Network Intelligence

Market-proven compliance and security solutions

NEbraskaCERT 2005:

Security Information and Event Management (SIEM)

Matt Stevens
Chief Technology Officer
Network Intelligence Corporation
8-10-05

Security Information/Events = Logs

- Logs are audit records generated by any software component running on your IT infrastructure
- Log records cover:
  - Normal activity
  - Error conditions
  - Configuration changes
  - Policy changes
  - User access to assets
  - Incident alerts
  - Unauthorized use of resources
  - Non-privileged access to files
  - User behavior patterns
  - Clearing of sensitive data
  - Access to audit trails
- Logs provide feedback on the status of IT resources and all activity going through them

Example Logs

- Sample Operating System Logs – Windows2K Server
  - 2005/05/17 12:59:12.387 EDT192.168.1.52%NICWIN-4-Security_529_Security: Security,91350077,Tue May 17 12:58:43 2005 , 529,Security,**NT AUTHORITY/SYSTEM,Failure Audit,WA1-MASTER-FDC,Logon/Logoff ,,Logon Failure: Reason: Unknown user name or bad password User Name: PIQA Domain: Ntoss Logon Type: 3** Logon Process: NtLmSsp Authentication Package: NTLM Workstation Name: UpTime-HA
  - 2005/05/17 12:59:29.793 EDT192.168.1.24%NICWIN-4-Security_560_Security: Security,69561800,Tue May 17 12:58:29 2005 , 560,Security,**NTOSS/ashtylla,Failure Audit,WA1-MAS90-DC,Object Access ,,Object Open: Object Server: SC Manager Object Type: SC_MANAGER OBJECT Object Name: ServicesActive** New Handle ID: - Operation ID: {0,261811266} Process ID: 784 **Primary User Name: C:\WINNT\system32\services.exe Primary Domain: WA1-MAS90-DC$ Primary Logon ID: NTOSS Client User Name: (0x0,0x3E7) Client Domain: ashtylla Client Logon ID: NTOSS** Accesses (0x0,0xF8EAAF4) Privileges READ_CONTROL Connect to service controller Enumerate services Query service database lock state

Traditional Interest in Event Logs

- Point security solutions provide log messages about critical network events
- Main focus on firewalls and IDS/IPS devices
- Correlation of events from multiple security points reduces false positives

Insider Threat Study

Paper: Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors

Published by: U.S Secret Service and CERT Coordination Center/SEI

Date: May 2005

From Section3 – Detecting the attack:

In general, 75% of the insiders were identified through manual procedures only, and 19% were identified using a combination of automated and manual procedures. The various mechanisms used to identify the perpetrators included

- **system logs** (70%)
- insider's own source IP address (33%)
- phone records (28%)
- username (24%)
- auditing procedures (13%)

In those cases in which **system logs** were used to identify the insider as the perpetrator, the following logs were used

- remote access logs (73%)
- file access logs (37%)
- system file change logs (37%)
- database/application logs (30%)
- email logs (13%)

But That Is Just The Beginning…

Event log data is the single most underutilized source of information within the organization.

Capacity Planning

- Compute Resources
- Network Bandwidth
  - LAN & WAN
- Disk space consumption
  - Servers
  - Clients

Performance & Uptime

- Where events happen
- When they occur
- Who is affected
- What sub-systems are involved
- Identify common elements

Legal & Human Resources

- Accurate, detailed audit trail
- Enforce acceptable use policies
  - A report sitting on your chair Monday AM is a powerful deterrent to further abuse…
- Provides supporting evidence
- Can link human assets to IT assets

Incident Investigation & Forensics

- A strong historical record is your best friend
- What seems benign today can turn out to be harmful tomorrow…
- Logs can quickly narrow down the search
- Similar incidents become easier to resolve

Help Limit Corporate Liability

- Determined abuse is hard to stop
- An effective policy that is actively monitored proves corporate responsibility
- It's hard to intimidate an event log…

Detect & Prevent I.P. Theft

- Makes spotting unusual patterns easier
- Proper resource access can be monitored
- An effective logging policy can serve as a strong deterrent to casual I.P. theft
- Supports efficient prosecution

Audit & Enforce Employee Productivity

- I.T. resources are expensive and budgets are tight
- Maintaining peak competitive stature is key to corporate entity survival
- 1% increase in information worker productivity can net nearly a 5% increase in corporate profits*

*Source: 2003 McKinsey report on global competition

Network Intelligence CORPORATION

Troubleshoot System and Network Problems

- The original reason for logging
  - Over 30% of the code in 1969 version of UNIX was dedicated to logging support*
- Can be extended to support internal application development
- Logs tell the story that other debugging techniques miss…

