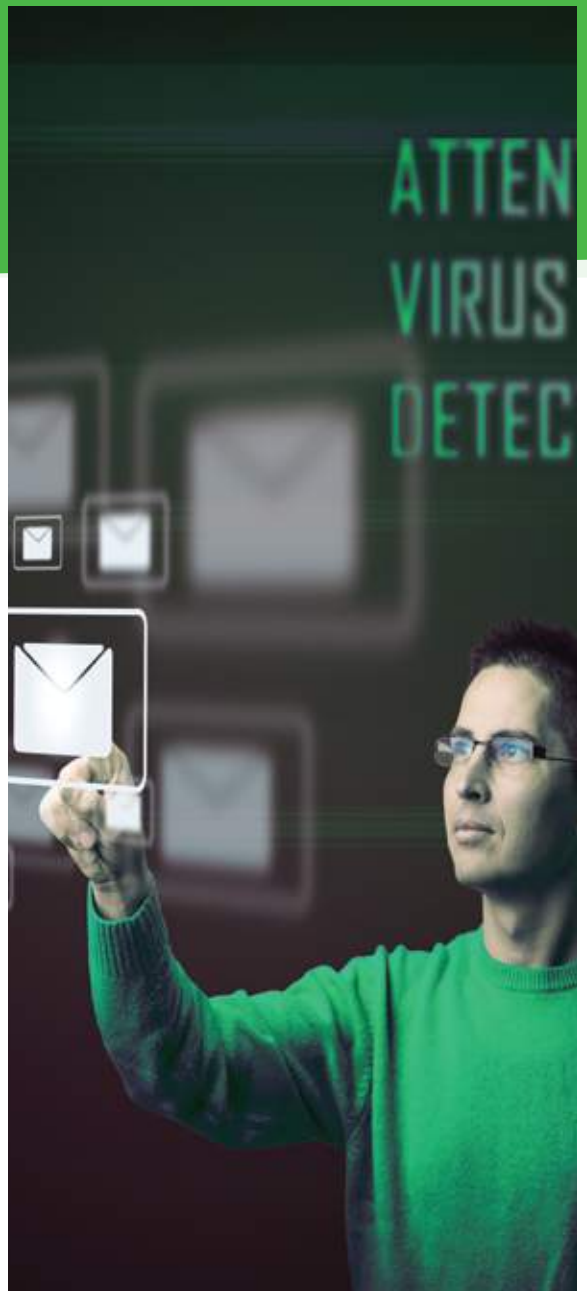
most **scalable**, **flexible** and **durable**
application whitelisting service.

With deep (i) – Endpoint Protection service, organizations attain the ability of enhancing security controls and advancing defenses against malware and targeted attacks by preventing unknown and/or unwanted applications from executing in corporate environments.

The deep (i) – Endpoint Protection service offers extensive list of approved and certified applications with the ability for customization according to the organization's needs. The service includes a unique combination of trust-based and policy driven application whitelisting techniques, real-time threat intelligence, continuously monitors and activity recording to ensure the timely prevention, detection and response to any threats and malicious outbreaks.

deep (i) – Endpoint Protection key benefits:

- **Defend environment** from unwanted and malicious executables.
- **Centralized management** of applications usage and policies.
- **Automated request and approval system** for new applications.
- **Monitor critical activity and enforce configurations** to assess risk and maintain system integrity.



Managed **Incident Response**

Unparalleled visibility and **immediate response** capability.

deep (i) – Incident Response is a complete state-of-the-art managed incident response service with complete visibility using instant Root Cause Analysis (RCA) to provide real time monitoring, prompt response and proactive remediation. deep (i) – IR service involves proactive threat hunting is also bundled with advanced cyber threat intelligence to provide highly accurate and up-to-date insights into known-good, known-bad, and unverified software.

Unlike other IR services, deep (i) – IR goes beyond signature based detections and delivers clear and accurate view of the cybersecurity state of endpoints and servers. In addition, deep (i) – IR involves data acquisition -by constantly recording and maintaining the relationships of every critical action on all machines- and events categorization such as executed binaries, registry modifications, file modifications, file executions, and network connections.

deep (i) – Incident Response key benefits:

- **Unlimited data retention** for investigating long and short term breaches.
- **Limit the scope of cyber-attacks** and **compromise of** the corporate environment through prompt, decisive and rapid incidence response.
- **Preserve forensic evidence** for investigations, law enforcement and prosecution.
- **Critical activities are monitored** for consistent risk assessment and maintaining system integrity.

Managed **SOC Monitoring**

Visionary SOC monitoring and
log management.

deep (i) – SOC Monitoring provides organizations with real-time analysis of security posture on an ongoing basis where information systems are continuously monitored, assessed and defended.

deep (i) – SOC Monitoring offers the capability of detecting organizational policy violations and takes in hand customized use-cases for security events according to business and operational requirements. The service offers powerful real-time data correlation of events to accurately flag threats that violate internal rules within the environment.

deep (i) – SOC Monitoring's systematic integration with multiple threat exchange sources makes this service optimal for addressing cybersecurity challenges as it keeps the solution up-to-date with the latest known and unknown threats.

deep (i) – SOC Monitoring key benefits:

- Complete visibility and management of security logs generated by network and other devices.
- In-depth logs analysis and correlation.
- 24×7 monitoring of activities taking place in the environment.
- Periodic vulnerability scanning of corporate devices.

Managed **Web Security**

A **modern solution** for Web application continuous assurance.

deep (i) – Web Application Security is an in-house developed tool that provides continuous assurance for web applications by employing early detection of weaknesses prior to exploitation. deep (i) – WAS combines state-of-the-art vulnerability management tools and experienced cybersecurity consultants to generate zero false-positive reports that are validated and tested (penetration testing) by qualified experts at regular intervals for flawless results.

In a conventional environment, an organization will have to purchase a vulnerability management tool for scanning web applications which will only produce an automated report. Obtaining useful information from these report is often time consuming as they usually contain numerous false-positive information which requires a great deal of sanitization and cross-checking. deep (i) Web Application Security will enable organizations to concentrates efforts and investments on remediation activities whereas the experts tackle the creation of actionable intelligence.

deep (i) – Web Security key benefits:

- Continuous and consistent assurance of Web application security.
- Comprehensive strategy and workflow for vulnerability management.
- Validated reports by a qualified penetration testing team.
- Flexible packages tailored to meet SAMA compliance requirements.

deep i™

Actionable
Intelligence.
Delivered!

INNOVATIVE SOLUTIONS

Your
Business.
Secured!

Head Office

P. O. Box 69328, Al-Uruba Road
Al-Wurud, Podium Building, 2nd Floor
Riyadh 11547, Saudi Arabia

+966 11 2931501

info@is.com.sa

Dubai, UAE

P. O. Box 414067, Office No. 4202 E
42nd Floor, Aspin commercial Tower
Sheikh Zayed Road, Dubai, UAE

+971 4 221 7197

dubai@is.com.sa

Branches

Jeddah | Al Khobar | Abu Dhabi | Dubai

@Innovative-Solutions

@is_Arabia

@innovative-solutions-sa

www.is.com.sa