NitroSecurity Intrusion Prevention Overview for OSSIR (Groupe SUR)

Marc Berlow, Cressida France
Cressida Int’l Company History

- Created by Systems Administration and Security Experts in 2001
- Distributes and supports software across all European markets

Main products:
- NitroSecurity Suite
  - Intrusion Prevention Systems
- Ecora
  - Configuration & Change Reporting, Baseline & Compare settings, Automated Patch Management, Devices Security
- Akonix
  - Real time solutions for Secure, Managed, Productive Enterprise Instant Messaging
- MQ Message Assurance
  - Track, Record, Audit, Replay, Edit WMQ Messages
- RepliWeb
  - Industrialized Strength Disaster Recovery cross platform tool, replication, distribution, synchronization
NitroSecurity Company History

Technology origins U.S. Department of Energy's Idaho National Engineering and Environmental Laboratory (INEEL) (Sister to Los Alamos, Sandia, Oakridge)

Products

- **NitroEDB**- High performance embedded relational database
  - Built to handle exact, high speed data demands of nuclear power industry
  - $30M and 65 man years invested
  - Commercialized in 1999 for the OEM community

- **NitroGuard IPS**- In line intrusion prevention solution
  - Open Source Debut in 2001 at DEFCON
  - Commercialized in 4th Quarter of 2001
  - 2002 version 3.0 introduced new Technologies for Detection, Analysis including integrating in-line SNORT, and Remote Communications
  - 2003 version 4.0 introduced improved Device Analysis and more comprehensive Management Console queries and analysis capabilities
So many attacks, so little time…
NitroGuard Concepts

- Next Generation Network-Based Intrusion Prevention System
  - No client agents
  - No version management or interoperability issues
  - Scalable to any size enterprise

- Ultra-fast database
  - Same database used to correlate data from all U.S nuclear power plants
  - Highly scalable
  - Technology embedded in upcoming Cisco monitoring products

- Enterprise management console
  - Enterprise wide correlation from all IPSs
  - Robust reporting
A Layered Security Approach

<table>
<thead>
<tr>
<th>Security Threat</th>
<th>Firewall</th>
<th>Antivirus</th>
<th>NitroSecurity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limits access to parts of the network</td>
<td>FULL</td>
<td></td>
<td>FULL</td>
</tr>
<tr>
<td>Translates internal addresses to external addresses</td>
<td>FULL</td>
<td></td>
<td>No IP Address</td>
</tr>
<tr>
<td>Protects against virus attacks</td>
<td>FULL</td>
<td></td>
<td>PARTIAL</td>
</tr>
<tr>
<td>Protects against worms</td>
<td>FULL</td>
<td></td>
<td>PARTIAL</td>
</tr>
<tr>
<td>Protects against combination worm/intrusion attacks (Nimda, CodeRed)</td>
<td>PARTIAL</td>
<td></td>
<td>FULL</td>
</tr>
<tr>
<td>Protects against intrusion</td>
<td>*FULL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prevents outbound attacks</td>
<td>*FULL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prevents outbound critical data loss</td>
<td>*FULL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enforces policy rules (porn, gambling, webmail, IM, etc)</td>
<td>*FULL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logs intrusion alerts for post-analysis</td>
<td>*FULL</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
NitroGuard Security Architecture
NitroSecurity IPS Family

- **Enterprise-Scale, In-line IPS**
  - Active (IPS) or promiscuous (IDS) mode in single device
  - Real-time event correlation and analysis across entire enterprise via embedded security database architecture

- **Integrated Signature/Anomaly Detection**
  - Industry’s largest signature (3600+) library
  - Fully customizable signatures/reports
  - Protocol and behavioral anomaly support

- **Stealth Operation Mode**
  - Industry’s only IPS that has no IP address using in-band management
  - Invisible to typical network attacks
NitroSecurity IPS Architecture

Network Traffic

- Deep Packet Inspection Engine
- Signature Detection Engine
- Anomaly Detection Engine
- NitroEDB™ (Embedded Database)