*Source: Ken Thompson and Dennis Ritchie, Bell Labs

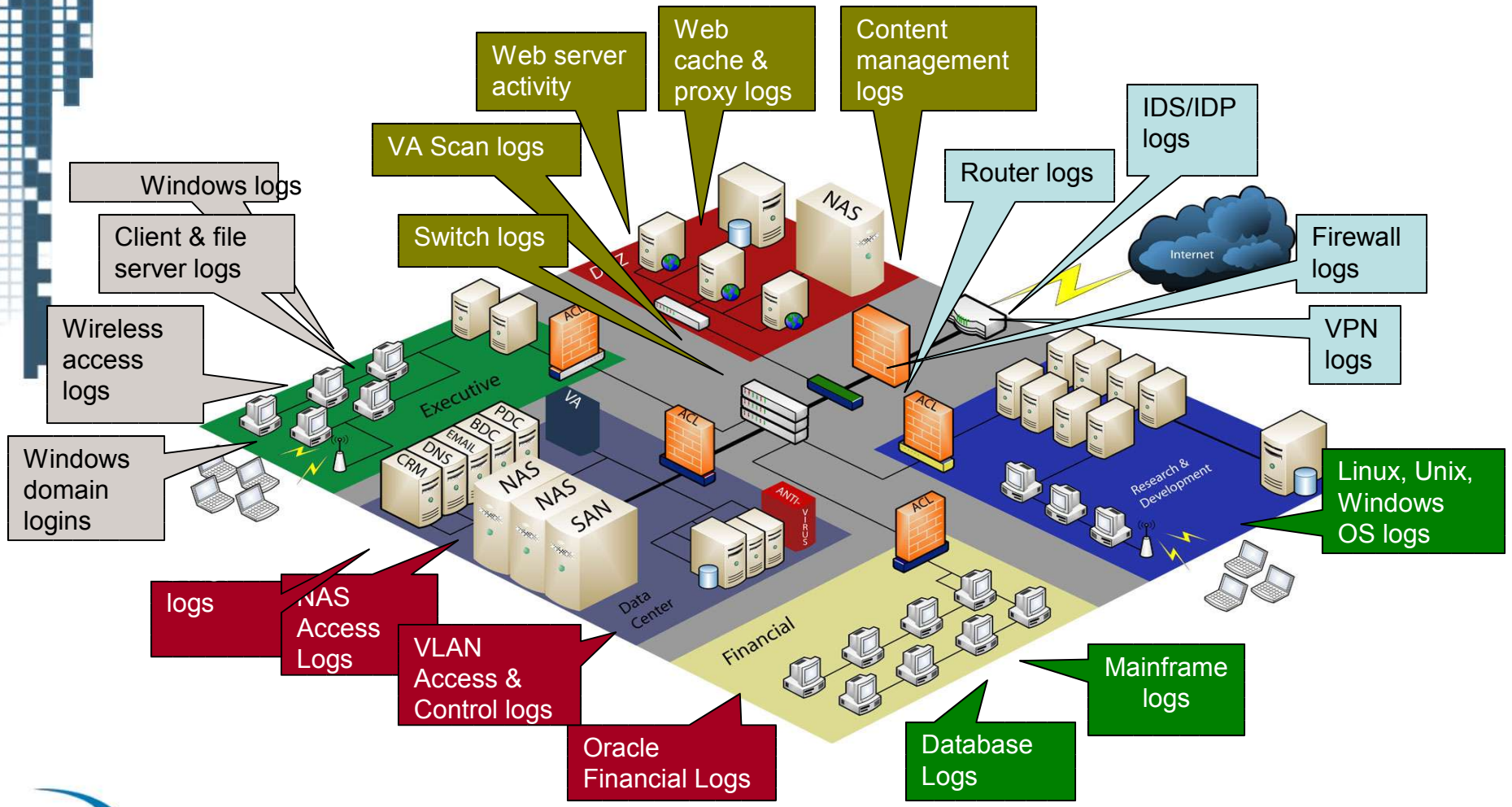
Support Compliance Regulations

- Applies to both Gov't and industry regs
- All regulations are based upon similar principles:
  - Establish controls
  - Monitor the controls
  - Report on the trends and monitoring efforts
- We all know today's list of regulations
  - An effective event log platform prepares you for tomorrow…

Audit & Enforce IT Security Policy

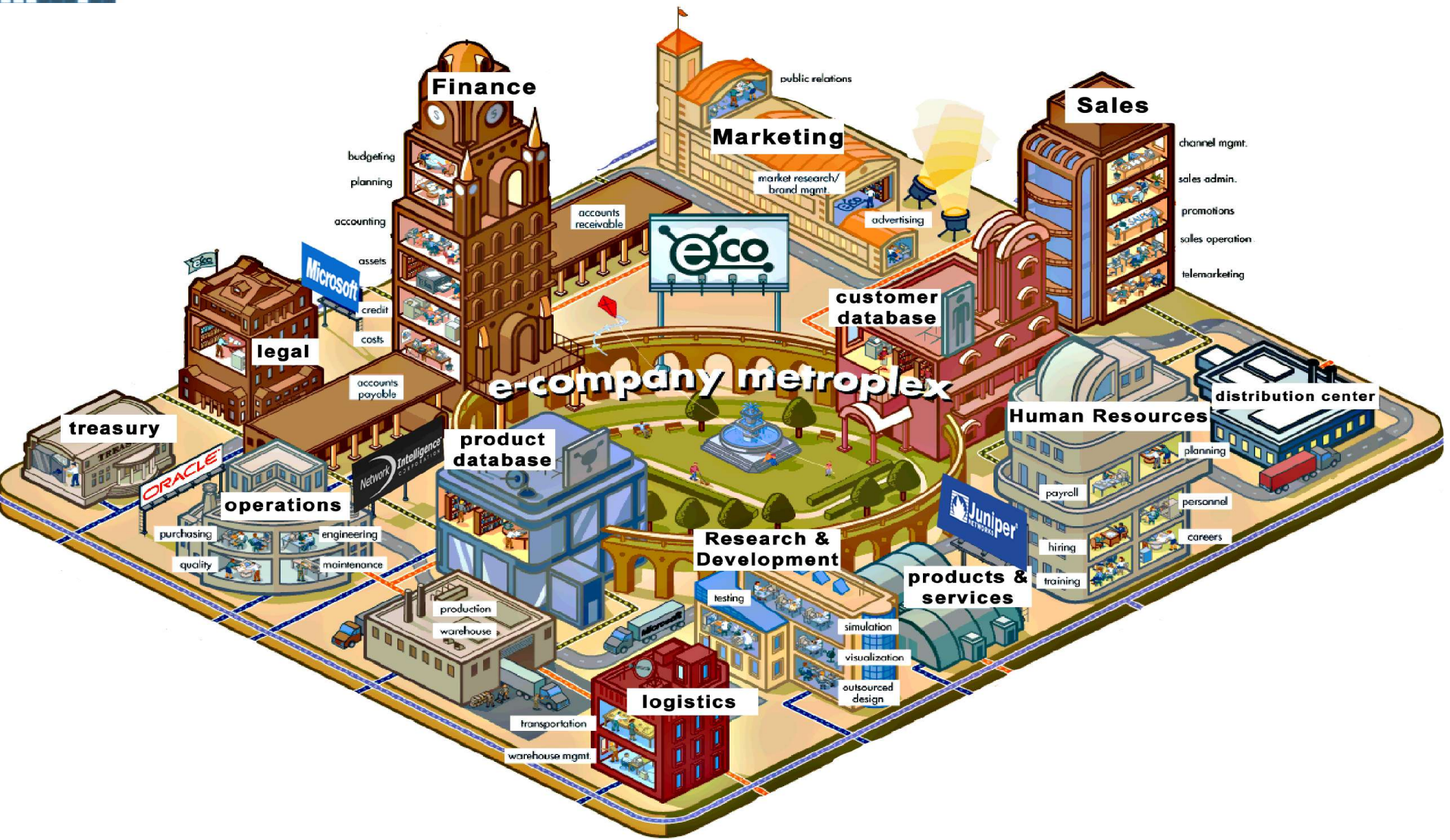
- Apply risk metrics to IT processes
- Finding breakdowns in IT security policy faster reduces IT risk
- Only effective way to validate point source security technologies

