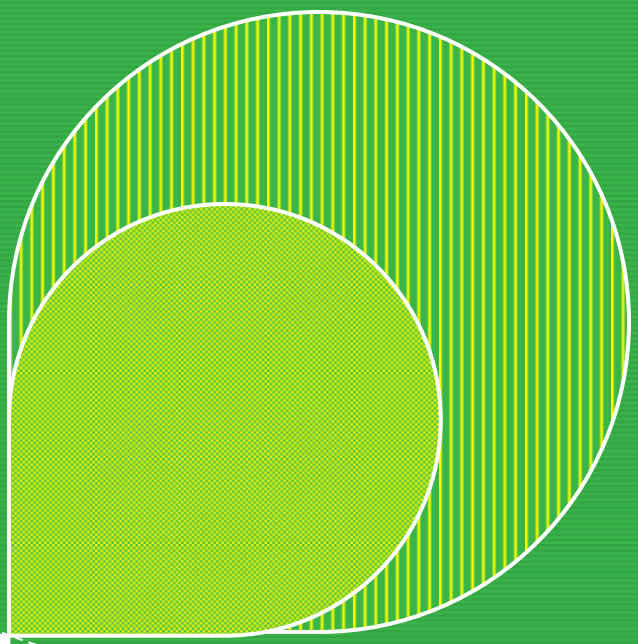
BATTLING IT OUT: APPLICATION AND MOBILE SECURITY

Key Threats and Attacks through APTs on Application and Mobile Environment

By Manoj Rai and Abdul Rehaman

Happiest Minds, Security Services Practice

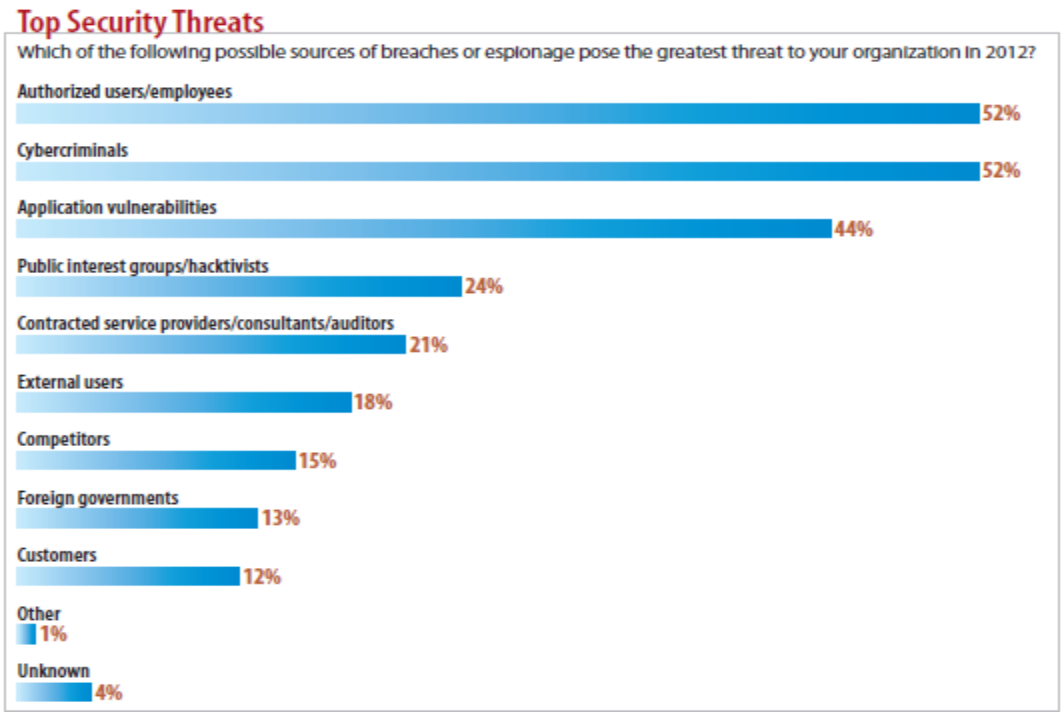


Introduction

Symantec source code hacked, LinkedIn password breached, Yahoo password breached - every week news of such major breaches capture the headlines. Dozens of less newsworthy acts of data theft occur on a regular basis and today, we are quite used to seeing new ways in which data security can be breached. However, the consequences still remain significant such as damage to reputation, steep fines and costs associated with fraud and other compensatory expenses.

