GRAMAX
CYBERSEC
A GMR AERO SERVICES INITIATIVE

CASE STUDY

VULNERABILITY & THREAT RESPONSE MANAGEMENT (VTRM)

GRAMAX CYBERSEC
A GMR AERO SERVICES INITIATIVE

Vulnerability & Threat Response Management (VTRM)

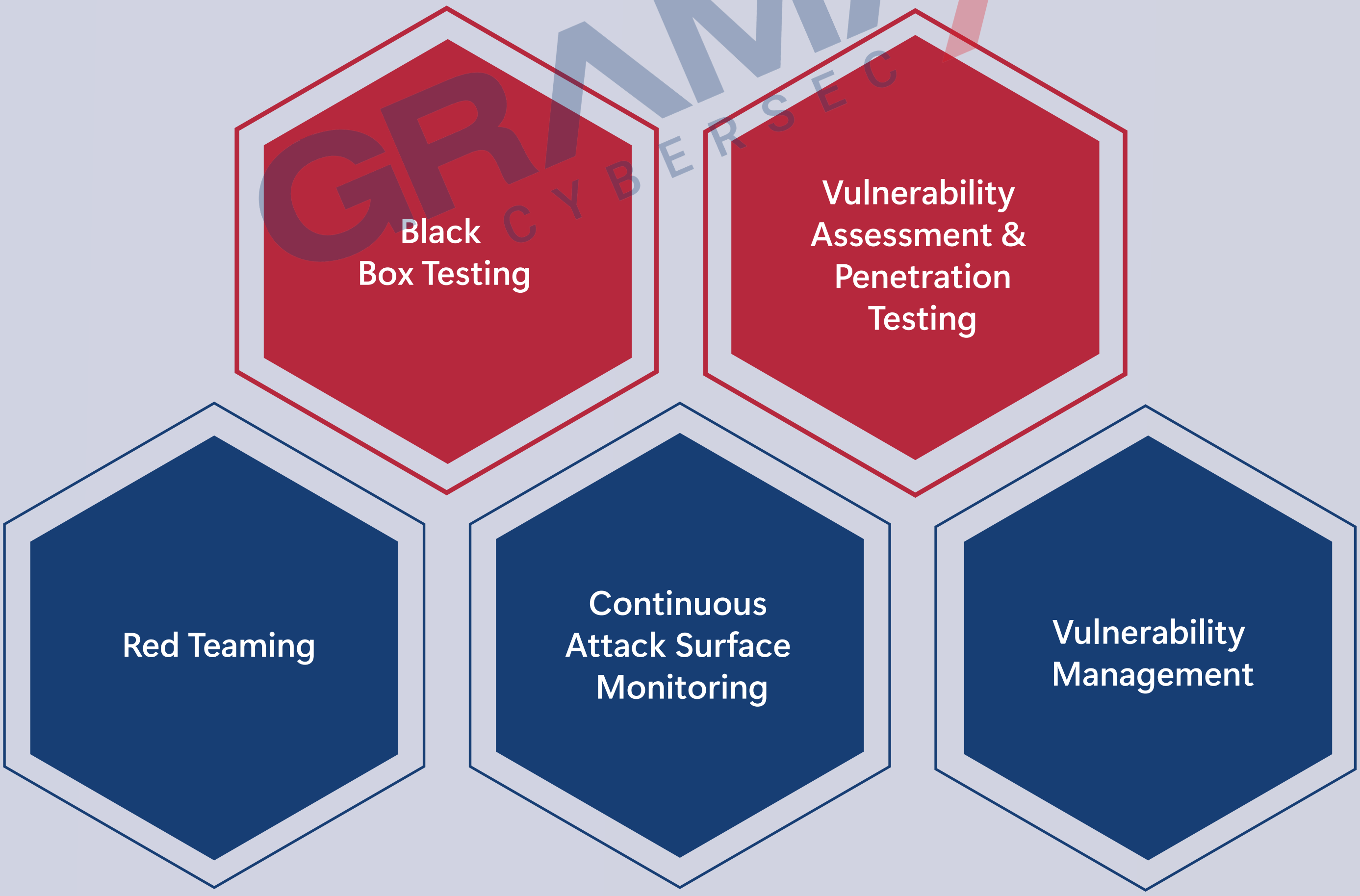
Executive Summary

GRAMAX Cybersec helped one of its clients, who is one of the leading Indian conglomerates, to enhance its overall cybersecurity posture by bringing in proactive vulnerability detection capabilities. The client was looking to perform in-depth security assessment of its critical asset and entire infrastructure to see whether the organization is really secure from internal and external threats. Furthermore, the purpose was also to come up with framework, which would result in improved visibility into the vulnerabilities in the environment and multi-dimensional continuous monitoring ability.