Secure Encrypted Control (NitroSEC™)

Desired Traffic

Alert → Block → Pass

In-Band Management
NitroEDB™ Overview

- NitroEDB™ enables real-time, enterprise-wide correlation of security data across an unlimited number of NitroGuard IPS
- Traditional IPS designs decrease in performance and correlation capabilities as security data increases
NitroSEC™ Overview

- NitroSEC™ makes NitroGuard IPS virtually impossible to attack (and does not require out-of-band management)
- Traditional IPS designs use an IP address for management (or require an out-of-band management interface and network)
NitroSecurity Demonstration

Please contact us at www.cressida.info for a live demo
## System Information

**Nitro Guard Control Panel**

Version 4.2.3 - 3440:10F6

Copyright (c) 2002, 2003 by Nitro Data Systems, Inc. All rights reserved.

## Rule Server Status

Connection Ok

## Company Information

Nitro Data Systems, Inc.

(208)552-5332

info@nitrodata.com

## Status And Alerts

<table>
<thead>
<tr>
<th>Last Check:</th>
<th>11/13/2004 16:25:00.000</th>
<th>Next In:</th>
<th>00:00</th>
</tr>
</thead>
<tbody>
<tr>
<td>Currently Checking</td>
<td>&lt;disabled&gt;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Notifications

<table>
<thead>
<tr>
<th>Last Check:</th>
<th>01/07/2005 08:47:53.000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Currently Checking</td>
<td>&lt;done checking&gt;</td>
</tr>
</tbody>
</table>

## Rules And Software

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Check:</td>
<td>11/30/2004 10:40:00.000</td>
</tr>
<tr>
<td>Current Checking:</td>
<td>&lt;inactive&gt;</td>
</tr>
<tr>
<td>Latest Software:</td>
<td>Version 4.2.3</td>
</tr>
<tr>
<td>Next Check:</td>
<td>01/07/2005 08:48:00.000</td>
</tr>
</tbody>
</table>
Nitro Guard Control Panel

Group

Group 1

Information | Settings | Alert Queries | EMail | Conditions | Custom Rulesets

Properties

Queries

<table>
<thead>
<tr>
<th>Query Name</th>
<th>Query Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>!CountSegment</td>
<td>CLEARFORMAT</td>
</tr>
</tbody>
</table>

FORMAT TIME('','LEFT, 20,'mm/dd/yyyy hh:mm:ss')

FORMAT TIME('','LEFT, 20,'mm/dd/yyyy hh:mm:ss')

FORMAT NUM('','RIGHT,13,'')

FORMAT NUM('','RIGHT,13,'')

SELECT ???P6??, ???P8??, COUNT(*), SUM(Alert.EventCount)

FROM Alert

WHERE Alert.IPSID IN (??P22??)

AND Alert.LastTime >= ???P6??

AND Alert.LastTime < ???P8??

??P9?? AND SrcIP IN (??P10??)

??P11?? AND SrcPort IN (??P12??)

??P13?? AND DstIP IN (??P14??)

??P15?? AND DstPort IN (??P16??)

??P17?? AND Protocol IN (??P18??)