Today's corporate world is part of the battleground fighting against potential threats and attacks. Though the threat landscape is evolving rapidly, security has usually always caught up to gain the upper hand. This paper throws light on sophisticated types of attacks that exist today and measures that exist to counter them. As per a report in InformationWeek, top threats can be classified as:

(Fig 1 Reference: InformationWeek)



Based on these key facts, multiple threat groups, depending on their threat levels and exploitable strengths, could be grouped as follows:

a) Advanced Persistent Threats (APTs)
b) Web Application (Web 2.0) Threats
c) Mobile Threats (application, web based and network)

Advanced Persistent Threats (APT)

APT is a buzz word in the corporate world but the hype has made it difficult to discern exactly what it is and extent to which it can be a threat to organizations. APT stands for Advanced Persistent Threat and it can be described as follows -

Advanced – Perpetrators of the threat utilize the full spectrum of computer intrusion technologies and techniques. It uses a combination of various methods of attack and tools in order to reach its target.

Persistent –Attacks with a defined objective that is followed through with constant monitoring and interaction. In this, attackers prioritize a specific task, rather than seek immediate financial gain.

Threat –These attacks are planned and synchronized. These attacks adopt a low-key approach in order to avoid being detected and usually steer clear of technical sophistication which can leave behind clues. In most cases, attackers only need to get the employee of a company to open a piece of malware which is based on zero-day vulnerability. This grants them access to not only to the employee's PC, but also through it, potentially to the entire corporate network. These attacks increased concerns regarding the type of information sought by the APT. For example, a spear phishing e-mail, that is sent from a fraud email account of an executive within an organization to seek unauthorized access to company data. Another example is that of an attacker who gained access to networked critical assets and network topology by gaining access to the passwords of administrator accounts. A third example unrelated to corporates but involved siphoning data from emails and attachments related to terrorism.

APT Lifecycle Process:

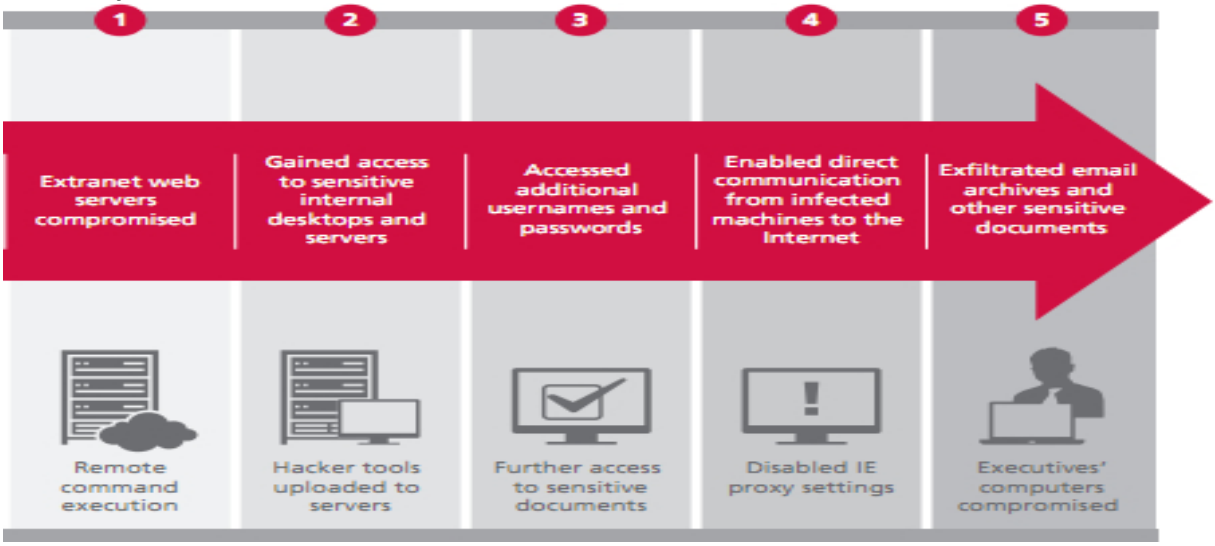


Fig 2: APT Lifecycle Process

The Impact:

APTs establish and maintain a session in its target environment and these sessions remains active throughout. This is helpful because when additional data is sought from the target environment, the

APTs reach for its existing assets in order to locate and steal data. They do not need to re-establish presence.

