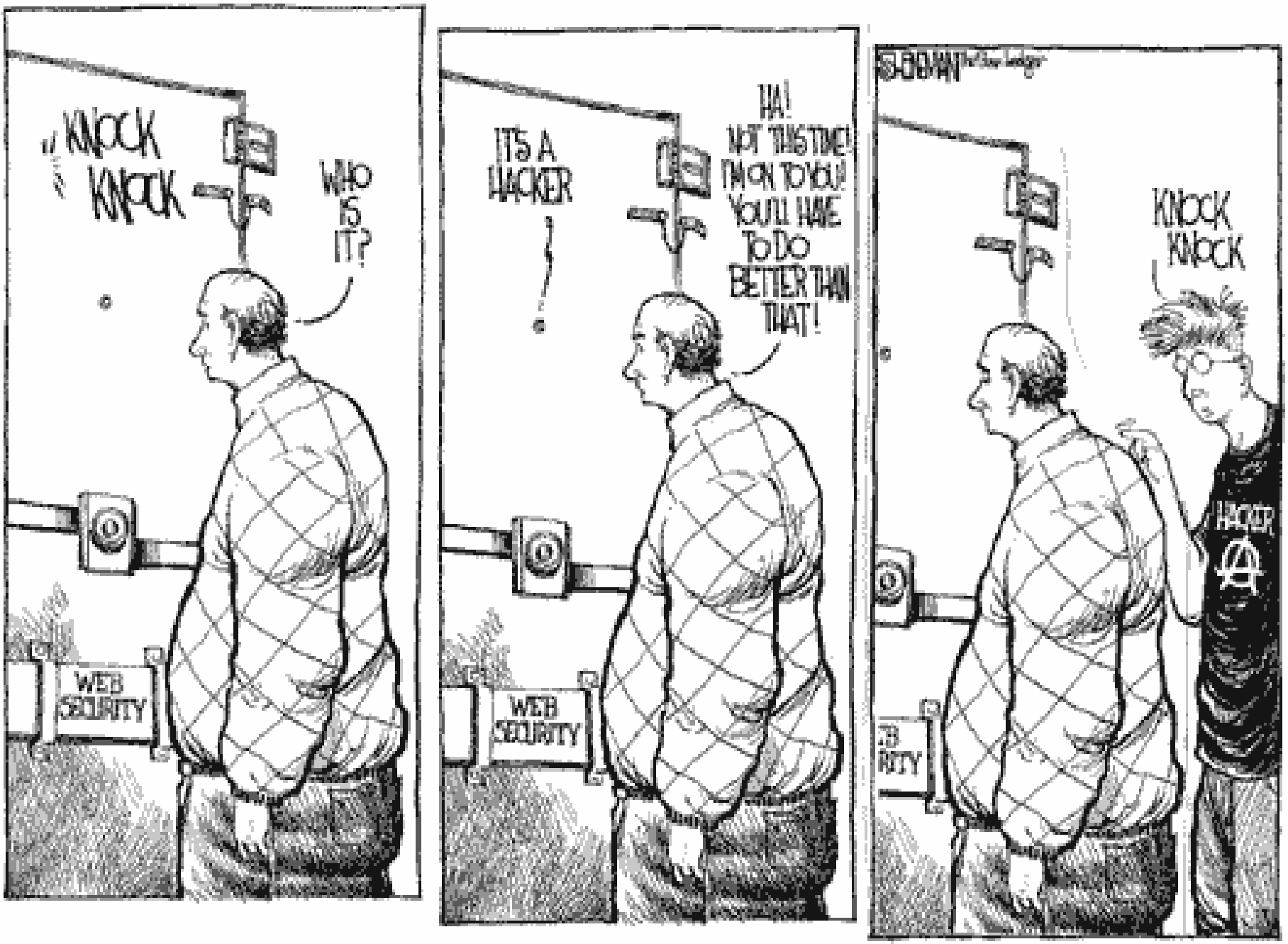
CITADEL™
SECURITY SOFTWARE

Serious and Secure.

