INNOVATIVE
SOLUTIONS

Whitepaper:

THE RISE OF CYBER ATTACKS AND THEIR COUNTERMEASURES

Table of Contents

Executive **Summary**

Spectrum of digital enhancements and innovation in the interconnected world of information technology is expanding at a very high. The concept of world to be a global village has become reality with **49.6%** active internet users in the world. The number of IoT sensors will grow to 50 billion by 2020, according to Cisco, and Intel estimates that we'll have 200 billion Internet-connected things by 2030. However, this rapid success is under a constant cyber threat from the malicious actors exploiting vulnerabilities in the system.

According to Panda Labs, in Q3 2016 alone, **18 million new malware** samples were captured. More than 4000 ransomware attacks have occurred since the beginning of 2016. These cyber threats are constantly evolving, forcing companies to become more aware of the security threats and implementing security controls to combat these threats. The rising tide of cybercrime has pushed cybersecurity spending on products and services to more than $80 billion in 2016, according to Gartner. A single breach can cause havoc to your business including crippling your operations, financial and reputation loss of your organization.

In this situation, with latest technologies available, **IS offers Managed Security Services (MSS)** including but not limited to endpoint protection, 247/ monitoring of your entire network using SIEM solutions and prompt incident response in case of any breach. Our services are designed for an end to end protection of an organization from any kind of threat.

Introduction

Saudi Arabia’s digital transformation has proven its success beyond doubt. According to MCIT, “The number of Internet users in the Kingdom continues to rise rapidly, reaching about 24 million at the end Q12017-, with a population penetration of 74.88%”.

Over 500 government services are being provided over the mobile and online. Similarly according to Internet World Stats, internet penetration in the Middle East is 57.4% slightly above the World average of 48.9%. With these advancements and digitization, adversaries have in parallel hiked up their efforts to destabilize the region’s IT advancements with cyber-attacks.

Where Middle East is set to mark its existence as a leader in E-Services and Internet of things (IOT) the risks and challenges to achieve that goal have surfaced in terms of lack of awareness of information security and cyber-attacks. PwC Middle East's Global State of Information Security survey reveals that, businesses in the Middle East suffered greater losses than any other area around the world by falling victim to the cyber incidents. According to the survey report "around 18% of respondents in the region have experienced more than 5,000 attacks, compared to a global average of only 9% ranking the Middle East higher than any other region".

The attacks vary between different ranges from those that hold data for ransom (such as Crypto Locker), hold a company for ransom (stealing data and threatening to release it), delete data or damage systems, add malicious code to a source code repository, or modify critical business data in the hope that it does not get discovered.

Recent wave of attacks like Shamoon 2 and Wannacry in Middle East region are live examples of looming threat over all organizations.

In current circumstances organizations are moving away from reactive approach of installing security devices and reacting after breach. To a greater extent organizations are adopting reactive approach with the assistance of in house SOCs and MSS providers.

According to Gartner's recent Magic Quadrant for Security Incident & Event Management (August 2016), "the SIEM market grew from **$1.67 billion** in 2014 to $1.73 billion in 2015". The major reason for organizations to invest in SIEM solutions is security second only to compliance. Organizations often want to employ SIEM to improve capabilities for external and internal threat discovery and incident management.

Challenges & Risks

The Middle East is adopting technologies at a very fast pace and e-services trend is on the rise. This growth has caught the attention of malicious actors who are very keen to take advantage of niche market. Cyberattacks on the organizations from Middle East is becoming a new norm in the emerging market of digitized businesses and government/semi government e-services initiatives.

UAE's federal authority NESA states Cyber-security as one of the biggest economic and national security challenges countries face in the twenty-first century. In 2015, Saudi Arabia alone recorded over 160,000 offensive cyber actions a day, making it the most targeted country in the Middle East. Predictably, most of the targets were the Kingdom's oil and gas, banking, and telecommunications sectors.

Businesses in the Middle East are more wide-open to threats and cyber threats, compared to the rest of the world (85% of respondents compared to a global average of 79%). As it is evident from the graph, the variance is particularly prominent at the top end: 18% of respondents in the region experienced more than 5,000 attacks, which is higher than any other region, and compares to a global average of only 9%.

The attacks vary between different ranges from those that hold data for ransom (such as Crypto Locker), hold a company for ransom (stealing data and threatening to release it), delete data or damage systems, add malicious code to a source code repository, or modify critical business data in the hope that it does not get discovered.