Event Log Data Creators…



Network Intelligence CORPORATION

Event Log Information Consumers…



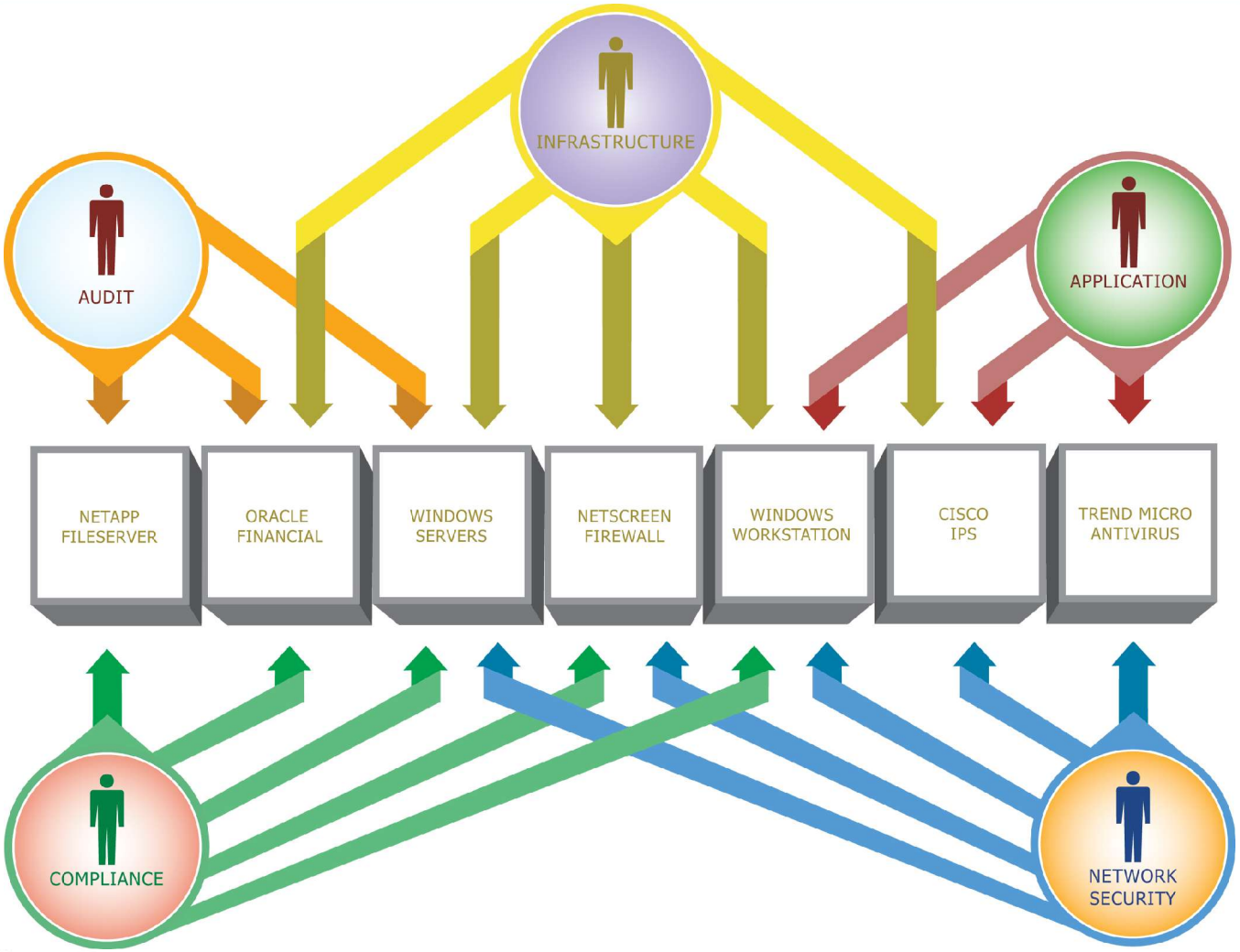
Event Log Information

Mapping Consumers to Use Cases

	Capacity Planning	*Perform. & Uptime*	*Legal/HR Action*	*Incidents Forensics*	*Corp. Liability*	*I.P. Theft*	*Employee Prod.*	*Trouble-Shooting*	*I.T. Security*	*Regulatory Compliance*
Customer Service		X	X			X	X			
Marketing			X			X	X			
Legal			X	X	X	X	X			
Sales			X		X	X	X			
Finance	X	X	X		X	X	X	X		X
Human Resources	X		X			X	X			X
Operations	X	X	X	X	X	X	X	X	X	X
Engineering		X	X			X	X			