Web Application Threats:

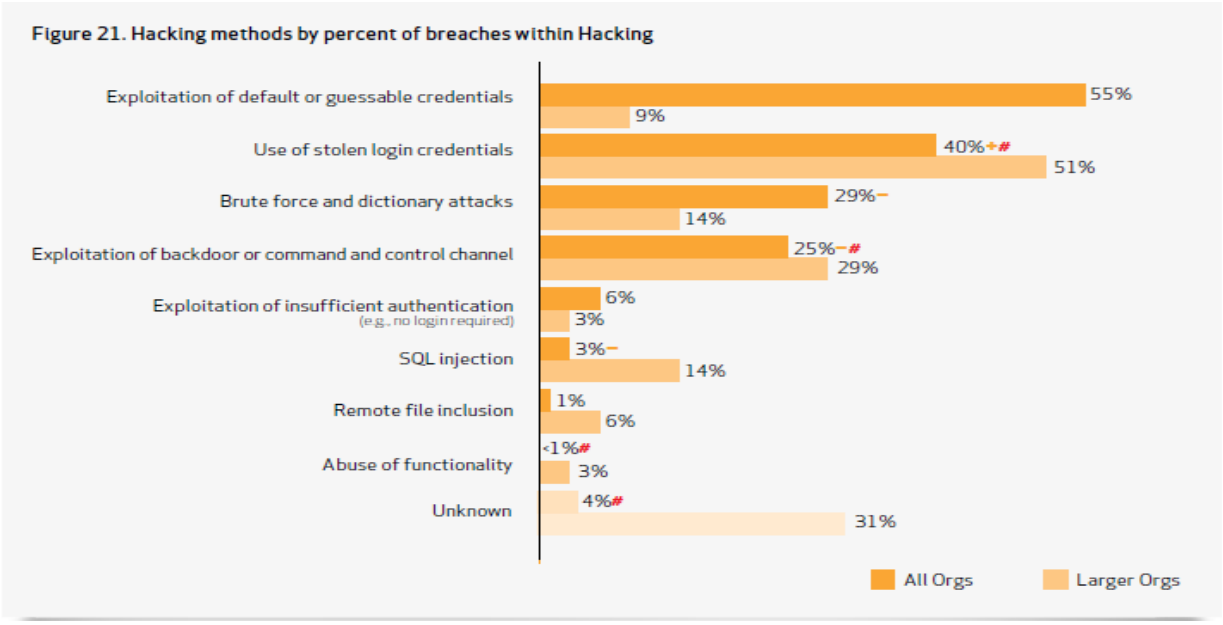
Web applications are the means of communication in today's internet world, where information sharing is no longer a one-way exchange. . Examples include web-based communities, web applications, social-networking sites, video-sharing sites, wikis, and blogs.While all this interactivity is exciting and motivating, there is an enterprise threat behind every web application: losses in productivity, potential data leaks, and increased inherent security risks. A few top web vulnerabilities are listed below:

- SQL Injection
- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF)
- Improper Session Management
- Improper Error Handling and Authentication Vulnerabilities
- DDoS attacks

The Impact:

Web applications can come under threat in many ways from attackers, including SQL injections, DDoS, etc. and newer methods are constantly on the rise. For organizations, a breach in web application data security can cost them dearly leading to financial, effort and reputation related losses. The recent brutal attacks on Twitter, LinkedIn and Microsoft India websites have shaken the enterprise world. The Verizon data breach report-2012 shows the most common web breaching methods.

(Fig 3 Image ref-Verizon data breach report-2012)



Mobile Threats (Application, Web based and Network):

Mobile phones have become ubiquitous in today's lifestyle and the exponential growth in the use of mobile devices has also lead to a corresponding growth in security risks.

Threat assessment: Mobile phones, tablets etc. function on operating systems and those with wireless connectivity are targets for a cyber-attack.