Hercules and Vulnerability Related Security Standards

Kent Landfield
Director, Remediation Security Group

Where Is The Problem?



Hercules in a Nutshell

- **Automated Vulnerability Remediation (AVR)**
- **World's largest repository of tested and proven remedies**
  - All 5 classes of vulnerabilities
  - In-house team of security experts
  - Automated V-Flash delivery
- **Heterogeneous platform support**
  - Windows, Solaris, HP-UX, AIX, Linux, Tru64 & Mac OS-10
- **Set and enforce security policy**
  - Policy templates
  - Scheduled compliance checks
- **ConnectGuard™ Endpoint security / NAC Support**

- **Scanner remediation**
  - Upholds separation of duties
  - Leverage existing IT investment
  - Aggregate scan data for comprehensive remediation
  - Independent vulnerability assessments
- **Zero day vulnerability remediation**
  - AssetGuard™ 'targeted' vulnerability management
- **Tested and certified solution**
  - Microsoft Windows 2000, 2003 certified
  - Common Criteria certification EAL 3
  - ISO 15408 Certified

CITADEL™ SECURITY SOFTWARE

Five Classes of Vulnerabilities

Vulnerability: A weakness in process, administration or technology that can be exploited to compromise IT security – *Gartner*

Unsecured Accounts

- Null Password, Admin no PW, no PW expiration…

Unnecessary Services

- VNC, PCAnywhere, KaZaa, Telnet . . .

Backdoors

- Spyware (KaZaa, DownloadWare, 180 Solutions, GAIN), MyDoom.A, BACKORIFICE, SUBSEVEN . . .

Mis-configurations

- Netbios shares, Anonymous FTP world r/w, hosts.equiv . . .

Software Defects (Missing Patches)

- Buffer overruns, RPC-DCOM, SQL Injection . . .

Hercules Supported Models of Vulnerability Remediation

Top-down

- Define asset baseline
- Define security baseline
- Enforce IT security configurations