Protiviti in their IT Security survey report says that "One in three companies do not have written information security policy". Cyber threat Defense Report (2015) clearly states that "Only 20% of IT security professionals are confident their organizations have made adequate investments in educating users on how to avoid phishing attacks."

Lack of security awareness is one more challenge that organizations face. Cyber Threat Security report declares social engineering as the biggest security threat to their organizations. Inside abuse and advanced persistent threats (APT) follow closely as top level threats.

Furthermore, now attackers retain access to the compromised network for a long time to steal the information and disrupt the network on their own choosing of time. Companies are mostly unware of any presence of malicious actors until it's too late. The average time that attackers stay hidden within a network before exposure is over 200 days, reports Microsoft Advanced Threat Analytics.

Information security skills shortage in a pressing issue being faced by organizations in fighting against cyber threats. In a survey by Global Information Security Workforce it was found that in the Middle East and Africa alone, 67 percent of respondents admitted that they felt their departments consisted of too few information security workers, with 40 percent saying that this was down to a lack of qualified personnel.

Majority of the target establishments and those which are working at their best to improve the security posture of their organization to protect themselves from cyber-attacks are still lacking vital security controls and competences to either prevent breaches or to minimize the damages and consequences of an inevitable compromise. However to be secure from future threats it is of paramount importance that organizations adopt a posture of continuous cyber security, risk evaluation and a proactive approach to identify the risks and attacks in the early stages.

Way forward

With booming IT in Middle East, despite the slow pace of security growth, companies are becoming increasingly proactive in protecting themselves against the cyber threats while expanding their IT departments.

To proactively respond to cyber threats, many organizations have resorted to different approaches like periodic risk assessment, enforcing security policies, increasing security awareness, deploying defense systems and most of the important is the solutions to continuously monitor and quick response to emerging threats in real time.

However, to endure attacks, companies must know beforehand about the emerging threats so that if breach occurs, team can swiftly detect, isolate and contain the threat. The best possible way to organize defenses, according to security experts is establishing security operations center (SOC) or utilizing managed security services.

Yet, 42% of companies participating in EY's 19th Global Information Security Survey 201617- reported they did not have a SOC (and only half said they could predict or detect a sophisticated cyberattack).

For continuous monitoring, analyzing and responding back SOC is essential, however resources including time, technology, people and processes makes it very expensive for organizations to build in house SOC. Many companies trying to develop the in house SOC failed miserably due to the lack of expertise in the specific domain. To rescue organizations in this situation there are managed security services providers who can take the pain on organization's behalf and protect them from untoward happening.

Use of managed security services is on the rise according to the Global State of Information Security survey 2017. As it can be seen in the figure below, Authentication and Data Loss Prevention take the lead with 64% and 61% usage ratio respectively. Important to mention is the use of managed security services for real time monitoring and analysis at 55% and Threat intelligence at 48% which is equivalent to our-sourced SOC.

Both of these services are on the continuous rise and companies are adopting this security model very rapidly to save cost and increase security posture of their organizations. This lessens their burden of running a parallel department for the cyber security with 24x7 monitoring shifts, dedicated resources with unique skill set and responding back to any incidents in real time.

Managed Security Services Providers (MSSP) have unique offering of threat intelligence which puts them way ahead than any in house SOC deployment.

MSSPs are well integrated with the threat intelligences around the world which keeps their client protected from the latest emerging threats. Threat intelligence helps organizations to be aware of latest threat spectrum and can take remediation measures before the attack expands into their network or even reach near it.