Mobile Application-Based Threats

Recent leading surveys have revealed that top online mobile phone activities include social networking (60%), reading the news (44%) and online messaging (42%). Closely behind these activities are mobile banking and payments (34%), location-based tasks, including navigation (25%); and online shopping (24%).

Regardless of mobile platforms (Android, IOS or Windows), downloading applications on mobile instruments throw up a host of security issues, including software specifically designed to be malicious as well as software that can be used for malicious purposes.

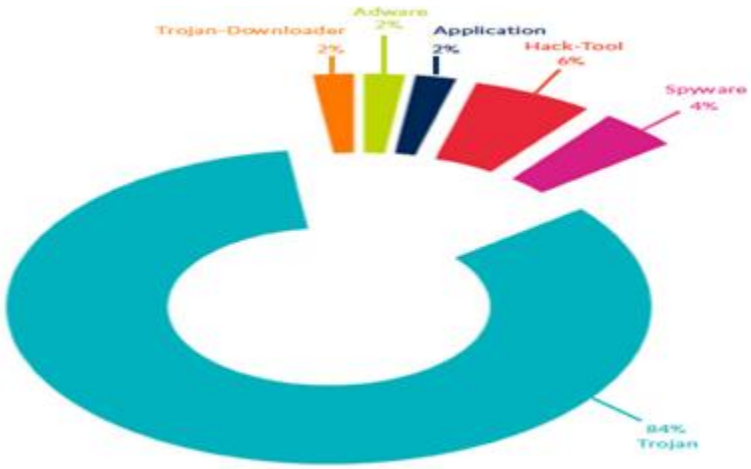
Malware is software that is specifically designed to engage in malicious behavior on a device. Malware can perform actions without a user's knowledge, like charging the user's phone bill, loss of files, sending unsolicited links to the user's email contact list etc.

Spyware, on the other hand, is designed specifically to collect or use data without a user's knowledge or approval. Spyware can capture data such as phone call history, text messages, authentication credentials, internet usage habits, and other personal information.

Privacy Threats can gather information that is more sensitive or critical than data obtained by Spyware like location, contact lists, personal information etc. and is caused by applications that are not necessarily malicious.

Vulnerabilities of software applications are often exploited to enable an attacker engage in such undesirable behavior as gaining access to sensitive information, perform questionable actions, prevent or inhibit a service from functioning correctly and automatically download more apps without it being requested.

(Fig 4 Image ref- F-Secure report-2012)



Mobile Web-based Threats

Mobile devices these days are continuously connected to the internet and are therefore susceptible to browser-based attacks and phishing.

Phishing - Often email, text messages, Facebook, and Twitter are used to send links to phishing sites.

Drive-By Downloads- This involves the automatic download of an application when a user visits a web page

Browser exploits - An unsuspecting user can trigger a browser exploit (Flash player, PDF reader, or image viewer) just by visiting a web page that can install malware or perform other actions on a device.

Mobile Network Threats

Mobile devices typically support cellular networks as well as local wireless networks. There are a number of threats that can affect these networks:

Network exploits target software flaws in the mobile operating system as well as other software networks like for Bluetooth, Wi-Fi, SMS, MMS etc. Network exploits typically do not require user intervention, making them particularly vulnerable to automatically propagate malware.

Wi-Fi Sniffing targets Wi-Fi network flaws by compromising data being sent across a local wireless network. Many applications and web pages do not use proper security measures, sending unencrypted data that may be easily intercepted.

Roadmap to mitigate risks – An approach towards integrated threat intelligence:

It is clear that the threat landscape is evolving at a rapid pace. It encompasses a complex grid of multiple symptoms and the ability to spot anomalous or erroneous actions over a period of time. Threats often targets specific objectives. There is a clear need to stay updated on threat-related information so as to face the challenges. There is therefore a pressing need for an enterprise security solution that helps in resolving security challenges as well as mapping out a clear picture of the potential risks, and evolving regulations for organisations to assess their options. With timely access to information on developing threats and vulnerabilities, organizations can start to counter the threat by detection, protection and mitigation responses more rapidly.