Check Compliance or Enforce Policy

Bottom-up

- Assess vulnerability state
- Remediate detected vulnerabilities

Scan Validate Remediate

Targeted

- New, critical vulnerabilities
- Key assets

Near Day Mitigation

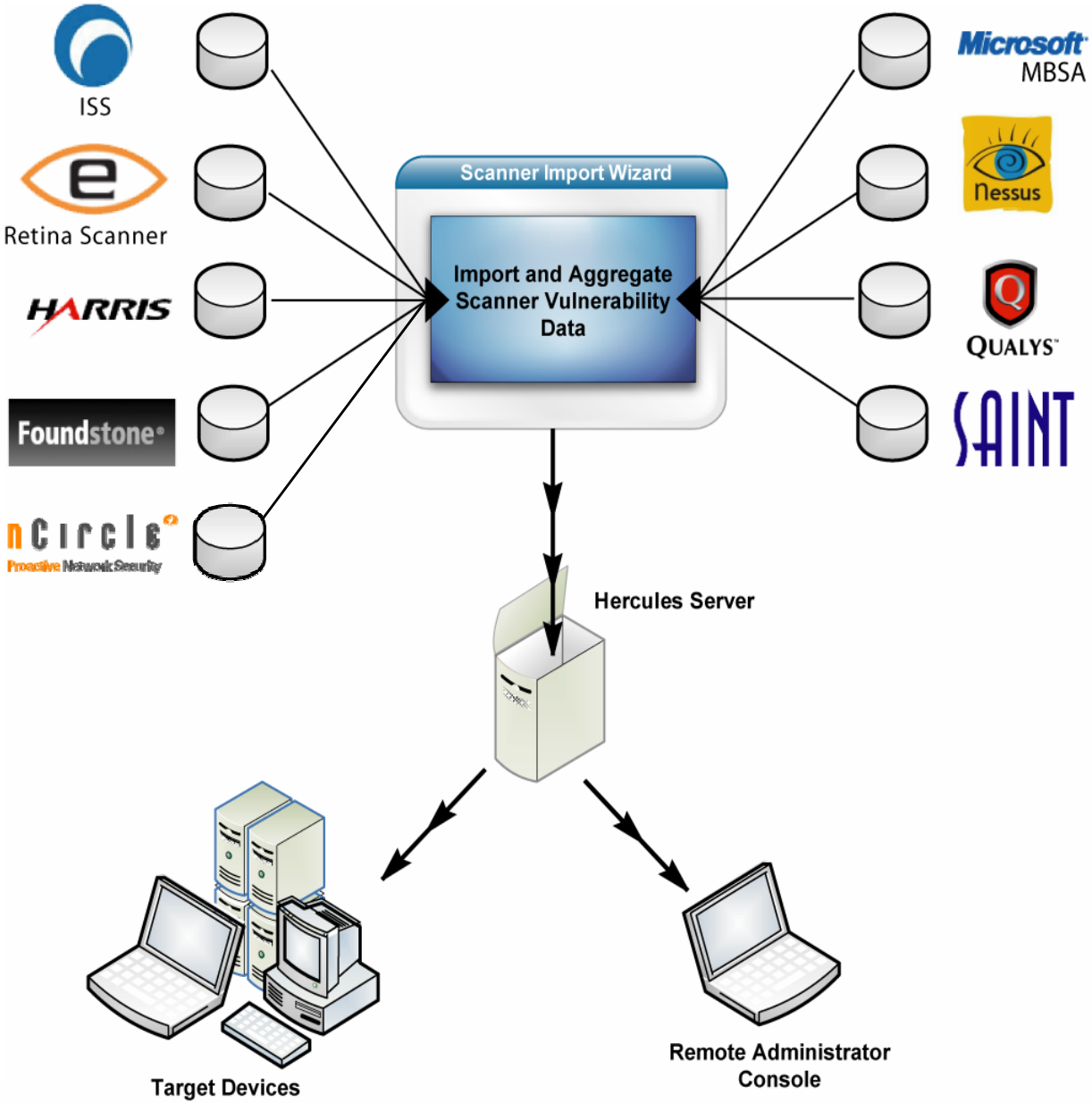
Compliance Enforcement (Top-Down)

- Consistently Assess and Enforce Security Policy Across The Enterprise
  - –Scheduled or On-demand
  - –Out-of-the-box Templates
  - –Custom Templates
- Detailed Compliance Assessment
  - –Password settings, account privileges, event logs, audit settings, files, services, legal notices, etc.
- Bring Non-compliant Devices Back Into Compliance

Hercules Provides "Best Practices" Policy Templates:

- GLBA
- HIPPA
- SOX
- SANS Top 20
- DISA STIGS
- FISMA
- MS Win2k Gold
- NSA Security Configuration Guides

Scan and Remediate (Bottom-up)



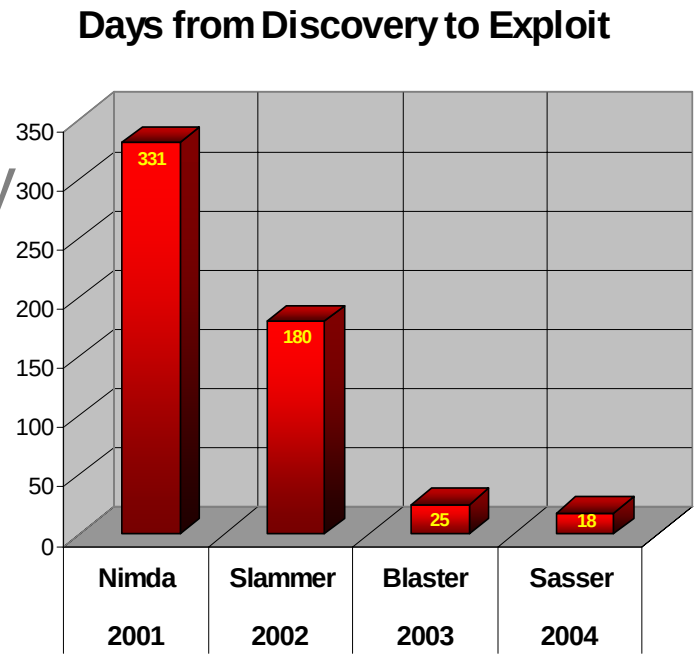
1. Aggregate scan data
2. Correlate with remedy library
3. Fix vulnerabilities
4. Report on status