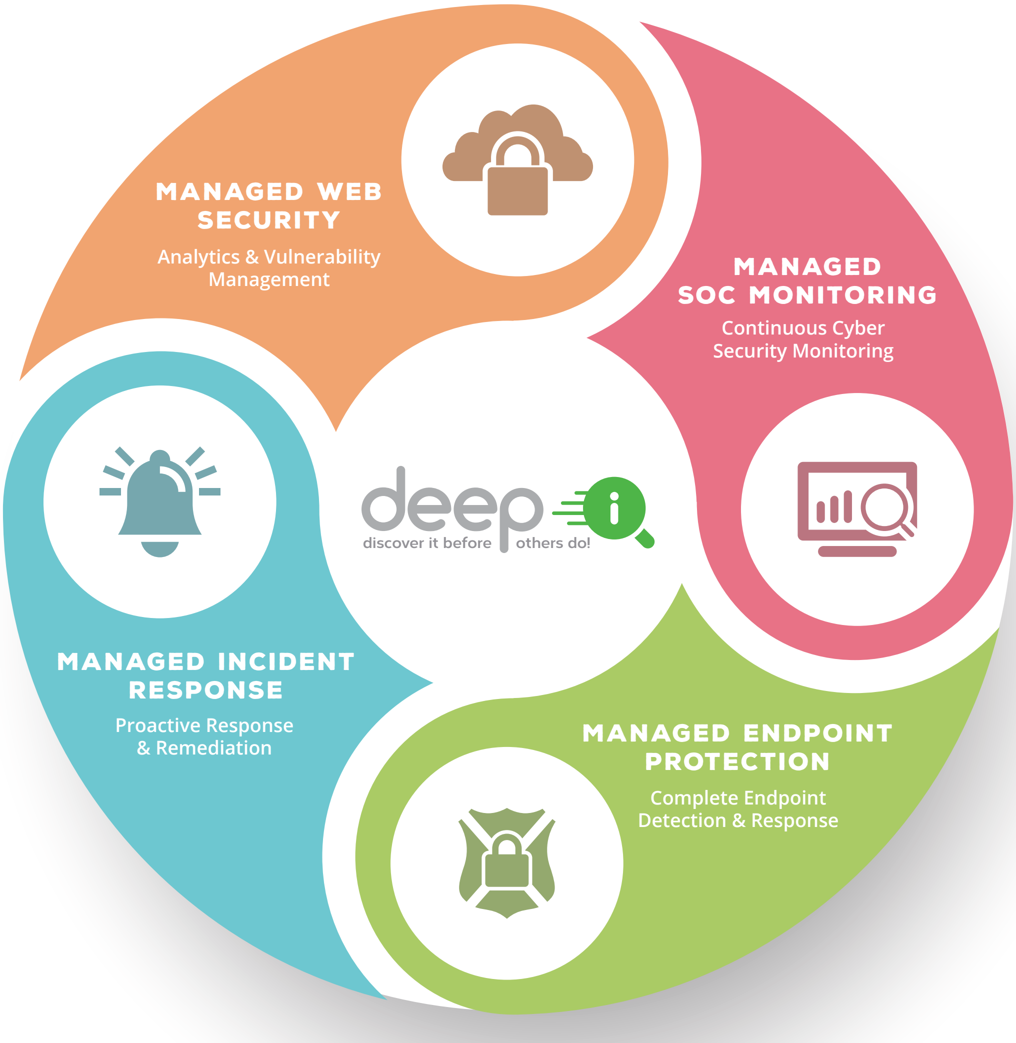
It is highly recommended to protect the organizations from future attacks by getting in touch with security experts and develop an in house SOC or out-sourcing the security of your organizations to MSSP. Due to the expensive SOC, organizations usually prefer to get themselves synced with MSSPs to help them with the security of the assets.

How **innovative solutions (IS)** can assist?

Experts at innovative solutions completely understand implementing few security controls and installing security appliances doesn't ensure complete protection of the environment since they don't provide the complete picture of any event. Organizations not aware of the context of the activities within the environment are at a very high risk of the attack, since separate events might not pose any threat to your organization. However, when correlated it may prove to be an active attack on your premises.

IS' department **MSSP Offers** its unique offerings to keep threats at bay and protecting your organization 24x7. These services come under deep I suite and are mentioned below:

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


MANAGED WEB SECURITY
Analytics & Vulnerability Management
MANAGED SOC MONITORING
Continuous Cyber Security Monitoring
deep discover it before others do!
MANAGED INCIDENT RESPONSE
Proactive Response & Remediation
MANAGED ENDPOINT PROTECTION
Complete Endpoint Detection & Response

Managed **SOC Monitoring**

IS' Managed Monitoring Service offers real-time analysis of security events. The Managed Monitoring Service solution is integrated with all relevant devices and systems of your environment and is configured according to the information security policy of the organization.

The services include but are not limited to log management and their correlation to make sense about the events happening across the environment. Instead we offer **Vulnerability Management**, **Auto Asset Discovery**, **File Integrity and Behavioral Monitoring.** The solution conveniently reports all the vulnerabilities and suggests their fixes to patch the systems protecting them from attackers from exploitation. Furthermore, the valuable files are protected and alerts are generated as soon as there is any change in the files which provides the ability to instantly flag and respond to any alert.

INNOVATIVE
SOLUTIONS

Head Office

P. O. Box 69328, Riyadh 11547,
Saudi Arabia

+ 966 11 2931501

info@is.com.sa

www.is.com.sa

Branches

Dubai | Jeddah | Al Khobar

@Innovative-Solutions

@is_Arabia

@innovative-solutions-sa