Many Consumers & Use Cases …

Silos of Redundant Information Management



Network Intelligence™ CORPORATION

How to Avoid Silos?
Deploy an Enterprise-class SIEM Solution

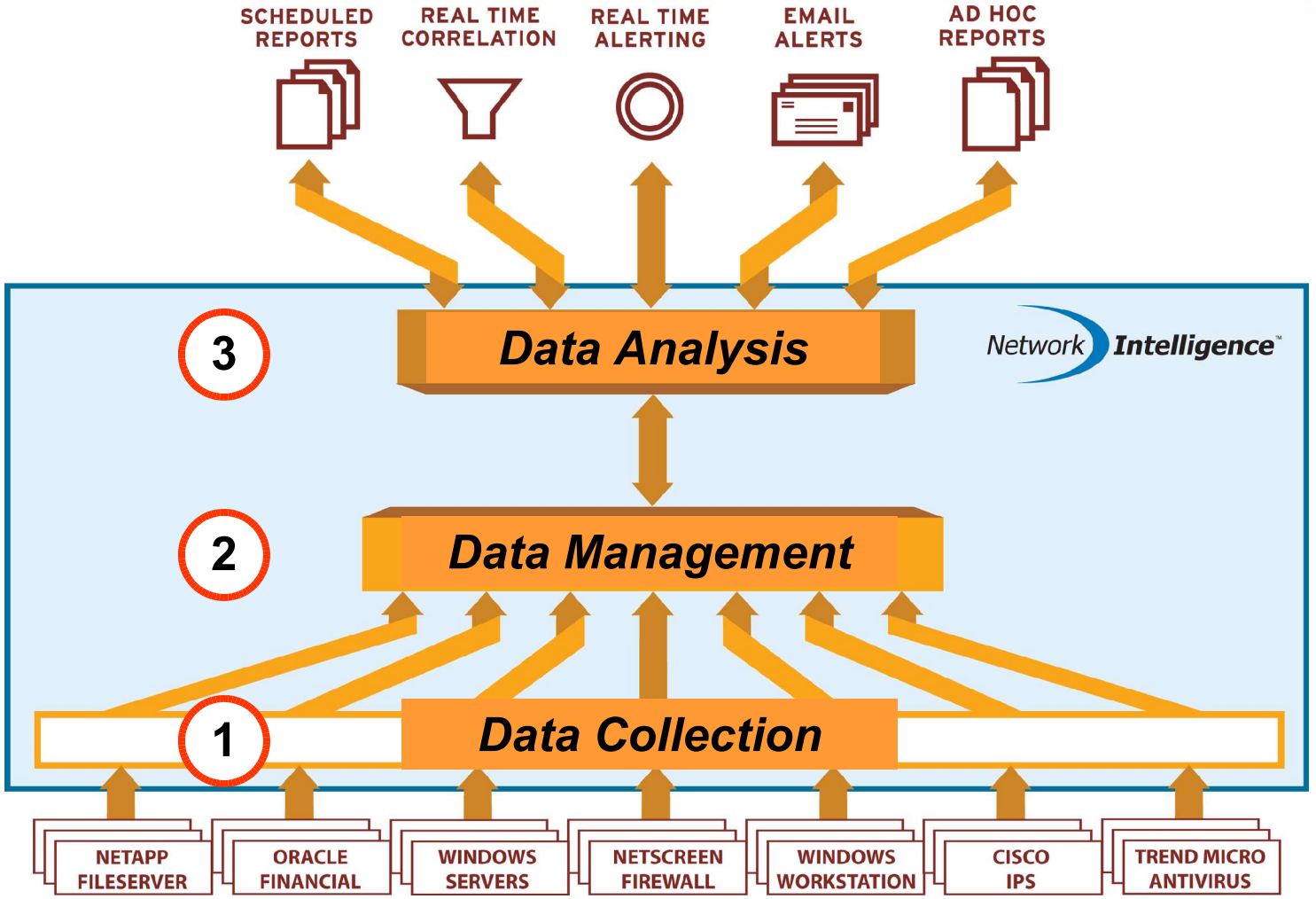
- **Collect "All the Data"….**
  - –Broad device support: network, security, infrastructure, & applications
  - –Agent-less, multi-protocol, non-normalized (no filtering) data capture
  - –100% raw data capture
  - –Deep source device coverage. Not a subset of events, all of the known events

- **…into a Scalable Enterprise Platform…**
  - –Modular growth to expand with business initiatives
  - –Price/performance for enterprise-class deployments
  - –Efficient storage and personnel utilization

- **…that Provides Powerful Analysis for Compliance Violations and Security Threats**
  - – Multiple views into the data
    - – Targeted reports for security, SOX, HIPAA, etc
    - – Correlation results between device types
    - – Baseline of workflows
  - – Detailed forensic analysis
  - – Guaranteed, real-time alert performance under load

Network Intelligence™ CORPORATION

Security Information and Event Management (SIEM)



Network Intelligence CORPORATION

Collection: Of Strategic Importance

It All Starts Here…

- Goal: Capture 100% of the Data
  - But still be able to make use of it
- Requirements:
  - Scalable system
    - Must be able to meet the accumulating collection rates
  - Wide device support
    - Analysis capabilities for many device types
  - No filtering or normalization of data
    - All data is important - normal activity included.
  - Robust data management tools
    - Raw data collection
    - High data compression rates
    - Encryption of stored data
    - Authentication of stored data
  - Agents vs. Agent-less

Collection: Implementing the Strategy

- Roll the device collection by types of devices or by departments
- Focus on the most critical assets first
- Turn on auditing features on your critical assets
- Leverage SIEM to transform the data into information that in turns drives knowledge