Near Day Mitigation (Targeted)

HERCULES AssetGuard™
Device Inventory & Remediation

Cisco Compatible

- Actionable asset intelligence
- Immediately identify and remediate vulnerabilities on key assets
  - Asset Inventory
  - Asset Query
  - ActionPacks
- Empowers policy enforcement and remediation
- Enables near day mitigation



Compiled from CERT, SANS and Microsoft websites

Extending Policy to the Endpoint

HERCULES ConnectGuard™
Host Quarantine & Remediation

Cisco Compatible

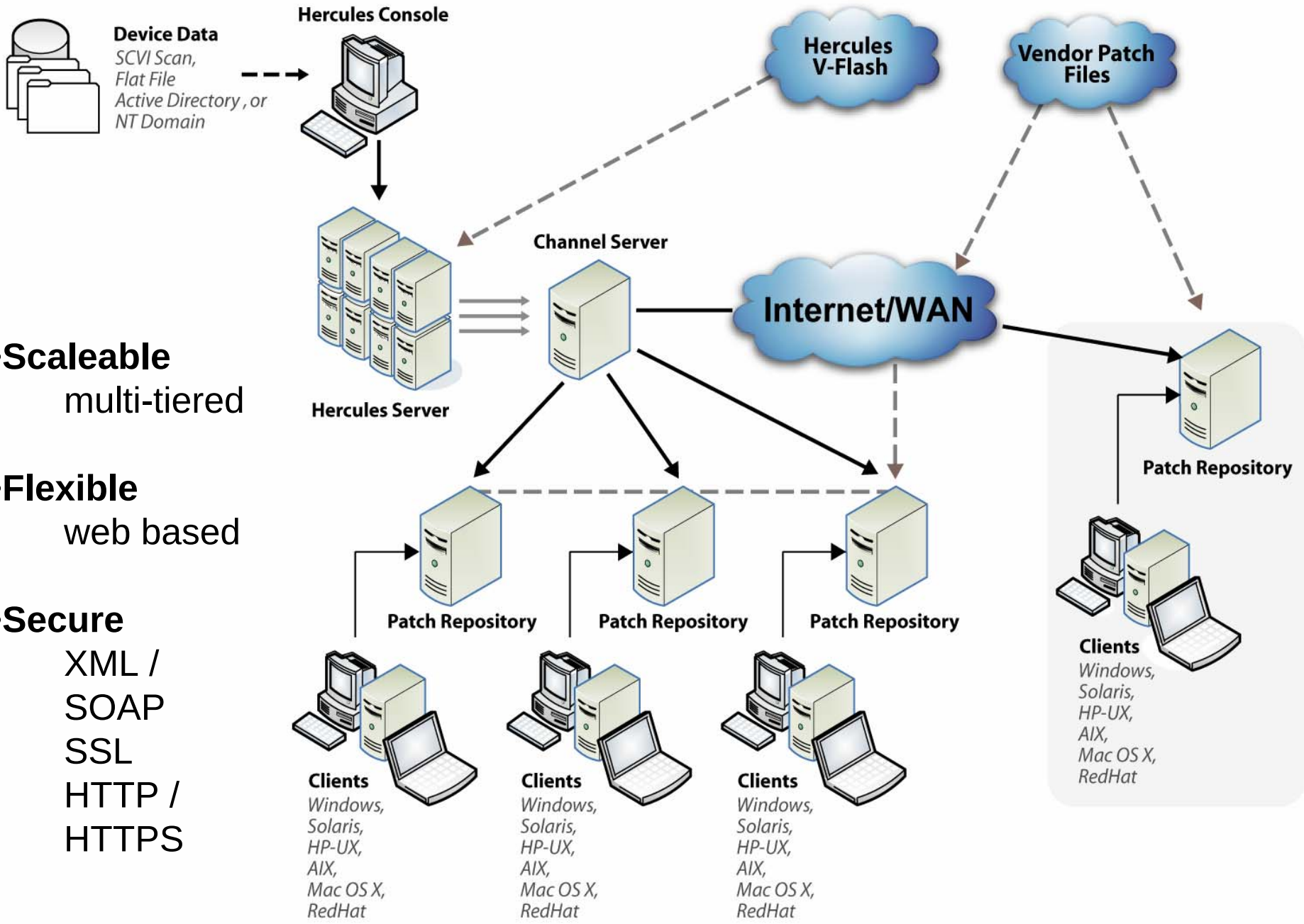
- Host-based quarantine *and* remediation solution
- Protection for disconnected devices (laptops, desktops, servers)
- Prevents un-trusted devices that have been off the network from gaining access to the network ***until*** remediated

