The Four Disciplines of Security Management

An Information Security Reference Model

SPiRE security 2004

INFORMATION SECURITY

Security 2004

Today's enterprises talk about "security" as an amorphous objective that means different things to different people. The very nature of security makes it difficult to define or classify because when it is working flawlessly, nothing happens - no runaway worms or viruses, no stolen intellectual property, no denial-of-service attacks, no system integrity issues. But security never works flawlessly. So it is up to the profession to define strategic security programs that balance the needs of the business functions we are trying to protect with a control infrastructure that minimizes the risk based on available resources and expectations.

This model introduces the Four Disciplines of Security Management - identity management, vulnerability management, trust management and threat management. It is a functional approach to security that identifies the relationships among the many point products that exist today, the corresponding functions that they assist in accomplishing, and the ultimate mission and objectives in the four functional areas.

Top Trends 2004

2004 has already brought us back to the future with a traditional email virus attack. The top trends for 2004 are:

Identity Management: Identities get vaguer as enterprises (and the RIAA) resort to MAC and IP addresses to identify individuals. Application identities become more apparent in their role of enterprise representative.

Vulnerability Management: Vulnerabilities dominate security activities as patch management takes center stage as the most popular product of 2004. Remediation in general drives the space towards lifecycle management and AVDL provides a model for future ecosystems.

Trust Management: The continuing separation of data from the application drives digital rights management and application integrity solutions. FUD becomes proactive as regulations reappear as key drivers in strategic security management.

Threat Management: The "insider threat" reawakens as IDSes move away from focusing solely on identifying hack attacks and towards monitoring for regulatory and policy compliance along with quality of service.

CORESTREET REAL TIME CREDENTIALS

Mission

To design controls that ensure the confidentiality, integrity, and availability of resources. The focus of trust management is twofold: first, on the computing processes that are being used to perform some business function; and second, on the transactional data as it is being manipulated and transferred throughout the environment.

Control Objectives

1. Allow only authorized users to read information/data in transit and at rest.
2. Allow only authorized users to insert or manipulate information/data in transit and at rest.
3. Prevent the unauthorized deletion of information/data in transit and at rest.
4. Allow only authorized users to run systems and applications.
5. Prevent the denial of service to any system or application.

Trust Management

Products

- **DRM** — **Digital Rights Management** solutions add access control mechanisms to data being presented to the user.
- **DSig** — **Digital Signature** solutions provide integrity and authentication that a transaction is valid.
- **AppInt** — **Application Integrity** solutions validate that a program is running in a trusted state.
- **PKI** — **Public Key Infrastructure** solutions manage certificates used to encrypt and sign information to maintain its confidentiality and integrity.
- **VPN** — **Virtual Private Networks** IPSec and SSL Virtual Private Networks encrypt data-in-motion - the communications between a source and destination.
- **Crypto** — **Encryption** products ensure the confidentiality and integrity of data at rest.