Challenges Faced by the Client

- Unable to manage shadow IPs
- Incomplete visibility of the entire security posture
- Undiscovered misconfiguration and loopholes in various applications
- Unable to go beyond VAPT compliance requirements

The key expectation of our client was that the service provider should be willing to go the extra mile to uncover all possible hidden security flaws within the infrastructure. So, to get a full view of existing vulnerabilities and explore all possible cyberattack scenarios, GRAMAX Cybersec decided to go with Vulnerability Threat Response Management (VTRM) solution, wherein we applied all five main approaches/services, which includes:



Black Box Testing

Vulnerability Assessment & Penetration Testing

Red Teaming

Continuous Attack Surface Monitoring

Vulnerability Management

VTRM framework consisting of 5 defined approaches is bundled as one-service with defined execution cycle/frequency in alignment with the environment&#39;s risk profile.

About Our Solution- Vulnerability & Threat Response Management (VTRM)

VTRM is the process of identifying, evaluating, treating and reporting of security vulnerabilities in systems and software that runs on them. This, implemented alongside with other security tactics, is vital for organizations to prioritize possible threats and minimize their attack surface.

VTRM Scope

This includes web applications, firewalls, switches, routers, databases, application servers, web servers, publicly accessible servers and cloud-based assets (if any). The Inventory of assets is supposed to be managed by the VTRM Team. However, it's the responsibility of stakeholders to share the same on time timely basis.

VTRM Framework & Service Description

Service 1: Black Box Testing

Adversary attack simulation service can be effective for organizations who have deployed adequate security measures andare looking to go further than regular VAPT assessments. This service delivers real-life cyber attacks that appears exactly similar to an APT group targeting an organization. It is not identical to a typical black box VAPT offered in the market by various vendors. This service yields multiple benefits, including:

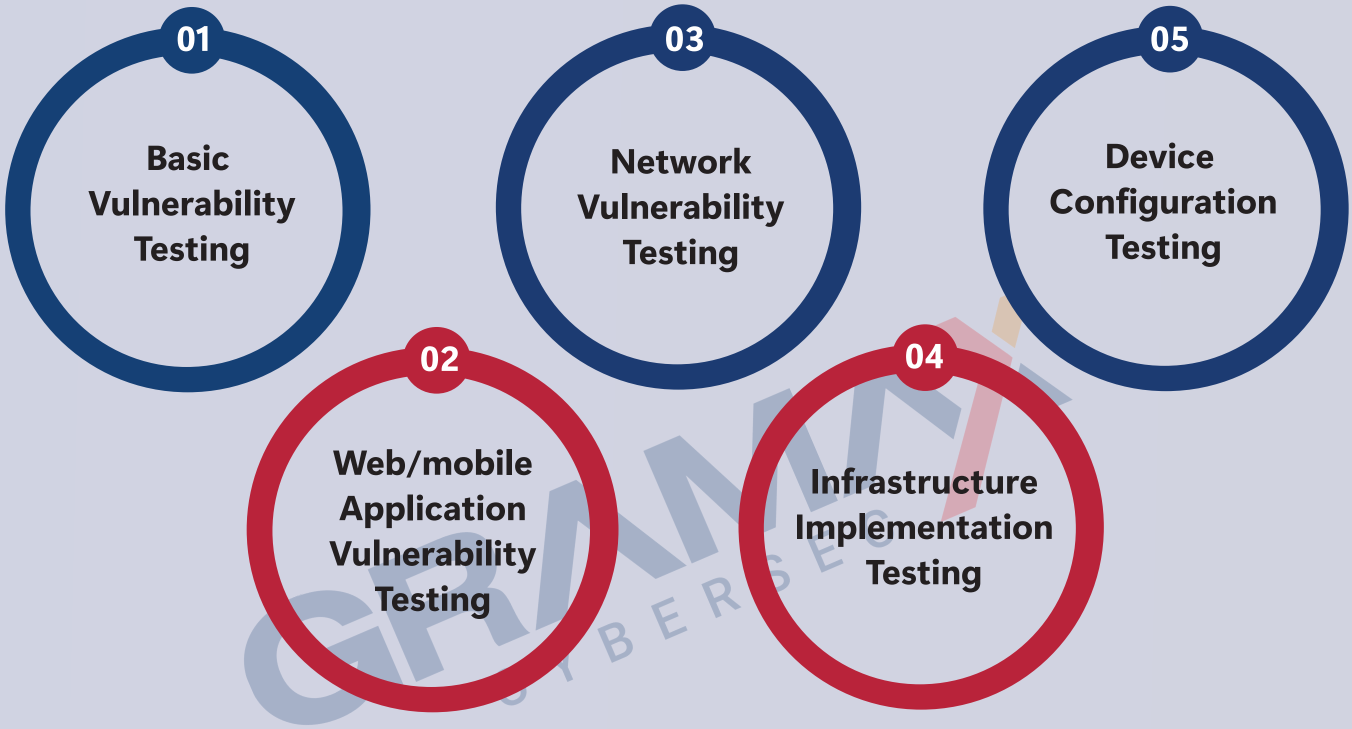
Covers social engineering attacks via email, employee contact, BYOD device compromise.