> "The consistent sanitization of infected endpoint devices and enforcement of security and configuration polices before reconnecting to the network is critical to ensuring the security of enterprise networks."
>
> *- The Meta Group*

Cisco NAC Partner

Hercules Scalability

- **Scaleable**
  multi-tiered
- **Flexible**
  web based
- **Secure**
  XML / SOAP
  SSL
  HTTP / HTTPS

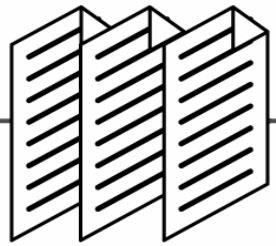


RSG Remediation Development

Security Knowledge Team
Collects & gathers security knowledge from as many sources as possible.

Vulnerability Remediation Team
Researches all vulnerabilities & possible solutions. Designs & develops all remedies. 1st line of testing.

Quality Assurance Team
Extensively tests all remedies before making them available to customers.



Remedies

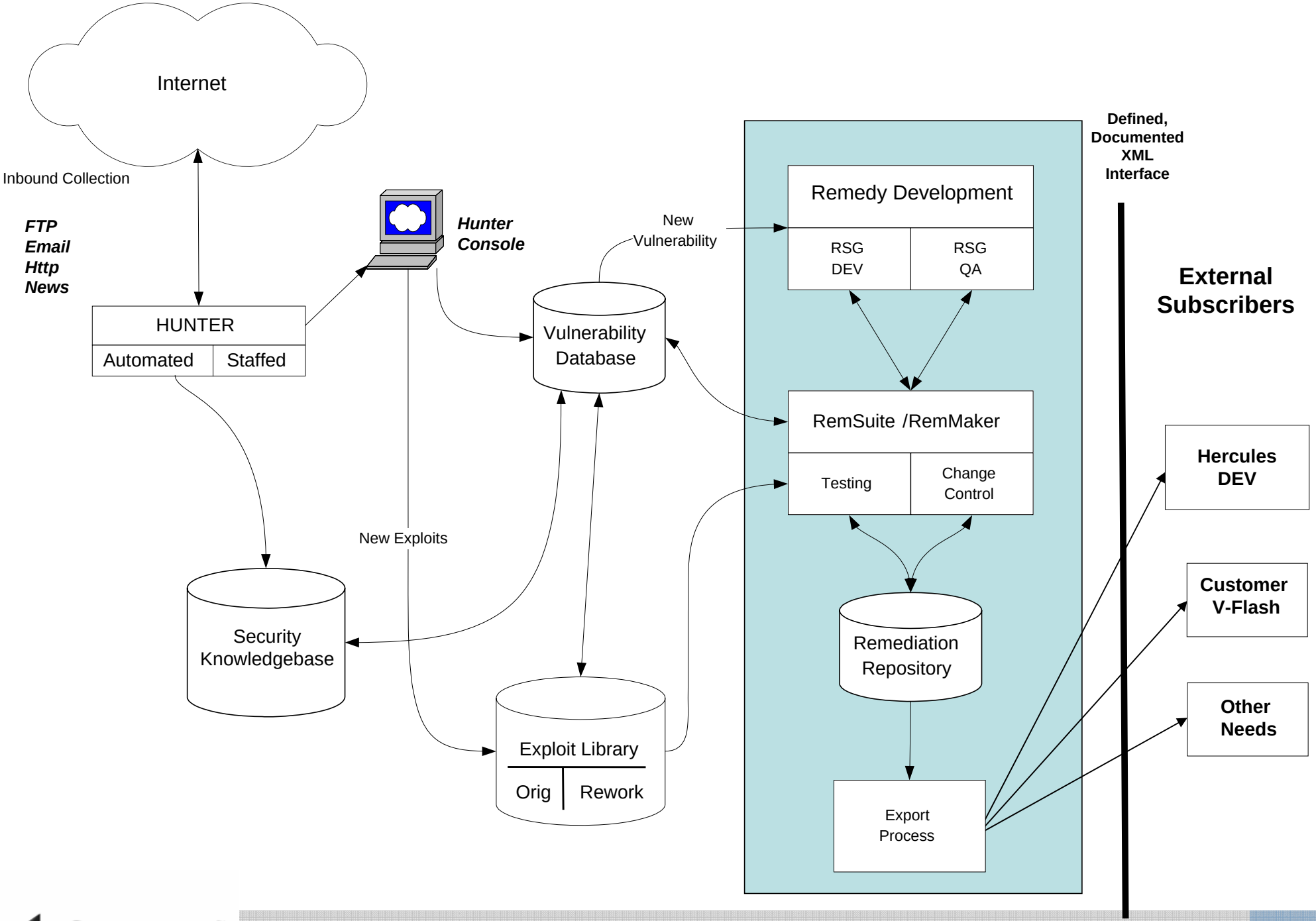
Gathered from:
OS vendor security lists
Security web sites
Global security mailing lists
Vulnerability scanner vendors
Anti-virus vendors
Application vendor security lists
Usenet news groups
IRC or Chat sites
Industry organizations (SANS, CVE, CIS, etc.)
Our security partners

28,000 + Remedies

Hercules Server at Client Site

Citadel's V-Flash Server