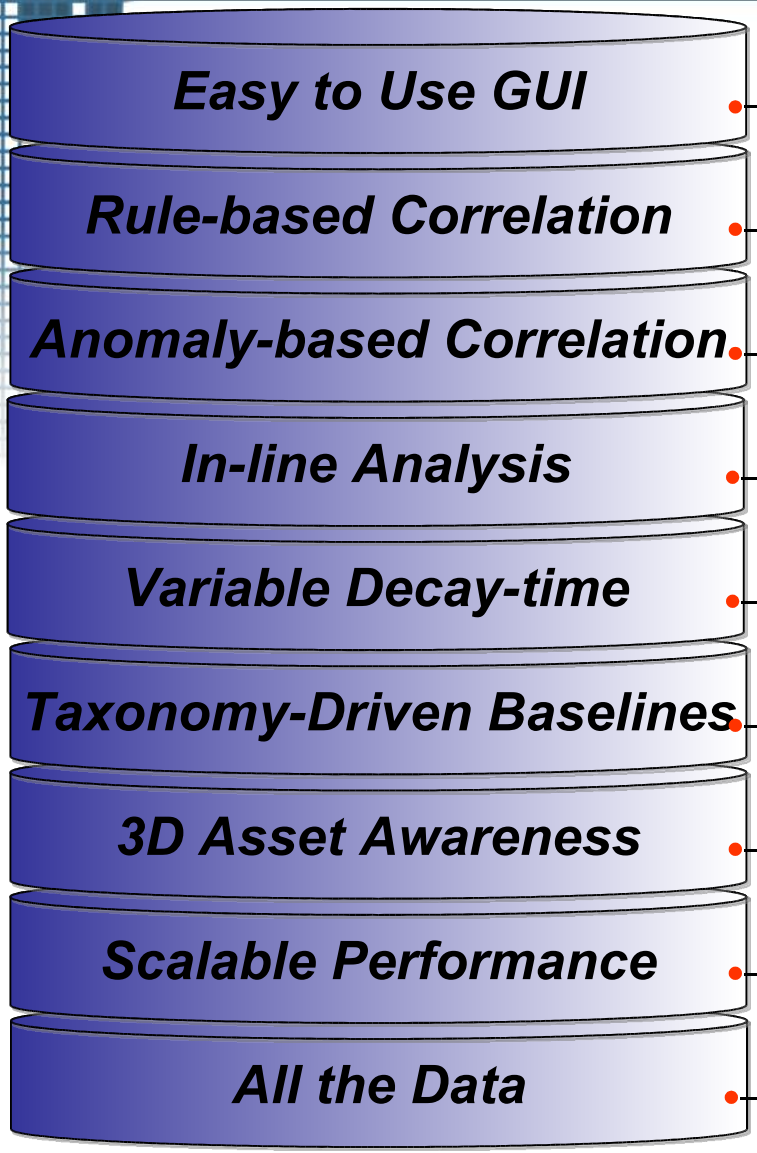
Collection: Source Device Protocols

- Syslog
- Syslog-NG
- SNMP
- Windows event logging API
- CheckPoint LEA
- FTP
- Formatted log files
  - comma/tab/space delimited, other
- ODBC connection to remote databases
- Push/pull XML files via HTTP
- Cisco IDS POP/RDEP/SDEE

Collection: Open Device Support

- Architecture should be open and permit in-field addition and updates of source device(s).
- Uses existing source device collection protocols
- Should not require changes to core product
- Treat devices as “added content” that can be distributed without interruption to production systems
- Automatically identify “unknown” events, yet still permit intelligent analysis later if required

Analysis: Real-time Correlation



- ***Delivers Efficient and Effective Security Operations. Correlation Logic can be Managed Online or Offline.***
- ***Advanced Boolean Logic Driven Correlation Enables Real-time Evaluation Against Corporate Policies***
- ***Detects and Alerts on Variations from Automatically Computed Baselines of both Events and Alerts.***
- ***REAL Real-Time Analysis with Consistent High Performance Alerting, Independent of Incoming EPS.***
- ***Permits Sophisticated Correlation Logic to Detect and Alert on Multi-Vector Fast Attack & Low and Slow***
- ***Auto Calculation of "Normal" for All Events, Devices and Alerts. 100% Mapped via Extensible Taxonomy***
- ***Intelligent Alert Ranking Via Automatic Gathering Of Asset Vulnerability, Value, & Type.***
- ***500-300K Sustained EPS from up to 30K Source Devices with 100% Data Capture Provides Best TCO***
- ***Accuracy Assured Regardless of Event Format Changes. Huge Device Breadth & Depth. No Agents.***

Analysis: Vulnerability Data

- VA tools provides a known list of hosts and detected vulnerabilities.
- Analysis can leverage this data to score threats based on asset vulnerabilities
- All rules evaluate vulnerability data of all the target assets. Higher vulnerability values of attacked assets escalate the severity level
- Customized rules should be able to evaluate individual assets or asset groups and alert when their vulnerabilities exceed a certain level

Analysis: Threat Scoring

- Alerts are grouped into alert categories
- All alert categories have (5) alert severity levels that default to US Homeland Security levels
- Internal scoring algorithm automatically computes alert severity levels based upon event contents, rates, baselines and asset values
- Incorporates asset attributes, including frequency of asset in event payload, importance and vulnerability
- Automatic ranking of all alerts contained in a view to focus security administrators on most critical incidents first