The following steps could help towards building a secure intelligence framework:

Step 1: Build threat intelligence on an on-going basis

Step 2: Perform malware analysis, application and network forensics

Step 3: Respond to an APT/malware incident

Step 1: Build threat intelligence on an on-going basis

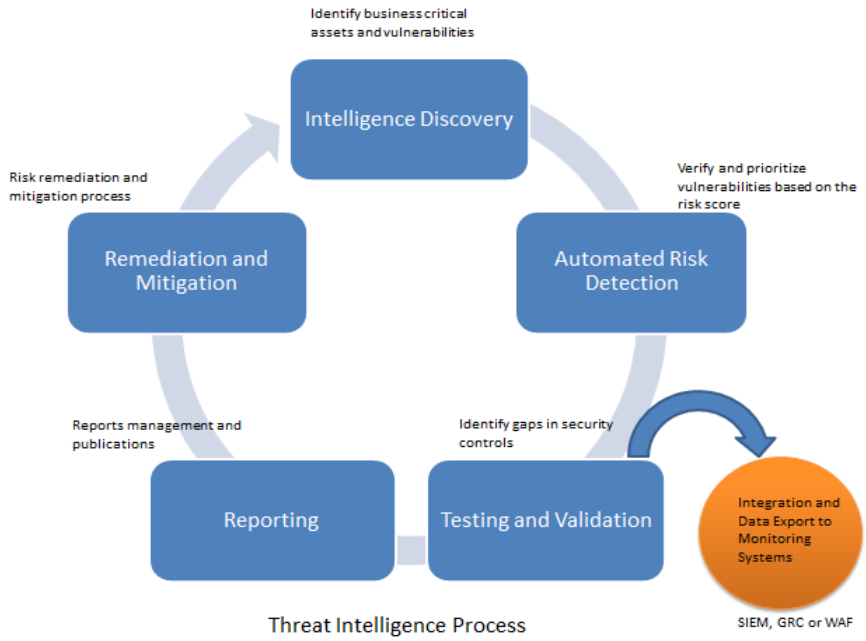


Fig 5: Threat Intelligence

The image in Fig 5 depicts the process of building threat intelligence in steps:

- Identify business critical assets and vulnerabilities
- Verify and prioritize those vulnerabilities based on exploitability and overall risk rating
- Identify gaps in security controls
- Test and prioritize mitigation tasks
- Establish effective controls

Step 2:

Perform malware analysis, application and network forensics

The common recommended solution approaches can be categorized into 3 different tracks. Firstly, perform malware analysis, followed by application security assurance and network analysis through forensics.

Malware Analysis includes:

- Behavioral analysis : understanding the environment in which the malware specimen's operates
- Code analysis: getting into the nuts and bolts of the code that of the malicious program to understand the source of the code
- Memory analysis: going through the past history of the infected system

Application Security Assurance includes:

- Secure SDLC: integrate security in each phase of the application life cycle.
- Network and application Vulnerability Assessment/Penetration Test: perform port scanning, vulnerability assessments and application PT
- Application code review: review the application code following the secure coding checklists and best practices

Network Forensics:

- Storage analysis: examine storage media for evidence
- Source code analysis: check software source code for malicious signatures.
- Network analysis: scrutinize network traffic and logs to identify and locate the suspicious system

Integration of all the above tracks and exporting the data to the monitoring system would help towards building a secure environment.

Step 3:
Respond to an APT/malware incident -on-going monitoring and remediation

In the event of an APT/malware incident, some of the processes enumerated below could enable in depth analysis of packet behaviour and establish controls, both technological and procedural, to prevent recurrence.
Some of the common scenarios that are designed to thwart application attacks and emerging malware are:

- Outbound traffic monitoring – At a primary level, specifically monitor outbound access whenever a suspicious packet is sent across the network. Organizations depend on proxy based features that monitor all outbound access.

- Layer 7 : Web Application Firewalls – The Layer 7 application firewall looks at protecting against some of the web based application attacks like persistent XSS, SQL Injection and request forgery attacks to name a few. These devices proactively track the pattern of the attacks and continuously update the database engine to prevent further attacks. They also have the ability to understand the behavior of users who interact with the applications and can track and prevent them from the norm.