Maintains the library of all Remedies

RSG Architecture



Required Data Stream Management

- New Scanner IDs Associated with Hercules IDs
- Updated Scanner Information
- Vendor Alerts (HP, AIX, Apple, Sun, RedHat, Microsoft, etc.)
- IAVA Alerts
- OVAL and CVE Updates
- Industry advisories (Secunia, BugTraq, CERT, IT-ISAC, etc.)
- Patch URL Updates
- Policy and Hardening Guide Updates
- Industry Checklists

RSG Scanner Support

Incorporating Daily Scanner Updates

- **eEye**
  - Retina
  - REM
- **Harris**
  - STAT
  - STAT Guardian
- **ISS**
  - Internet Scanner
  - System Scanner
  - SiteProtector
- **McAfee Foundstone**
  - Foundscan
- **Microsoft**
  - Baseline Security Analyzer 1.2 and 2.0
- **OVAL**
  - OVAL Reference / ThreatGuard
- **Qualys**
  - QUALYSGUARD
- **netVigilance/NextaniS**
  - SecureScout
- **Saint**
  - Saint Scanner
- **Tenable**
  - Nessus
  - NeWt
- **OpenSource**
  - Nessus
- **OS2A**
  - Nessus
- **nCircle**
  - IP360

Additional RSG Initiatives

OVAL / CVE / CCE

Exploit Library

Remediations Operations Center

IAVM Support and DB

XCCDF

Security Research

DISA STIG Remedy Enhancements

CITADEL™
SECURITY SOFTWARE

Serious and Secure.