??P19?? AND SigID IN (??P20??)
Cressida presents NitroSecurity
Cressida presents NitroSecurity
<table>
<thead>
<tr>
<th>SigID</th>
<th>Count</th>
<th>Total</th>
<th>Usage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1001483</td>
<td>2</td>
<td>2,760</td>
<td>Alert</td>
<td>MISC UPNP malformed advertisement</td>
</tr>
<tr>
<td>1003048</td>
<td>3</td>
<td>186</td>
<td>Reject</td>
<td>MISC WATCHLIST - 20030613-window size 0xDA00</td>
</tr>
<tr>
<td>1002981</td>
<td>4</td>
<td>49</td>
<td>Alert</td>
<td>SCAN Traceroute UDP</td>
</tr>
<tr>
<td>1001358</td>
<td>6</td>
<td>44</td>
<td>Alert</td>
<td>ICMP Time-To-Live Exceeded in Transit</td>
</tr>
<tr>
<td>1001375</td>
<td>12</td>
<td>34</td>
<td>Reject</td>
<td>ICMP Communication Prohibited by Filtering</td>
</tr>
<tr>
<td>1002873</td>
<td>5</td>
<td>33</td>
<td>Reject</td>
<td>NETBIOS name-query</td>
</tr>
<tr>
<td>1000276</td>
<td>2</td>
<td>30</td>
<td>Reject</td>
<td>ICMP L3retriever ICMP PING</td>
</tr>
<tr>
<td>1002486</td>
<td>5</td>
<td>19</td>
<td>Alert</td>
<td>ICMP PING zeros</td>
</tr>
<tr>
<td>1001316</td>
<td>4</td>
<td>18</td>
<td>Alert</td>
<td>ICMP Port Unreachable</td>
</tr>
<tr>
<td>1003583</td>
<td>4</td>
<td>8</td>
<td>Alert</td>
<td>SMTP Non-SMTP Server Emails</td>
</tr>
<tr>
<td>1001299</td>
<td>2</td>
<td>7</td>
<td>Alert</td>
<td>ICMP Traceroute</td>
</tr>
<tr>
<td>1003604</td>
<td>1</td>
<td>7</td>
<td>Drop</td>
<td>EDONKEY connection to server</td>
</tr>
<tr>
<td>1001322</td>
<td>1</td>
<td>6</td>
<td>Alert</td>
<td>ICMP Echo Reply</td>
</tr>
<tr>
<td>1003583</td>
<td>1</td>
<td>6</td>
<td>Drop</td>
<td>SMTP Non-SMTP Server Emails</td>
</tr>
<tr>
<td>1001379</td>
<td>1</td>
<td>3</td>
<td>Alert</td>
<td>ICMP Large ICMP Packet</td>
</tr>
<tr>
<td>1001986</td>
<td>2</td>
<td>2</td>
<td>Alert</td>
<td>WEB-CGI adycle access</td>
</tr>
<tr>
<td>1001375</td>
<td>1</td>
<td>1</td>
<td>Alert</td>
<td>ICMP Communication Prohibited by Filtering</td>
</tr>
<tr>
<td>3116054</td>
<td>1</td>
<td>1</td>
<td>Alert</td>
<td>DECODE_TCP0PT_BADLEN</td>
</tr>
</tbody>
</table>

Total = 56  3,134
----- Group1:FIRST IPS -----
root$ |
NitroGuard Product Line

- NitroGuard 500 IPS
  - Ready for the enterprise
  - Redundant hardware
- NitroGuard 200 IPS
  - SME and departmental solution
- NitroGuard WG IPS
  - Work Group Solution
  - Protects internal assets
- NitroGuard M IPS
  - Built for SMB
  - Managed by a partner

In the US, Nitroguard is delivered embedded within a hardware box.

In Europe, NitroGuard is mostly provided as a software suite in order to run on hardware based on NitroSecurity exact specifications.
The NitroGuard Advantage

- User Customizable
  - Custom Signatures / Alerts
  - Custom Reports
  - Secure Application Gateway

- Signature updates
  - Based upon the industry’s most widely deployed Intrusion Detection System core – SNORT
  - Over 3,000 built in attack signatures
  - Multiple source vs. proprietary
  - Automated signature updates

- World Class Service and Support
  - 24X7 and managed service options available
  - Alpha response available
In an October 2003 release, Gartner advised clients to purchase a network-based IPS and states, “A true network-based intrusion prevention system must:”

- Operate as an in-line network device at wire speeds. √
- Perform packet normalization, assembly and inspection. √
- Apply rules based on several methodologies to packet streams, including (at a minimum) protocol anomaly analysis, signature analysis and behavior analysis. √
- Drop malicious sessions - don't simply reset connections. √

“Enterprises that have not yet made large investments in network IDSs should delay investment while investigating the advantages of Intrusion Prevention Solutions.”
Other Cressida Security Solutions: Ecora

- **Enterprise Auditor**

  *Ensure proper implementation and use of Security settings & policies*
  - Automatically generate configuration settings and change reports,
  - For security audits and compliance.
  - Covers all critical OS's, databases, network devices, and applications, including Cisco, Citrix, IBM, Microsoft and Oracle.

