ADVISORY SERVICE AND VMS

TAKTACOM

INTRODUCTION

nowadays by expanding use of information technology and communication and complexity of the role of virtual space in society, we see growth of cyber threats and increasing from day to day to discover vulnerability in technology, equipment, operating systems and…
Due to the daily development of these vulnerabilities, large and small organizations will be influenced by serious cyber threats, so continuous preparation and continuous observation on cyber - security is inevitable. on the one hand, the necessity of huge amount of equipment and technology in organizations, and the other hand discovering vulnerabilities that make 100 vulnerabilities in a month(which 10% of these vulnerabilities could important) if we haven`t knowlegment of vulnerabilities, we couldn`t eliminate the vulnerability in the first step, attackers can easily find a way for penetrate to our network.

According to SecurityWeek research in vulnerability field,68% of attacks come from vulnerabilities at the technology level,which cab be prevented by continuous monitoring and eliminated befor it penetrates.

IMPORTANCE FOR ORGANIZATION

The issue of multiplicity of technology and it`s various versions in organization become important when we don’t know anything about when and where the vulnerability happened and how critical was the vulnerability.

On average , each organization has more than 10 critical vulnerability in the month

Advisory service

Nowadays one of the most important topics in the world of security is the CSIRT. A Computer Security Incident Response Team (CSIRT) is an organization that receives reports of security breaches, conducts analyses of the reports and responds to the senders. A CSIRT may be an established group or an ad hoc assembly.
In large organizations, there are a lot of equipment and technologies and services that involve complementary vulnerabilities.In the same way, we need a proper way to find and solve these vulnerabilities. So Security Advisory is responsible to fill this gap in organizations.We offer neutral advice to create a comprehensive strategy that helps you better prevent, detect and respond to threats and reduce risk.If any new vulnerability is introduced in the world of technology, contacted items will be notified in the least possible time and a proper solution will be provided according to the organization's requirements in order to detect and resolve the vulnerability in the shortest possible time.
Enterprises need sound threat, vulnerability and risk management built on reliable security intelligence to stay ahead in a dynamic risk environment. we draw on their deep experience to develop or review existing vendor risk, risk management, or vulnerability management programs for our clients. It execute technical-based engagements to help organization’s identify associated risks in infrastructure, mobile, applications, or IoT. Building robust vulnerability management and testing programs enable better risk visibility, allowing security leaders to strike a better balance between risk mitigation and business enablement.