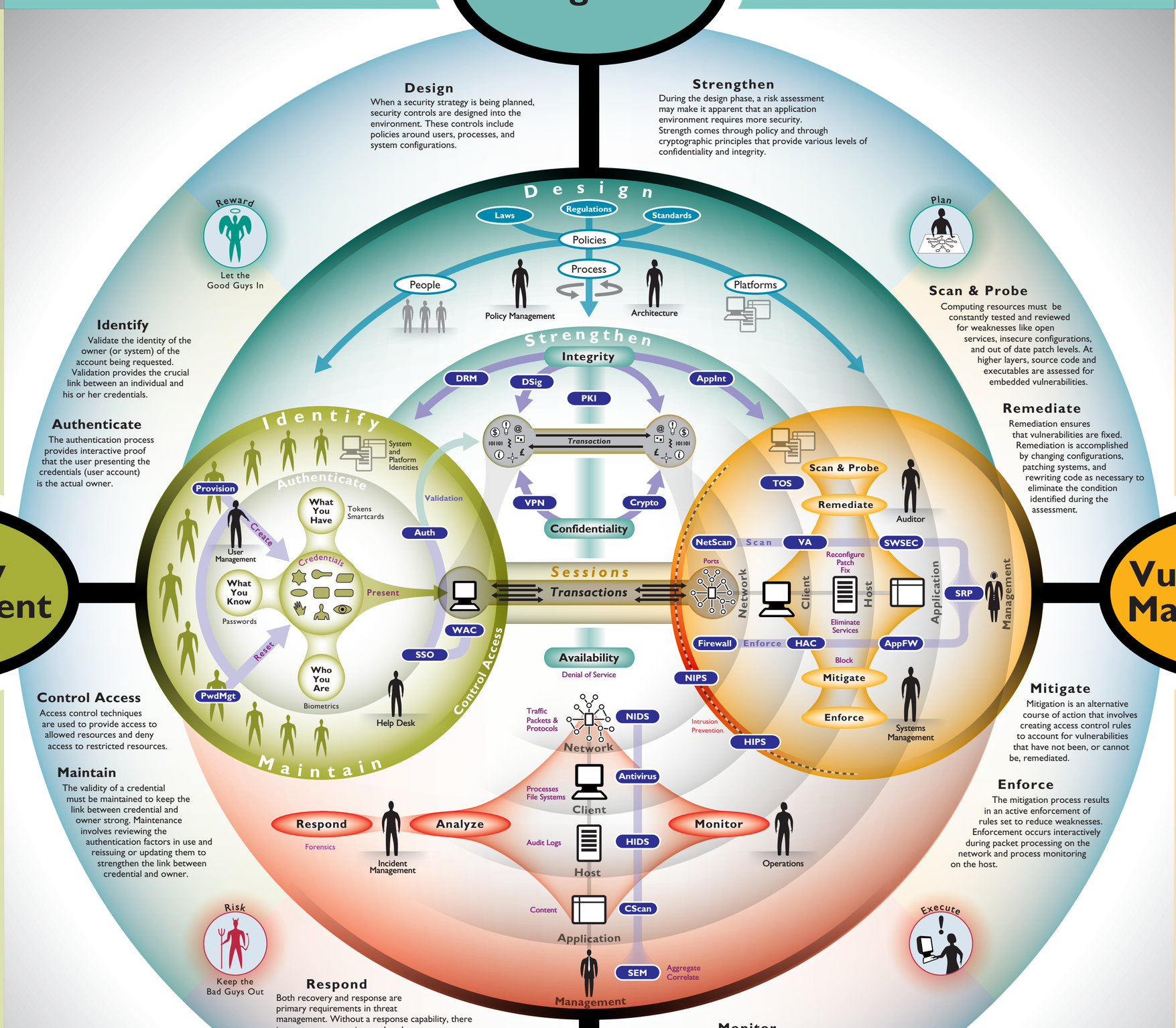
Voltage security

Design

When a security strategy is being planned, security controls are designed into the environment. These controls include policies around users, processes, and system configurations.

Strengthen

During the design phase, a risk assessment may make it apparent that an application environment requires more security. Strength comes through policy and through cryptographic principles that provide various levels of confidentiality and integrity.



Identify

Validate the identity of the owner (or system) of the account being requested. Validation provides the crucial link between an individual and his or her credentials.

Authenticate

The authentication process provides interactive proof that the user presenting the credentials (user account) is the actual owner.

Control Access

Access control techniques are used to provide access to allowed resources and deny access to restricted resources.

Maintain

The validity of a credential must be maintained to keep the link between credential and owner strong. Maintenance involves reviewing the authentication factors in use and reissuing or updating them to strengthen the link between credential and owner.

Respond

Both recovery and response are primary requirements in threat management. Without a response capability, there is no reason to monitor and analyze.

Analyze

Analysis involves looking for attacks directly or identifying good traffic and eliminating the rest. Analysis can include pattern matching, matching complex rules, comparisons to standards and policies, and statistical analysis.

Monitor

When monitoring, we capture and decode packets on the network and system calls and logs on the host. In addition, we review data streams and application processing to identify threats.