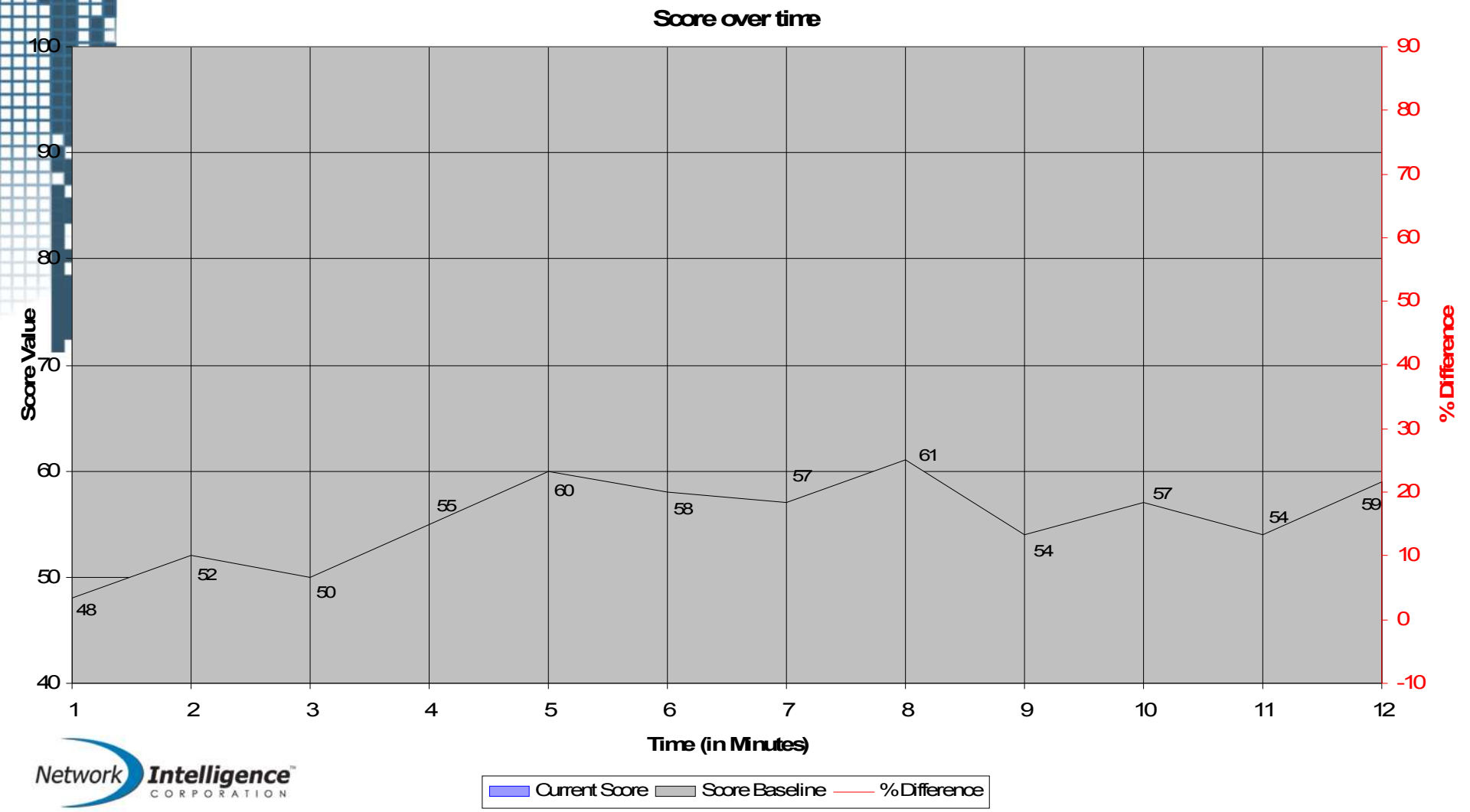
Analysis: Event Classification

- All events should be classified using a global taxonomy structure – thus providing a standard to the myriad of non-standard log events from all source device vendors
- Leveraging taxonomy to evaluate events by category, regardless of source device permits correlation to stay current and relevant far easier
- Event classification should be fully exposed to the user. Users should be able to create new categories and assign new messages to any level in the taxonomy tree

Analysis: Baseline Data

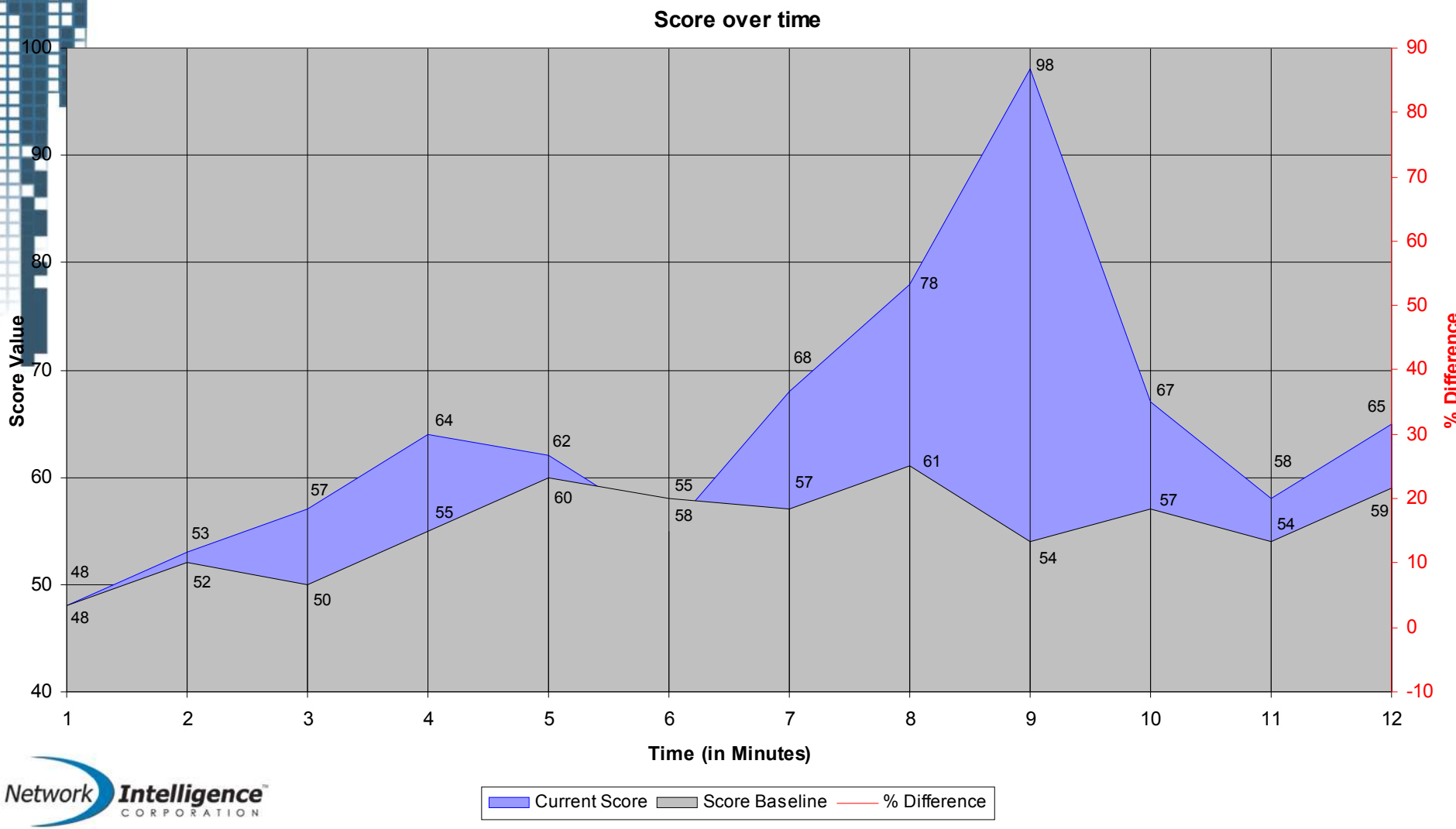
- Baselines should be created automatically – “learned” from the actual network activity
- Minute, hour, day and week baselines permit tracking of spikes as well as “low and slow” patterns
- Baselines are aware of normal activity pattern changes over the course of the day, week and month.
- Correlation engines can use baseline data to detect anomalies based on activity percent change from normal behavior