Advanced AD forest trust & privilege escalation attacks on linux & windows OS.

Customized exploits/scripts written specifically for clients, helping them to understand the current security posture & fill any gap that regular security solutions may not fix.

Service 2: Vulnerability Assessment & Penetration Testing

Vulnerability Assessment and Penetration Testing (VAPT) a e two types of security services that focus on the detection of vulnerabilities in web applications, mobile applications, networks and servers. Both of these services carry different energies and are often integrated together to work better. VAPT protects enterprises from cyberattacks and provides the necessary intelligence to allocate security resources efficiently. As part of the VAPT process, the following components (minimum) are covered:



01 Basic Vulnerability Testing

02 Web/mobile Application Vulnerability Testing

03 Network Vulnerability Testing

04 Infrastructure Implementation Testing

05 Device Configuration Testing

Vulnerability Assessment Phase:

Discovery

Identification of all hosts in the client's network that are visible from the internet.

Exploitation/Analysis

Each service and application discovered a cross-reference to an extensive database to generate a list of potential vulnerabilities.

Reporting

Detailed and easy-to-read reports containing High Risk, Medium Risk & Low Risk will be provided along with remediation recomendations.

For high-risk vulnerabilities identified by team, client may opt to install comprehensive security solution or other services in the areas of Policy & implementations.

Penetration Testing Phase:

- Reconnaissance
- Discovery
- Public Domain Sources
- Port Scanning
- Identification of Services
- Short Listing of Crucial IPs
- Identification of Operating System
- Identification of Vulnerabilities
- Exploitation of Vulnerabilities
- Other Attacks

Service 3: Attack Simulation & Defense Readiness Testing aka Red Teaming

Red team is a defense readiness exercise where different attacks mapped to MITRE ATTACK framework are executed and responses to which are recorded from the defense team. An undetected attack by passing security solutions and defense team constitutes a successful effort from the red team. This exercise is designed to identify vulnerabilities and find detection &amp; Response gaps in a companys security infrastructure. The goal of a red team exercise is not just to identify holes in security, but to train security personnel and management to better defend their infrastructure.

Techiques utiled by the team to conduct red-teaming exercise:

- Social Engineering
- Internal Attacks
- Phishing/Spear Phishing
- DLP Attacks
- Malicious Attachments
- Physical Access

Customer Engagement Steps:

Engagement Kickoff

- Formal designing of documents
- Assigning of SPOC
- Walkthrough of customer’s infrastructure

Mapping of relevant attacks on
ATTACK Framework

Vendor Attacks Preparation

- Formulation of attacks
- Creation of attack campaigns
- Attack infrastructure readiness

Attack Simulation

- Simulation of sttacks
- Correlation with defense teams

Analysis & Reporting

- Analysis of the attacks performed
- Report submission

Service 4: Continuous Attack Surface Monitoring

The aim of this exercise is to continuously monitor the external facing assets of the organization. This activity ensures that possible threats on exposed assets are reported to the organization even before any adversary does. This activity can be performed using automated tools as well as manual methods. Below are the steps that were followed:

- Identification of assets in each LOB via multiple inputs (procurement, usage, health, usability), usually as followed in Iso 27001 asset inventory procedures
- Classification of assets based on functionality under each LOB
- Patch management process review
- Vulnerability & testing status
- Business process review for critical assets

security detection and response process review

Vulnerability management is a cyclical process of identifying IT assets and correlating them with a continually updated vulnerability database to identify threats, misconfigurations, and vulnerabilities. VM Life Cycle:

- **Discover:** Finding and onboarding assets to the scope.
- **Prioritize Assets:** Prioritization between critical and non-critical assets.
- **Assesses:** Run the vulnerability scan on the assets prioritized.
- **Report:** Do a false positive analysis and prepare report.
- **Remediate:** Remediate the vulnerabilities bases on SLA and severity.
- **Verify:** Run a confirmatory/ new cycle scan for verification.