Scan & Probe

Computing resources must be constantly tested and reviewed for weaknesses like open services, insecure configurations, and out of date patch levels. At higher layers, source code and executables are assessed for embedded vulnerabilities.

Remediate

Remediation ensures that vulnerabilities are fixed. Remediation is accomplished by changing configurations, patching systems, and rewriting code as necessary to eliminate the condition identified during the assessment.

Mitigate

Mitigation is an alternative course of action that involves creating access control rules to account for vulnerabilities that have not been, or cannot be, remediated.

Enforce

The mitigation process results in an active enforcement of rules set to reduce weaknesses. Enforcement occurs interactively during packet processing on the network and process monitoring on the host.

Identity Management

RSA SECURITY® Confidence Inspired™

Mission

To control the users of a system or any other source of a request (this includes other systems and applications). The intent is to ensure that the activity is legitimate by reducing the possibility that inappropriate people or systems will compromise the systems and gain access to the functions and information they provide.

Control Objectives

1. Allow only authorized users to receive credentials for systems and applications.
2. Limit the number of unknown users on systems.
3. Maintain the integrity of the owner with his/her credentials.
4. Validate the identity of credential owners and control access to systems and applications.
5. Oversee and monitor the use of credentials throughout the computing environment.

Products

- **Provision** — **Provisioning** solutions automate the assignment, management, and deletion of user accounts.
- **PwdMgt** — **Password Management** solutions automate requests for password resets to reduce social engineering risks.
- **Auth** — **Authentication** solutions strengthen the initial credential offerings from users and drive access control.
- **WAC** — **Web Access Control** solutions manage the authorizations that a user has during a web session.
- **SSO** — **Single Sign-On** solutions provide a single interface for users to login to systems and applications.

M-TECH™ Identity Management Solutions

Vulnerability Management

QUALYS SECURITY ON-DEMAND

Mission

To limit exposure for a particular set of resources - users, computing systems and applications, and physical locations. Exposure is reduced by evaluating the security posture of an environment and eliminating, remediating, or mitigating weaknesses.

Control Objectives

1. Eliminate unnecessary services and processes running in the computing environment.
2. Configure systems to reduce the number of known weaknesses that exist and strengthen the functions that remain.
3. Reduce the number of coding errors that are written into software developed in-house.
4. Act as a gatekeeper to system resources by controlling access to them.

Products

- **TOS** — **Trusted Operating Systems** integrate encryption and mandatory access control.
- **NetScan** — **Network Scanners** probe networks and perform various levels of penetration testing.
- **VA** — **Vulnerability Assessment** solutions look for vulnerabilities in systems.
- **SWSEC** — **Software Security** solutions scan source code and applications for common vulnerabilities and coding errors.
- **SRP** — **Security Resource Planning** solutions manage the vulnerability remediation process and provide a link to policies.
- **Firewall** — **Firewalls** filter the flow of network activity on an enterprise perimeter and on client PCs.
- **HAC** — **Host Application Control** solutions control how applications interact with other resources.
- **AppFW** — **Application Firewalls** provide system access control for web, email and other app layers.
- **NIPS** — **Network Intrusion Prevention Solutions** combine the features of intrusion detection and firewalls to add deeper content inspection.
- **HIPS** — **Host Intrusion Prevention** solutions monitor and control file systems, registries, networks, and other resources.

CITADEL SECURITY SOFTWARE

Threat Management

Mission

To identify inappropriate or malicious behavior within a computing environment and reduce its likelihood of compromising systems. Threat management systems monitor, analyze, aggregate, and correlate information from logs and alerting systems to identify activity for review and response.

Control Objectives

1. Monitor network traffic to review protocol usage and manage bandwidth.
2. Monitor packets on networks to identify malformed packets and known attacks.
3. Monitor users and processes on systems to identify inappropriate activities.
4. Respond to activities that are identified as malicious or inappropriate.
5. Gather evidence that inappropriate or malicious activity occurred.

Success means... nothing happens.

