2009 Nebraska Cert Security Conference

Security Operations in a Multi-Vendor World

Jerry Errett PMP CISSP
Dan Jacobson

Security operations in a multi-vendor world

There are great open source security solutions for intrusion detection, vulnerability management, access control, and audit logging. This presentation shows you how to use them together to provide an overall security picture for environments containing up to 100,000 devices.

Presentation Agenda

- Security Software
- Background
  - Target environment
  - Security areas
- Issues
  - Size matters
  - Operational issues
- Solution
  - Device model
  - Groups
  - Rules
  - Databases
- Another Perspective
- Unisys
- Q/A

Open Source Security Software

Top 100 Network security tools http://sectools.org

8 Great Free Security Tools http://www.networkworld.com/

10 Best Free Security Tools
http://www.itsecurity.com/features/10-best-free-security-sec

INSECURE.ORG http://insecure.org

Background - Target Environment

- 100,000 devices
- Thousands of routers
- Thousands of offices
- Multiple web farms
- Very complex management structure
- International operations

Background – Security areas

- Access control
- Anti-virus
- Incident response
- Intrusion detection
- Log analysis
- Security device management
- Vulnerability management
- Vulnerability research

Issues – Size Matters

- “Census” problem
- Hardware issues
- Network issues
- Data capture issues
- Data processing issues

Size matters - Hardware issues

- Identifying hardware is challenging
  - Network
    - Firewalls
    - NAT
    - DHCP
  - Mobile users
    - Multiple offices
    - Remote access

Size matters - Hardware issues

- Identifying hardware in a large environment is challenging
    - Intermittent devices
        - New devices
        - Rebuilt devices
        - Off-line devices
        - Third party devices
    - Virtual devices
    - Clustered devices
    - Generic host names

Size matters - Network issues

- Topology
  - Multiple security device locations
  - Redundant paths
- Connectivity
- Bandwidth
- Latency

Size matters – Data capture

- Multiple security devices
- Multiple security device locations
- Multiple software security tools

Size matters – Data processing

- Data captured at different times
- Security data is often unreliable
  - OS fingerprinting
  - Network issues
  - Signature issues (false positive/negative)
- Mountain of data
- Multiple data formats

Operational Issues

- Who owns the device?
- Who uses the device?
- Who maintains the device?
- Who is responsible for the security posture of the device?