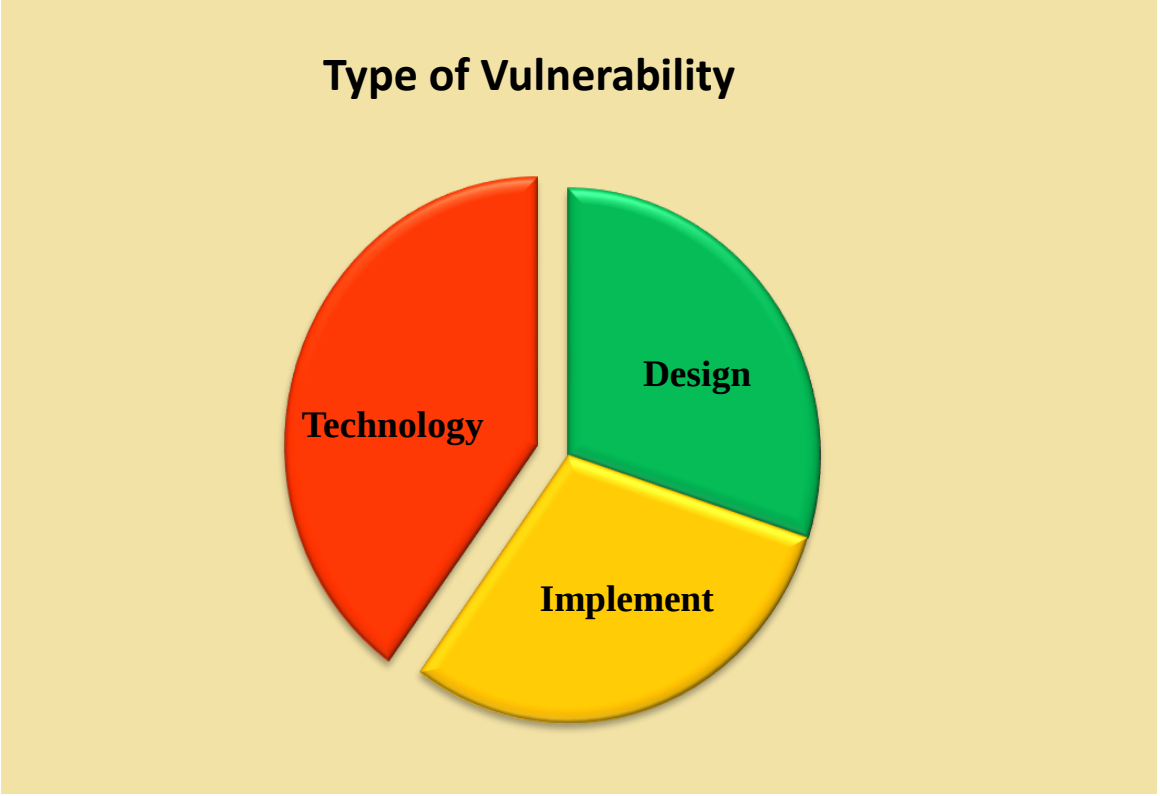
VARIETY OF VULNERABILITY

Vulnerabilities are divided into three categories:

Design: This vulnerability occurs in designing such as mistakes in network architecture, mistakes in software architecture and ...This type of vulnerability is visibility with White Test

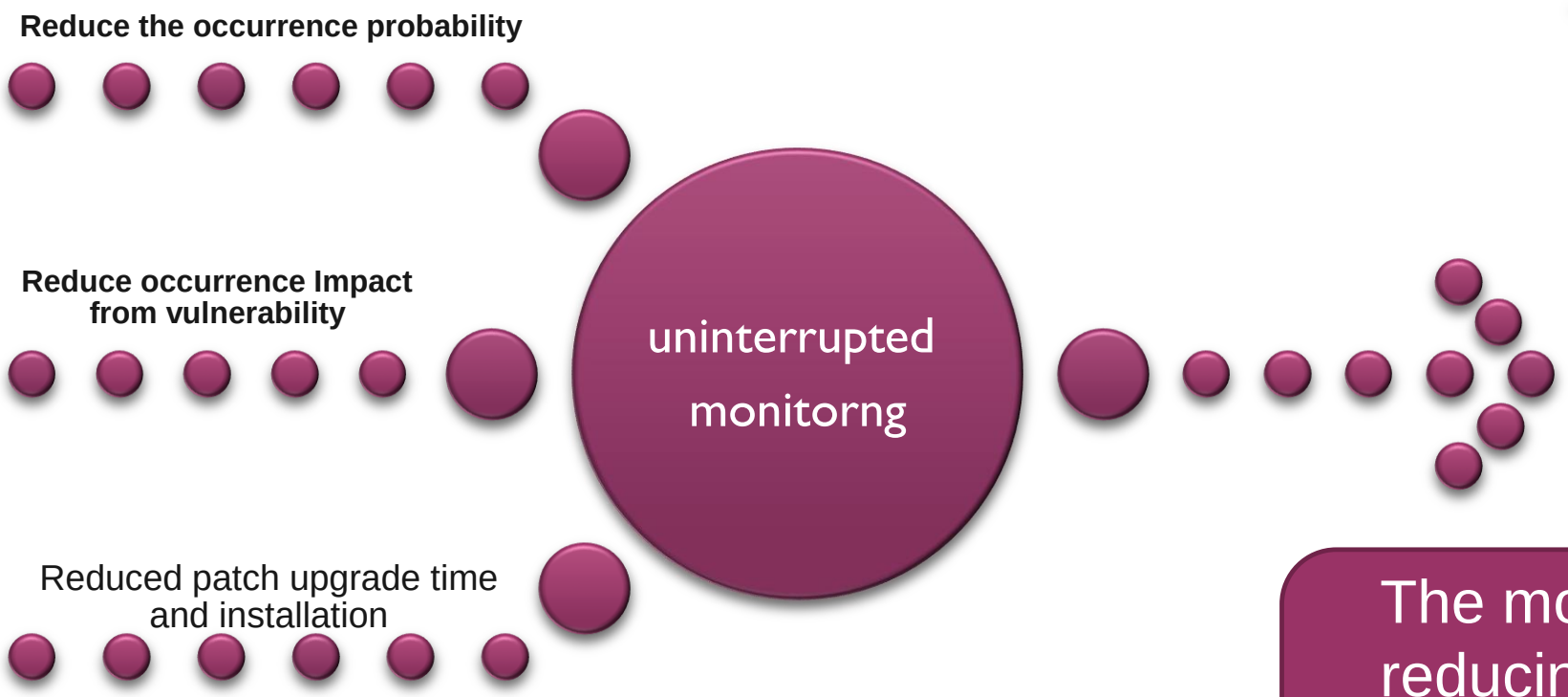
Implement: This kind of vulnerability is usually due to user mistakes that are related to the design and implementation of technologies. For example, application vulnerabilities and programming errors are one of these vulnerabilities. These vulnerabilities are detectable by penetration testing