Products

- **NIDS** — **Network Intrusion Detection Solutions** monitor network traffic and seek out malicious or inappropriate activity.
- **Antivirus** — **Antivirus** solutions protect systems from being exploited by common viruses and worms.
- **HIDS** — **Host Intrusion Detection Solutions** passively monitor processes and logs to identify signs of inappropriate activity.
- **CScan** — **Content Scanners** evaluate data (web and email) to identify inappropriate information.
- **SEM** — **Security Event Managers** collect and correlate events from the computing environment.

SOURCEfire

PROTEGO NETWORKS

2003 Retrospective

In 2003 the Internet was hit with Slammer and Blaster, signaling new attacks and driving the need for new defenses. Top trends:

Identity Management: Identity fraud picked up in 2003 as phishing techniques were used to "socially engineer" end-users via malicious email and websites. In addition, keystroke loggers were "in," being used to steal information from shared computers in public facilities and universities.

Trust Management: In the face of new regulations, encryption became a popular topic and options have multiplied. Application integrity began its rise in popularity in response to the increasingly common buffer overflow attacks.

Vulnerability Management: Getting a handle on remediation through patch management picked up steam in the latter half of 2003, thanks to Blaster et.al.

Threat Management: If IDS is dead, there are a lot of IDS zombies getting great value from new techniques that add context and correlation through security event managers. Intrusion prevention began building its head of steam.

2003 set the table for the upcoming trends of 2004 - compliance managing and monitoring, stronger authentication, insider protection, and strategic security management.

Value and Loss

Computing environments have become the lifeblood of many companies. Any strategic program to secure these assets requires an understanding of their value to the enterprise. In security, the true value of an asset is calculated by identifying its loss potential. There are five key classes of costs:

1. Intellectual property loss.
2. Liquid asset loss.
3. Legal/Regulatory costs.
4. IT productivity costs.
5. End user productivity costs.

Further, there are five key types of losses:

1. Data being stolen or read (confidentiality).
2. Data being deleted (availability).
3. Data being modified (integrity).
4. Systems being abused (liability).
5. System access denied (productivity).

To measure the value of the computing assets, each discrete unit should be evaluated in a 5x5 grid with these two lists at the vertical and horizontal axes respectively.

SPiRE security

About Spire Security

Spire Security, LLC conducts market research and analysis of information security issues and requirements. Spire's objective is to help define and refine enterprise security strategies by determining the best way to deploy policies, people, process, and platforms in support of an enterprise security management solution.

To schedule a meeting to discuss the Four Disciplines of Security Management or other security issues, contact Pete Lindstrom at:
petelind@spiresecurity.com
or visit our website at: **www.spiresecurity.com**

Poster Design by Idiagram
www.idiagram.com
Idiagram ▪ Knowledge Visualization & Integration

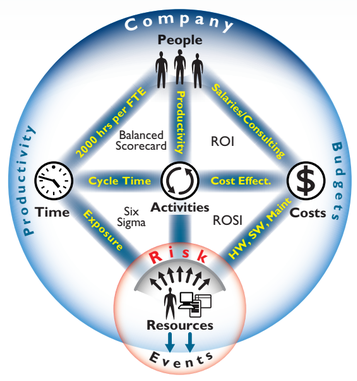
How to Use This Poster

This poster describes Spire Security's Four Disciplines of Security Management. The horizontal axis of Identity Management and Vulnerability Management identify the functions, processes, and products used to provide ongoing operational management of users and resources. The vertical axis of Trust Management and Threat Management integrates proactive security measures during design with ongoing security monitoring.

Security Metrics

At the core of any metrics program is information about activities. From that center, data can be collected about people, time, and costs associated with these activities. Finally, resources can provide information about risk - the true core of our security program.

When these metrics are compared and contrasted, they provide applicable information to address Return on Investment (ROI -people, costs, activities); Return on Security Investment (ROSI - activities, costs, resources); Benchmarking programs like Harvard's Balanced Scorecard (people, activities, time); and finally quality programs like Six Sigma (time, activities, resources).



SIERRA VENTURES
www.sierraventures.com