

Summary

evision is a leading consulting firm delivering a niche bouquet of high quality information compliance services to renowned enterprises in the Middle East region. Our services include information security and information operations management.

evision information security consulting team has custom built our evision internal methodology based on worldwide standards including ISO 17799, FIPS, CobiT, SOX; bundled with a mixture of quantitative and qualitative security risk assessment techniques. The evision methodology adopts a strategy called "**Defense-in-Depth**"; sometimes referred to as security in depth or multi-layered security. The term is derived from a military term used to describe the layering of security countermeasures to form a cohesive secure environment without a single point of failure. To achieve this, we have developed and continually enhancing our "evision Toolbox" to assist enterprises deploy a full Security Risk Management Model and guarantee maximum security across the information infrastructure.

Our projects address end-to-end information security from the assessment of technology, process, and people; across all layers of the architecture including perimeter networks, internal networks, hosts, applications, and data layers; to regulating effective policies driven by efficient procedures; to deploying security solutions with our customers and their partners.

Objectives

We at evision understand that the overall objective of our client is to ensure that appropriate information security controls are implemented and that computing platforms preserve integrity, confidentiality, and availability of its information and computing resources. Effective implementation of these security controls will aid in the prevention of unauthorized, accidental, or deliberate disruption, disclosure, modification, and use of our clients information technology resources. evision will partner with it's clients' teams to ensure that the following objectives are accurate and achieve our clients overall security requirements.

- To investigate whether or not an attacker could penetrate the system to be evaluated, without the organization providing any more information than would naturally be available to legitimate users.
- To determine the likelihood that an attacker with access to computers connected to the Internet could compromise the specific systems under evaluation.
- To penetrate the security of the system, acquiring capabilities that exceed those of a normal user.
- To provide evidence that verifies the possibility of exploiting the vulnerabilities found, as well as the scope of these vulnerabilities
- To determine the degree of the organization's exposure to external attacks on its information security infrastructure
- To penetrate the internal systems that have security vulnerabilities regarding resulted from configuration mistakes or un-patched systems.

Project Phases

External and internal attacks

Assuming the profile of an external attacker with no more information than a range of IP addresses for the client, eVision will attempt to identify and penetrate as many systems as possible within the time constraints given below.

The tests will include but are not limited to:

- Information gathering tests

- Generic vulnerability tests
- Network characteristics and topology tests
- Miss-configuration tests
- Authentication and access control schemes tests
- Client side attacks
- Web application attacks

Success criteria

- **Positive results:** A test will be considered successful with positive results if an attacker gains the ability to manipulate the components of the company's IS infrastructure or the data it processes in a way that provides any kind of benefit to the attacker OR provokes any kind of loss to the company.
- **Negative results:** A test will be considered successful with negative results if a reasonable number of penetrations attempts have been performed and documented within the predetermined time period OR if an attack procedure has been defined that has high probability of generating positive results but requires more time or resources than those specified for the project.

Deliverables

Throughout the execution of the penetration test eVision will provide the following deliverables:

High-risk findings report

On a daily basis, or according to the needs of the client, eVision will provide a report on those high-risk vulnerabilities detected which represent a direct threat to the company's information infrastructure. The report will be presented and sent to the Customer via encrypted e-mail.

Final report

Upon the completion of the penetration test, eVision will present the final report to the Management describing the following sections:

- **Summary**
This section describes the objectives and scope of the work done as well as the methodology used for each phase of the penetration test performed.
- **General conclusions and recommendations**
This section describes overall conclusions for each penetration test phase performed detailing the critical aspects of the customer's security infrastructure that should be modified or fixed in order to enhance the security of the components within the defined scope.
- **List of Vulnerabilities**
For each of the vulnerabilities found, a vulnerability record will be presented using a standard format.