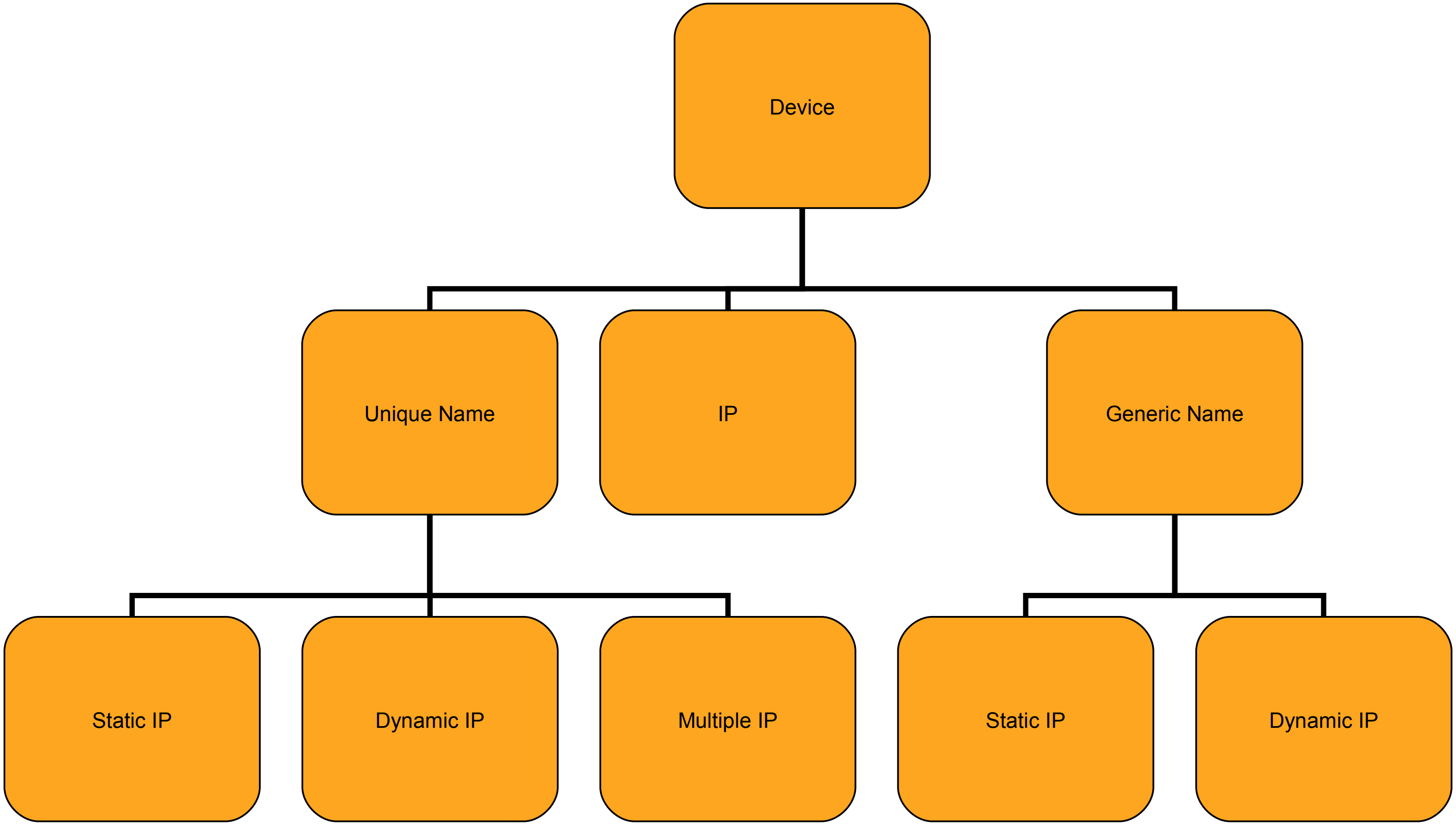
Presentation Agenda

- *Security Software*
- *Background*
  - *Target environment*
  - *Security areas*
- *Issues*
  - *Size matters*
  - *Operational issues*
- Solutions
  - Device model
  - Groups
  - Rules
  - Databases
- Another Perspective
- Unisys
- Q/A

Device model
How many devices were scanned?

Scan Date	IP	DNS Name
1/1/2010	10.10.10.10	MFP-k2000
1/1/2010	10.20.10.10	MFP-k2000
1/1/2010	10.30.10.10	MFP-k2000
1/1/2010	10.100.50.100	WebServerOne
1/1/2010	10.100.50.101	WebServerOne
1/1/2010	10.100.50.102	WebServerOne
1/1/2010	10.100.50.103	WebServerOne
1/1/2010	10.10.10.100	Laptop150
1/1/2010	10.10.10.2	
2/1/2010	10.10.10.10	MFP-k2000
2/1/2010	10.20.10.20	MFP-k2000
2/1/2010	10.100.50.100	WebServerOne
2/1/2010	10.100.50.101	WebServerOne
2/1/2010	10.100.50.102	WebServerOne
2/1/2010	10.100.50.103	WebServerOne
2/1/2010	10.10.10.120	Laptop150
2/1/2010	10.10.10.2	