Technology: This model of vulnerability is the result of the use of various technologies, which is usually very high, The most commonly encountered typical PHP, mysql, and microsoft vulnerabilities are typical examples that we are facing with.These type of vulnerabilities are detectable by Advisory.



Variety of vulnerability in technology

DAILY REQUIREMENT –MONITORING



Prevent from attackers penetrating

Prevent from information leakage

Prevent from create access

The most important factor in reducing the organization's impact is identifying and timely handling of hazards

THREAT SCRUTINY

PWC: 90% of large organizations and 74% of small businesses had security breach , 42 million incident have been detected and 71% haven`t been detected.

Verizon Company : more than 70% of incidents that occur are reported by foreign entiries.
“The problem is not whether we are facing a security breach or not, the issue is how many times does it happened and why these events occur.”

Gartner: we have to go for defense in depth and quick response

MTTD = Mean Time To Detect

MTTR = Mean Time To Response

DEFINITIONS

- **vulnerability(with CVE specific identifier):**

Any weakness in design or implementation and an error that causes an unexpected and unpleasant event and endangers the security of the system.

- **Recommendations:**

For each identified vulnerability, a recommendation is prepared ad submitted by the vendor.

- **solutions:**

Explained solutions in the Recommendation are different to the type of vulnerability and equipment

Provide patches , Work around and Regular updates

https://cve.mitre.org/

COMMON VULNERABILITY SCORING SYSTEM(CVSS)

- Attacker access level
- Attacker access vector
- Access complexity
- Abuse ability
- Impact level of damage in organization
- Solution level

Categories of CVSS v3.0

CVSS Score	9.3
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code

REVISION RECOMMENDATION APPROACH

1. **Manually(** Check all vulnerabilities and recommendations by human resources)
   - mistakes
   - Need for human resources 24 hours
2. **Automatic approach(**Production of tools to observe vulnerabilities and recommendations.)
   - False Positive
   - Lack of intelligence and ability to analyze
   - Different ways to handle vulnerabilities in different organizations
3. **Combinatorial(**Applying appropriate tools along with Expert human resources)
   - Absence Disadvantages that we said