- **Patch Manager**

  *Make sure latest Operating System Security capabilities are effective*
  - Automate and accelerate patch management –
  - Easy to install and use,
  - Unsurpassed graphical reports.
  - Agentless or agent-based – your choice.

- **Device Lock**

  *Stop improper use of mobile and volatile storage devices*
  - Prevent users with USB drives from stealing your data.
  - Halt unauthorized Wi-Fi networks and manage user access to devices.
Other Cressida Security Solutions: Akonix

- Full and Comprehensive of Management of Public and Enterprise IM
  - Public IM - AOL, ICQ, IRC, MSN and Yahoo!
  - EIM – Lotus SameTime and Microsoft Live Communication Server (LCS)
- IM Logging and Report for other selected Enterprise IM solutions
  - Reuters Instant Messaging
  - Bloomberg Instant Message
  - Authenticates user/screen name
    - Integrates with Active Directory
  - Manages by single user, groups of users or everyone
  - Full Access Controls – Chinese Walls
  - File Transfer Controls
  - IM Feature Controls
  - Full or Selective Content Filtering
  - Anti-virus scanning (with 3rd party)
  - IM conversation logging and reporting
  - IM Content Archiving Integration (with 3rd party)
  - Compliance Reporter and protocol
  - Dynamic update for protocol changes
  - Auto install, no downtime
  - Offers full scalability
Other Cressida Security Solutions: ReQuest

- **Recovery**
  - Time Stamp Recovery
  - Detection of valid recovery points
  - Cross Queue Manager
  - Allows MQ data to be recovered in sync with DBMS data.
  - Recover deleted queues and purged data.
  - Forward Recovery
  - Individual Q’s or group of Q’s, possibly cross queue manager
  - Mass recovery in fail over situation.
  - Purged Queues

- **Reporting**
  - Granularity is MQ-call
  - Cross Queue Manager
  - By Q, By application, By Time-span
  - “Message Propagation”-report
  - MQPUT by appl A on RemoteQ in QMGR_A
  - Put on transmission Q for QMGR_intermediate
  - Put on transmission for QMGRB by QMGR_intermediate
  - Put on Q_Receiving in QMGRB by receiver.
  - MQGET from Q_Receiving
  - MQPUT of reply message (correlid!) by appl B on…
  - Filtering options
  - Raw data, in fixed documented format
  - To interface with other reporting tools
Other Cressida Security Solutions: RepliWeb

- Recovery
  - Fire and forget
    Recovers from networks failures or system crashes down to block level

- Data transfer
  - Integrity
  - Compression
  - Bandwidth control
    - Absolute
    - Relative
    - Time frames
  - Differential Transfer
    on large files only transfer the differences
Thank You

Interesting free downloads:

- NitroSecurity:
  - White papers on IPS (Intrusion Prevention System)
  - [http://www.cressida.info/whitepapers_page.htm#NitroGuard](http://www.cressida.info/whitepapers_page.htm#NitroGuard)

- Akonix RogueAware software:
  - *free monitoring tool that detects and reports on IM and P2P File Sharing use within corporate network*

- Ecora
  - Free software evaluation (Systems Configuration Audit & Patch Management)
  - [http://www.cressida.info/products_ecora_overview.htm](http://www.cressida.info/products_ecora_overview.htm)

Cressida, NitroSecurity Distributor for Europe,
In France: 03 20 38 06 46, Int’l HQ: +44 1483 23 93 00, [www.cressida.info](http://www.cressida.info)