Device model overview



Device

Unique Name

IP

Generic Name

Static IP

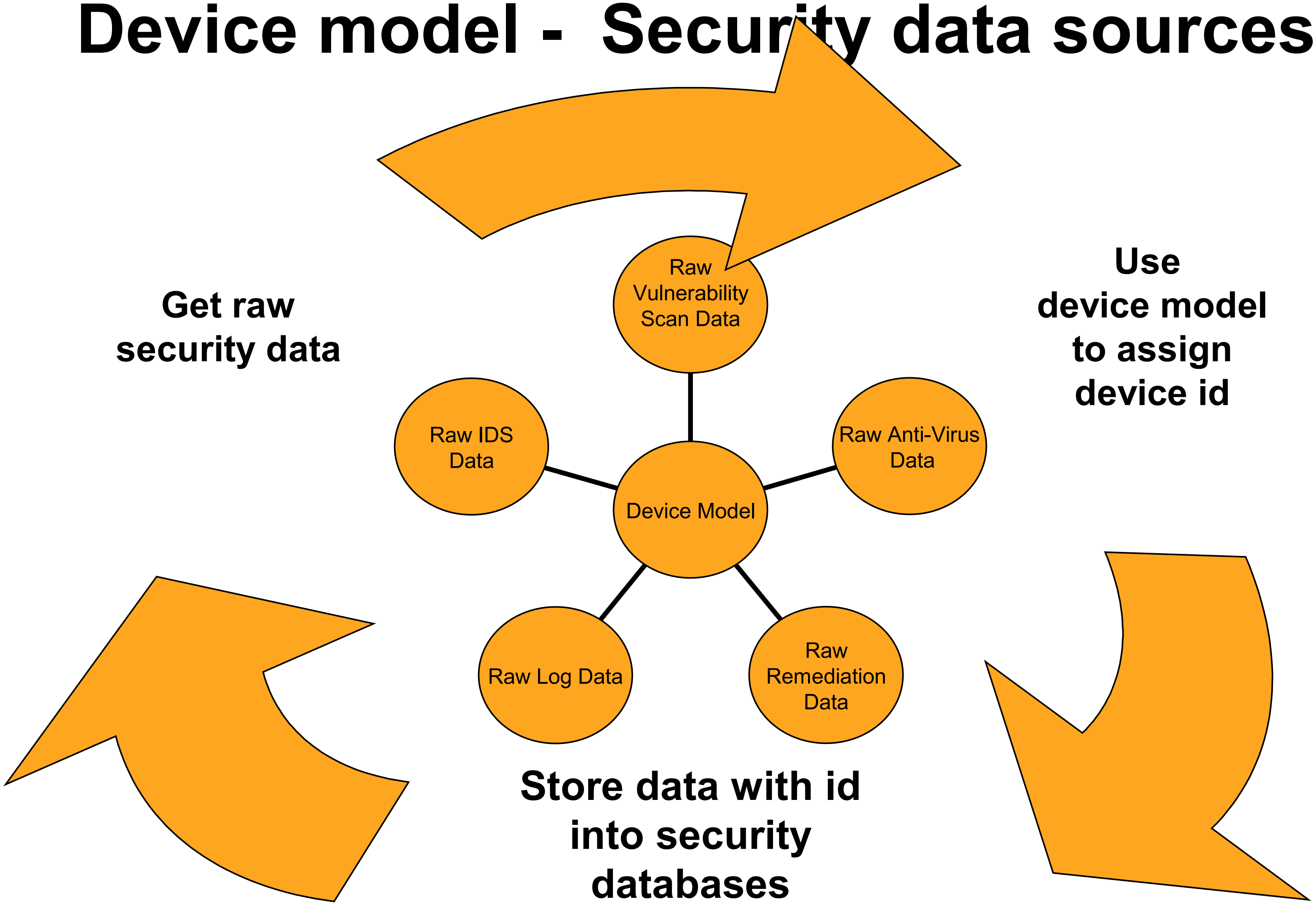
Dynamic IP

Multiple IP

Static IP

Dynamic IP

Device model - Security data sources

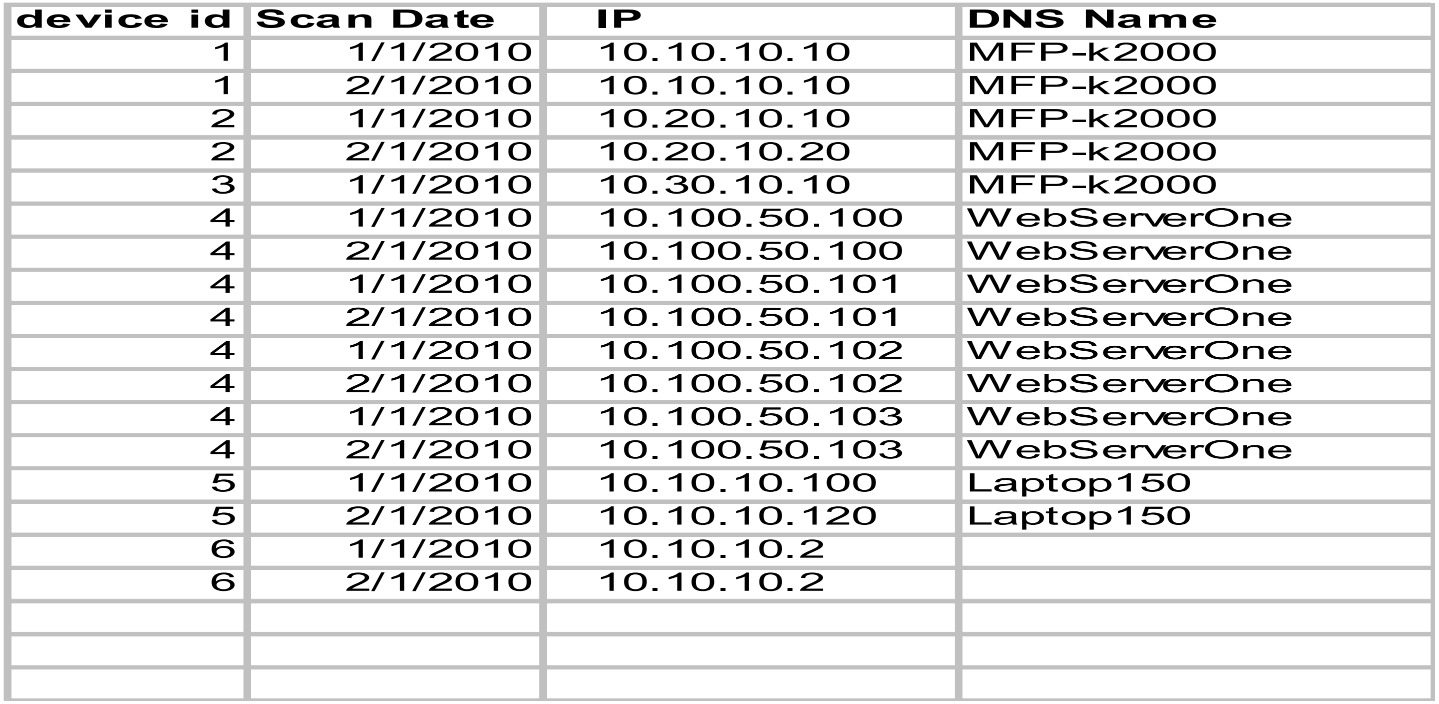


Get raw security data

Use device model to assign device id

Store data with id into security databases

Device Model
Scan data with device id



device id	Scan Date	IP	DNS Name
1	1/1/2010	10.10.10.10	MFP-k2000
1	2/1/2010	10.10.10.10	MFP-k2000
2	1/1/2010	10.20.10.10	MFP-k2000
2	2/1/2010	10.20.10.20	MFP-k2000
3	1/1/2010	10.30.10.10	MFP-k2000
4	1/1/2010	10.100.50.100	WebServerOne
4	2/1/2010	10.100.50.100	WebServerOne
4	1/1/2010	10.100.50.101	WebServerOne
4	2/1/2010	10.100.50.101	WebServerOne
4	1/1/2010	10.100.50.102	WebServerOne
4	2/1/2010	10.100.50.102	WebServerOne
4	1/1/2010	10.100.50.103	WebServerOne
4	2/1/2010	10.100.50.103	WebServerOne
5	1/1/2010	10.10.10.100	Laptop150
5	2/1/2010	10.10.10.120	Laptop150
6	1/1/2010	10.10.10.2	
6	2/1/2010	10.10.10.2	

Solution - Groups

Always treat devices as a group/set

- Even if the group only has one device
- Allow a single device to exist in multiple groups
- A hard sell for some people
  - Too abstract and/or complicated
  - It can be difficult to quantify achievement gained for the effort expended
  - Difficult to determine “correct” groups
  - Handling “exceptions” can be difficult
- Critical for successful management of large numbers of devices

Solution - Groups

device id	Group
1	Printer
1	Low Risk
2	Printer
2	Low Risk
3	Printer
3	Low Risk
4	Web Server
4	Medium Risk
4	Marketing
4	Midwest
5	VIP
5	High Risk
6	Telecom