OUR SUGGESTED SOLOUTIONS

❑ Product

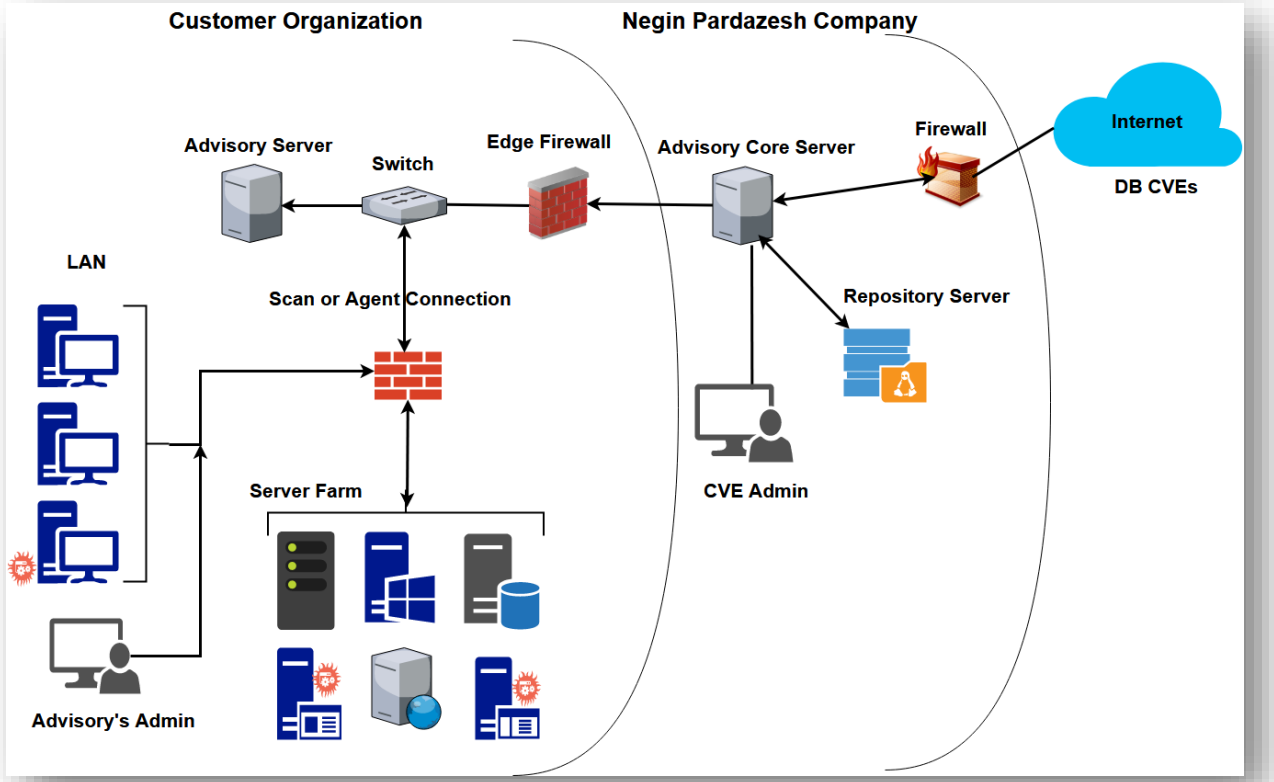
- In this part, an updated and equipped software in the case of vulnerabilities will be used and all critical information will be recorded in this software.

❑ Services

- In this section, an expert team is monitored for all system activities, and the team is continuously monitoring critical services to record and report vulnerabilities.