- Using Security Incident and Event Management (SIEM) tool to continuously analyze logs and perform event correlation: Various logs collected from different scan sources would be fed into the monitoring system in order to study the pattern and behavior of malicious packets. The SIEM tool would provide event data aggregation and event correlation. This way, all the activity, irrespective of inbound, outbound or internal data, are analysed at a single location.

The methodology using the SIEM tool helps to greatly expand the scope of threat analysis and provides the ability to work around various weaknesses in the traditional intrusion detection environment.

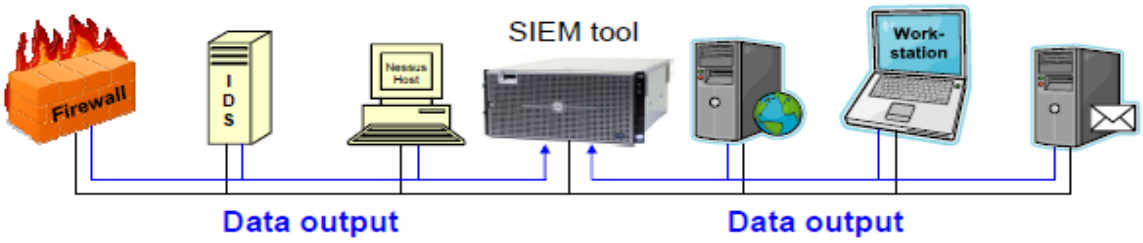


Fig 6: SIEM process

This becomes a very effective tool and offers an in depth defense strategy to the corporate world when some of the IDSs and IPSs fail to capture malicious packets.

A Proposed Solution Framework:

Evolving threats add to a different set of challenges that may require continuous vigil over new threats or discovery of a new vulnerability or disclosure of a new exploit or a new malware threat. With these challenges, there is a need to develop a solution framework that could address the organization's resources in such a way that the relevance of new vulnerabilities, exploits or malware is tested and the organization responds instantly to them.

The solution framework depicted in Fig 7 takes a holistic view of threats from network, application (enterprise and mobile), databases and various APT's.