Solutions - Rules

Use table driven rules to massage data

- Must support effective dates
- Rules apply to groups
- Support exceptions and defaults
- Automatic assignment of default groups
- Automatic assignment of default roles
- Log and track all changes to rules
- Log and track rule execution

Solution – Databases

- Assume the databases will receive meaningless data.
- Separate raw data from security devices from processed data.
- Spend time on reducing database size
- Be prepared for iterative processing cycles
- “Outlier” reports are critical
- Secure security data

Presentation Agenda

- *Security Software*
- *Background*
  - *Target environment*
  - *Security areas*
- *Issues*
  - *Size matters*
  - *Operational issues*
- *Solutions*
  - *Device model*
  - *Groups*
  - *Rules*
  - *Databases*
- Another Perspective
- Unisys
- Q/A

Another Perspective

Third party security suites that provide comprehensive solutions can be nice, but they can also be expensive, and there is always the risk that they won't scale well. Another risk is that the ability to respond to potential security issues is limited to what a single software vendor is able to provide. They may also have cumbersome and opaque proprietary code that is difficult (if not impossible) to customize to suit the needs of your network.

Vendors may also insist upon managing the solution themselves and only alert your security staff after conducting research into any issues. Many organizations can't afford any delay in notification, even for false positives.

Another Perspective

It is entirely possible to combine several separate tools in a way that serves a similar purpose to the comprehensive security suites.

Any software distribution system that employs a server/client type of model can be very useful.

Many anti-virus products work in that way; a central server retrieves signature updates from the vendor's repository, and then pushes those updates down to endpoints on the network. In order to make sure that it's working properly, the server maintains a database where clients that check in are able to deliver information about detections and about their update status.

Another Perspective

Get to know the network and its devices

- In user environment, what is the standard OS and software package?
- When are people allowed to install and run additional software?
- Is there a list maintained somewhere of users who are authorized to have other software?
- What are basic user permissions, what are the exceptions, and where is this information available for verification if necessary?
- Who is responsible for patches and updates, especially in the case of non-standard (but still authorized) applications?
- What is the naming convention for devices and users?
- In the server and web environment, what applications are running? What is the standard authorized version for each of them?

Another Perspective

There are several ways of obtaining information, and many system and network tools are able to do more than what they were designed/marketed/purchased for.

Security staff should familiarize themselves with all of the tools, with the information they gather, where they store it, etc.

It helps to spend some time looking around in the databases for the software (or in the logs for logging tools) and seeing what the entries and activity for normal systems look like.

"Normal" is actually a dynamic state, so keep the available information as current as possible.

Another Perspective

Some sites that are useful in keeping up to date are:

- http://isc.sans.org/diary.html (updated several times daily)
- http://ddanchev.blogspot.com/ (a security consultant and zdnet columnist--the place to go for information on fake anti-virus domains and social networking exploits)
- http://www.malwaredomainlist.com/ (updated regularly with a list of known malicious sites and sometimes the type of exploits they run or code they are serving.)
- http://www.robtex.com (this site allows reverse dns lookup on IP addresses, allows IP address lookup when given a dns name, has information on the class-c network of any IP address, does a whois lookup for domain registrations, has the AS numbers, and can do rough geo-location. It's also able to list shared domains--if an IP address has several domain names pointing to it that can be a red flag, especially if they were recently registered)
- http://wepawet.iseclab.org/ (this is a free web-based tool for analysis of a suspicious web page without having to actually browse to the page to find out. It looks for malicious flash objects, javascripts, and pdf files and then puts together a report on the fly)

Presentation Agenda

- *Security Software*
- *Background*
  - *Target environment*
  - *Security areas*
- *Issues*
  - *Size matters*
  - *Operational issues*
- *Solutions*
  - *Device model*
  - *Groups*
  - *Rules*
  - *Databases*
- *Another Perspective*
- Unisys
- Q/A

UNISYS
imagine it. done.

A worldwide information technology services and solutions company

- Unisys designs, builds, and manages mission-critical environments for businesses and governments who have no room for error. Because we have a deep understanding of high-volume, transaction-intensive, and secure computing, we can partner with our clients to deliver operational efficiencies, reduced complexity, increased productivity, and peace of mind.

Q / A