Security Content Integration

Bringing Together Security Information Streams

Standards Value to Vendors and Customers

Daily Security Content Issues

- **Data streams are rapidly growing**
- **Only way to keep up is automating the tasks**
- **Correlate information using industry standard reference information (CVE, BID, Vendor IDs, etc)**
- **Making heavily content-based products possible and more useful**

Participation in the Security Industry

- **Cyber Security Industry Alliance**
  - Advocacy group dedicated to the improvement of cyber security through public policy, education and technology-focused initiatives
- **OVAL (Open Vulnerability & Assessment Language)**
  - Carl Banzhof, Kent Landfield OVAL Board Members
  - Hercules certified as OVAL Results Schema Compatible
- **CVE (Common Vulnerabilities & Exposures) Standard**
  - Kent Landfield early CVE Editorial Board Member
  - Hercules certified as a CVE Compatible product
- **CCE**
  - Participating in initial CCE foundation work
- **OASIS**
  - Application Vulnerability Description Language Standard
  - Web Application Security XML (WAS) Technical Committee
- **NIST**
  - The Vulnerability Management solution compliant with NIST Pub 800-70 requirements as defined by the Cyber Security Research and Development Act of 2002
  - Participating in NIST/NSA's Extensible Checklist Configuration Description Format (XCCDF) effort
  - Participated in the NIST "Workshop on State of the Art in Software Assurance Tools"

Vulnerability and Compliance Related Standards efforts

- CVE (Common Vulnerabilities and Exposures)
- OVAL (Open Vulnerability and Assessment Language)
- XCCDF (The Extensible Configuration Checklist Description Format)
- CVSS (Common Vulnerability Scoring System)
- NVD (National Vulnerability Database)
- CCE (Common Configuration Enumeration)

Information Exchange (or why are we here?)

- Purpose:
  - Provide the community with the ability to exchange security, system state and vulnerability related information within the networked community and security products

- Standards:
  - CVE
  - OVAL
  - XCCDF
  - CVSS
  - CCE (an early work in progress)

- Repositories:
  - CVE
  - OVAL
  - NVD

Security Standards Development Models

- IETF Approach
  - Can be effective, can easily fail
  - Can take a great deal of time to produce results
  - Can be swayed by a small group of vocal participants
- OASIS Approach
  - Pay to vote
- Vertical Special Interest Group
  - Pay to vote (sometimes)
  - Focus only on the interest of a specific group
- CVE/OVAL Model

CVE/OVAL Model

Whether intended or just by accident, the CVE/OVAL Model is working.

- Focuses on the end goal
- Listening to the community directions and desires
- Hard to be taken over by a single company or individual
- Hard to be ignored by vendors over the long run
- Educates the community at the same time promoting the standard
- Moderated/Managed with the end customer community at large in mind

Marketing to the Security Vendor and end user community at trade shows and conferences has a real impact.

But the reality as I see it is…

While we are all excited about what we can accomplish, we need help to make the entire XCCDF/OVAL vision succeed…

Funding history for these valuable efforts has not had a good history. Vendors are being asked to invest in these efforts. The government needs to step it up as well so more vendors and customers feel comfortable in investing in the efforts. Nothing is free.

The XCCDF Editor is CRITICAL. Without it modifying XCCDF documents for local use will be extremely time consuming and laborious. The success of the XCCDF Editor Project could end up being the enabler allowing organizations to adopt XCCDF/OVAL Checklist usage in the near future. We can either speed up the availability of that enabling tool or we can wait and potentially loose momentum.

We need to look at the overall efforts and apply the resources where we can truly benefit the community at large.

Questions???

We have come a long way in a year. Let's not stumble now.

Kent Landfield

klandfield@citadel.com

Office: 214.750.2492

See y'all at the Third Annual Security Automation Conference.