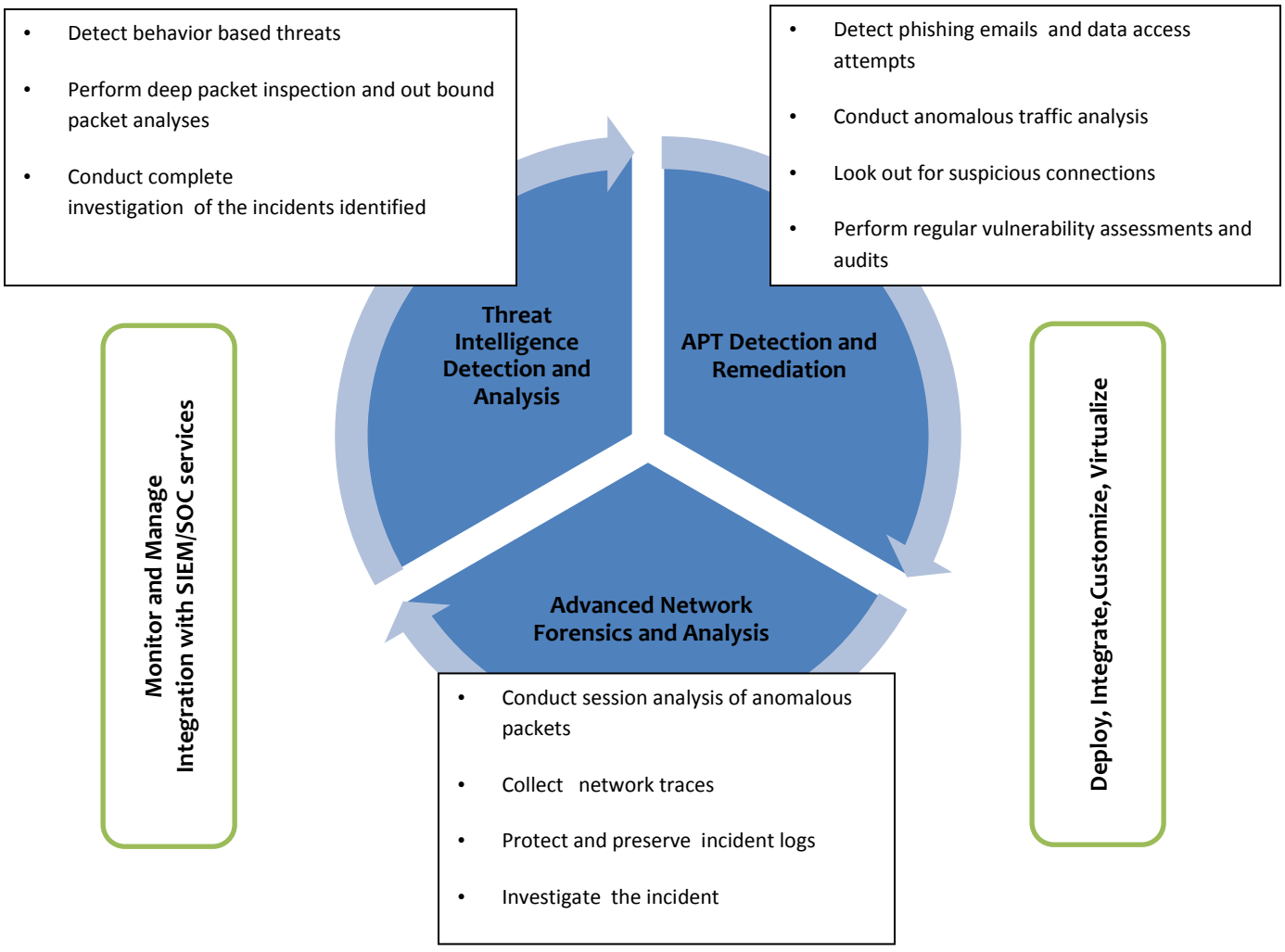


Fig 7: Next gen Threat Solution Framework

Added Benefits:

The solutions approach detailed above allows organizations to protect their data by evaluation the security levels of the network, web application, database and end point system when faced with complex threats. A majority of the solutions discussed above
are available as a hosted service on-premise or over the cloud. This standard structure is fortified by delivery models that will allow a user to choose a security solution that best suits their organization's needs while also reducing the total cost of ownership.

The overall benefits include:

- Next-generation threat management solutions that is simple to use, including centralized reporting and controls
- Detailed analysis on the latest APTs, malwares and exploits
- Increase in overall security across remote and local IT assets. Reduction of cost of ownership with security-as-a-service from the cloud

Conclusion:

With the rapid pace at which attackers develop newer means to access unauthorized data, organizations are in urgent need to find a solution that responds to stringent security requirements. Enterprises require an intelligent and integrated enterprise security solution that allows real-time visibility, proactive vulnerability management and penetration testing across enterprise and mobile applications. A combination of host and network based protection that focuses on the application layer is to be considered as only layer 3 protection is no longer sufficient.

An approach where customizable services are based on multiple solution stacks and based on an amalgamation of knowledge, best practices, compliance regulations and the latest technologies to deliver optimum results is s truly the need of the hour.

About the Author

Manoj Kumar Rai (manoj.rai@happiestminds.com) is the Technical Director and Practice Head of IMSS Application and Mobile Security at Happiest Minds. With over 12 years of experience in Application and Mobile Security specializing in Mobile Enterprises (E-commerce) and Mobile Payments, he is a frequent speaker on various technical subjects like Ethical Hacking and Secure SDLC. He is currently working on next-generation integrated threat management systems connecting enterprise cloud and mobility platforms.	**Abdul Rehaman** (abdul.rehaman@happiestminds.com) is a Technical Consultant in the Happiest Minds IMSS Practice. He has more than seven years of industry experience in Application and Information Security. He has worked with several customers across various domains of information security.

To learn more about the **Happiest Minds Threat Security Offerings,** please write to us at **business@happiestminds.com**

About Happiest Minds Technologies:

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Security, SDN-NFV, RPA, Blockchain, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/ transportation/hospitality.

Headquartered in Bangalore, India; Happiest Minds has operations in USA, UK, The Netherlands, Australia and Middle East.

Business Contact: business@happiestminds.com **Media Contact:** media@happiestminds.com

happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**