ARCHITECTURE OF PRODUCT DEPLOYMENT IN THE NETWORK

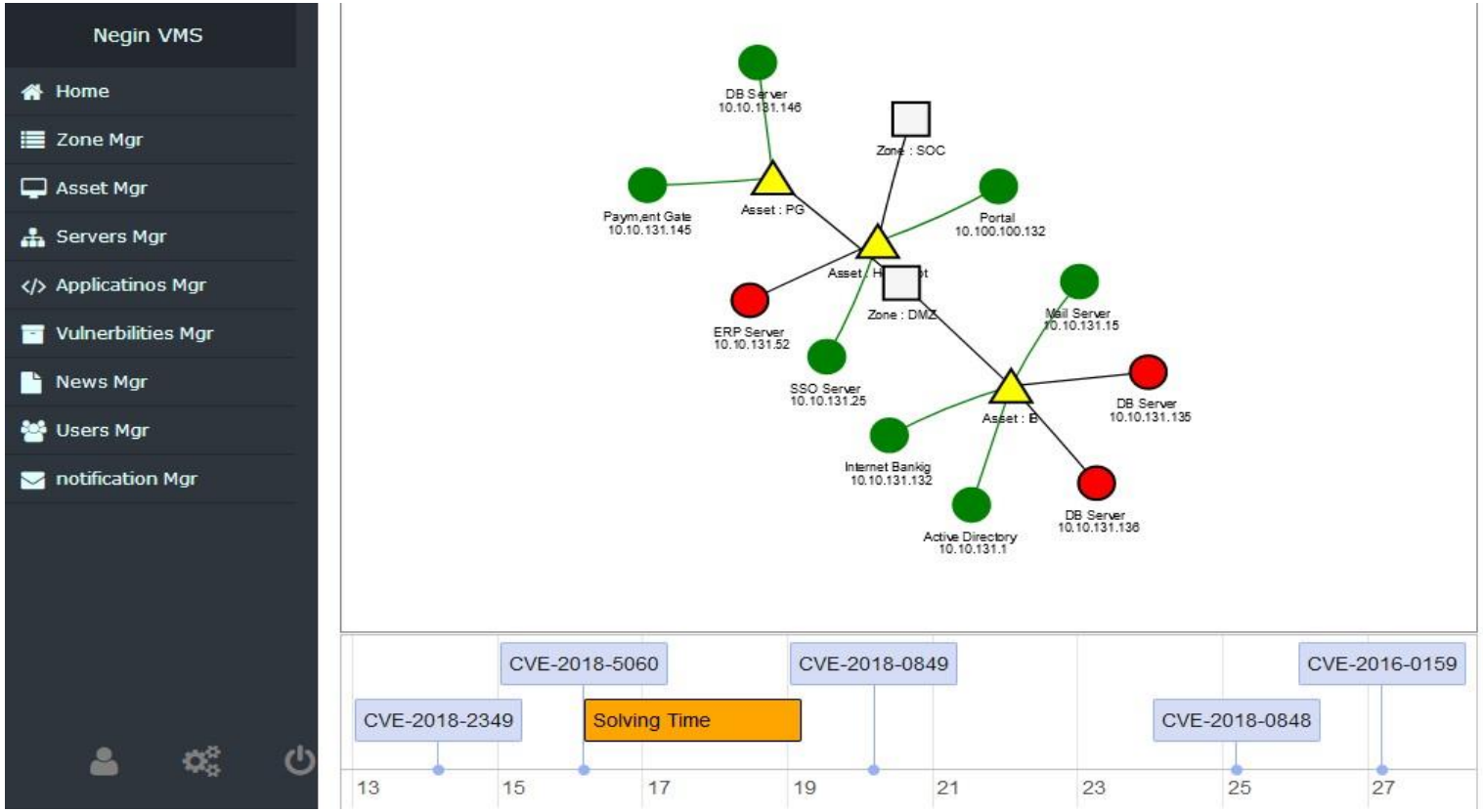
This product has two server, one of them is in customer organization and the other one is in our company. there is One-*way* communication between our server and customer organization`s server , the information will be sent to it and no data will gain from the organization.



PRODUCT FEATURES

- immediate warning of discovered organization`s vulnerabilities
- Show the time of creating and fixing vulnerabilitiesProvide all CVEs related to the organization in real time and monitor themIdentify and categorize vulnerabilities based on the type and classification defined in the organization
- Provide solution to solve identified vulnerabilities
- The possibility of using technologies in three ways : User, Automatic Scan, Agent
- Warning about vulnerabilities with Email and SMS
- Determining the severity of vulnerability and its impact on the organization
- Managing devices by web console
- Ability to communicate with Syslog server to present output to SOC
- Analytical report by the organization based on massive data
- Ability to add asset
- Ability to automatic asset scan
- Provide latest security news

VIEW OF THE PRODUCT



PROVIDED SERVICE WITH PRODUCT

- ✓ Providing a suitable solution to reduce vulnerability risks
- ✓ Monitor and scan system and equipment vulnerabilities
- ✓ Supervision product performance
- ✓ Managing and configuring the product tailored to the organization's requirements
- ✓ Update asset list
- ✓ Notify and edit recommendation
- ✓ Add technologies in the software