Analysis: Baselines



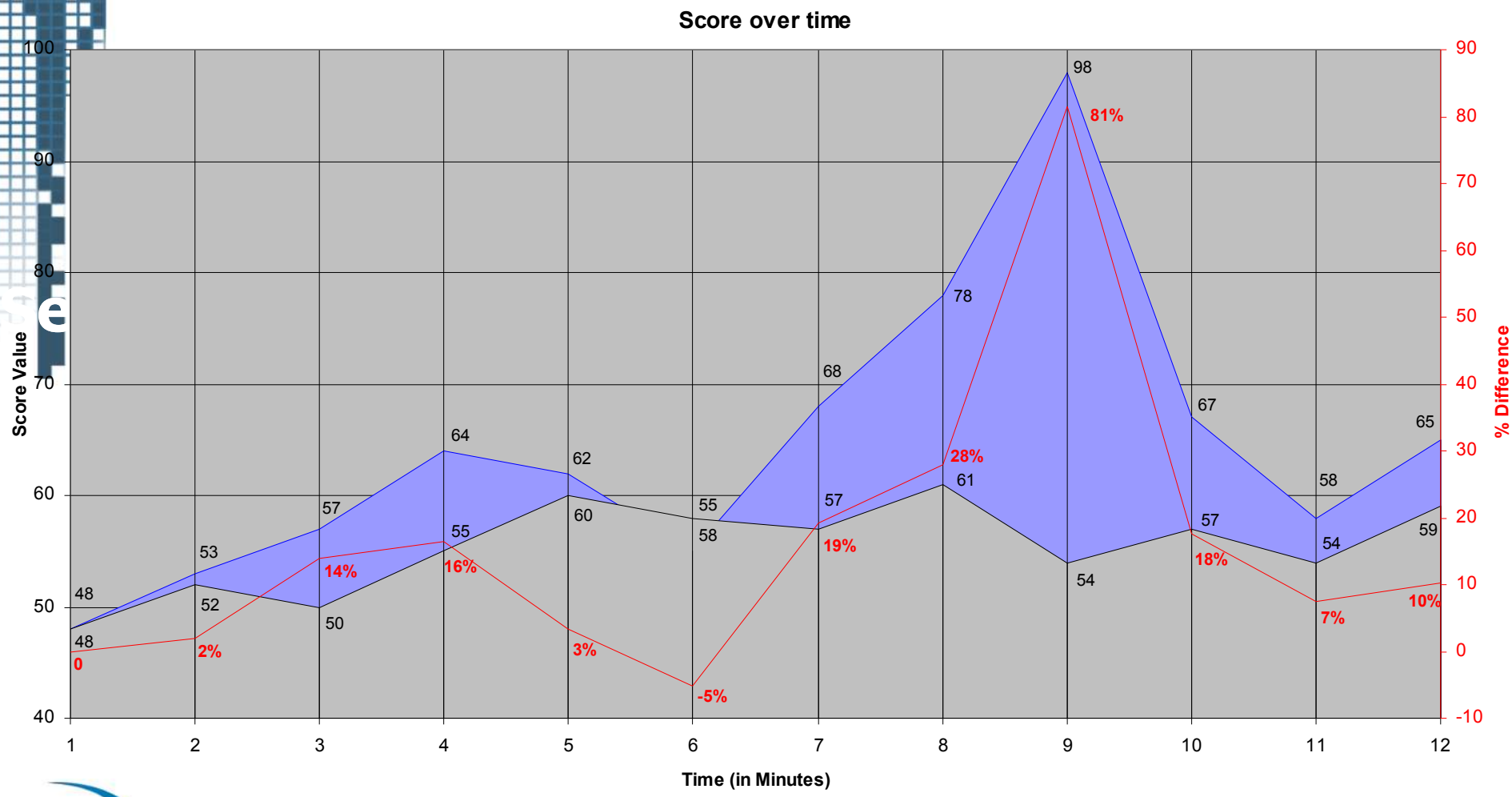
Network Intelligence CORPORATION

Analysis: Baselines



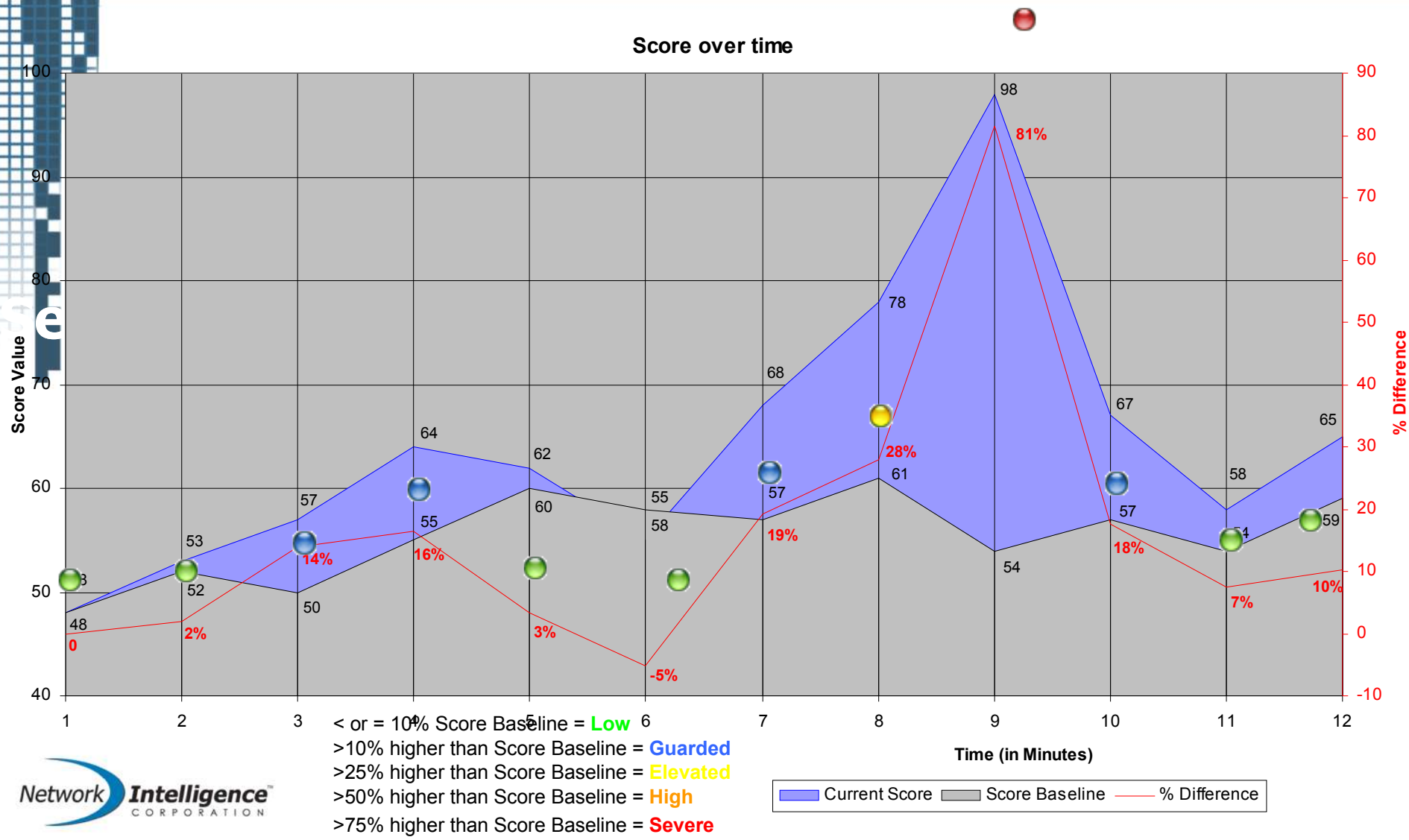
Network Intelligence CORPORATION

Analysis: Baselines



Network Intelligence CORPORATION

Analysis: Baselines



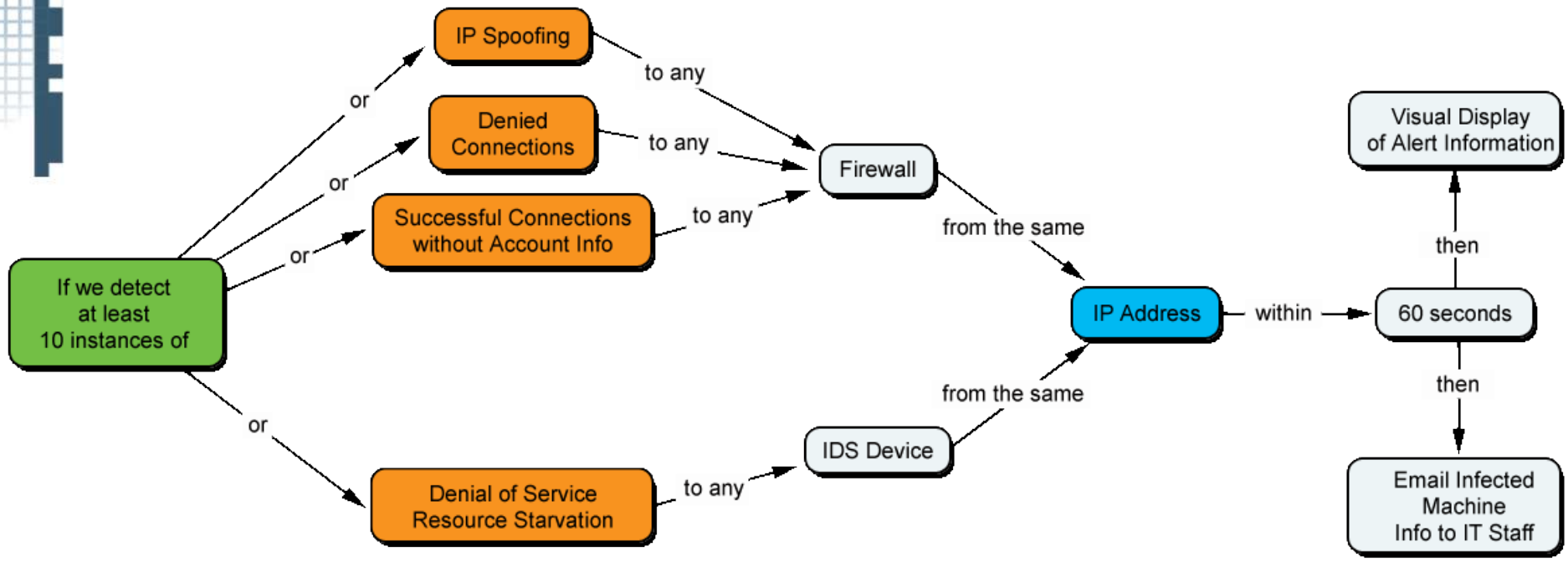
< or = 10% Score Baseline = Low
>10% higher than Score Baseline = Guarded
>25% higher than Score Baseline = Elevated
>50% higher than Score Baseline = High
>75% higher than Score Baseline = Severe

Network Intelligence CORPORATION

Analysis: Correlation Example – Worm Detection

Correlation Rule Name: W32.Blaster Worm

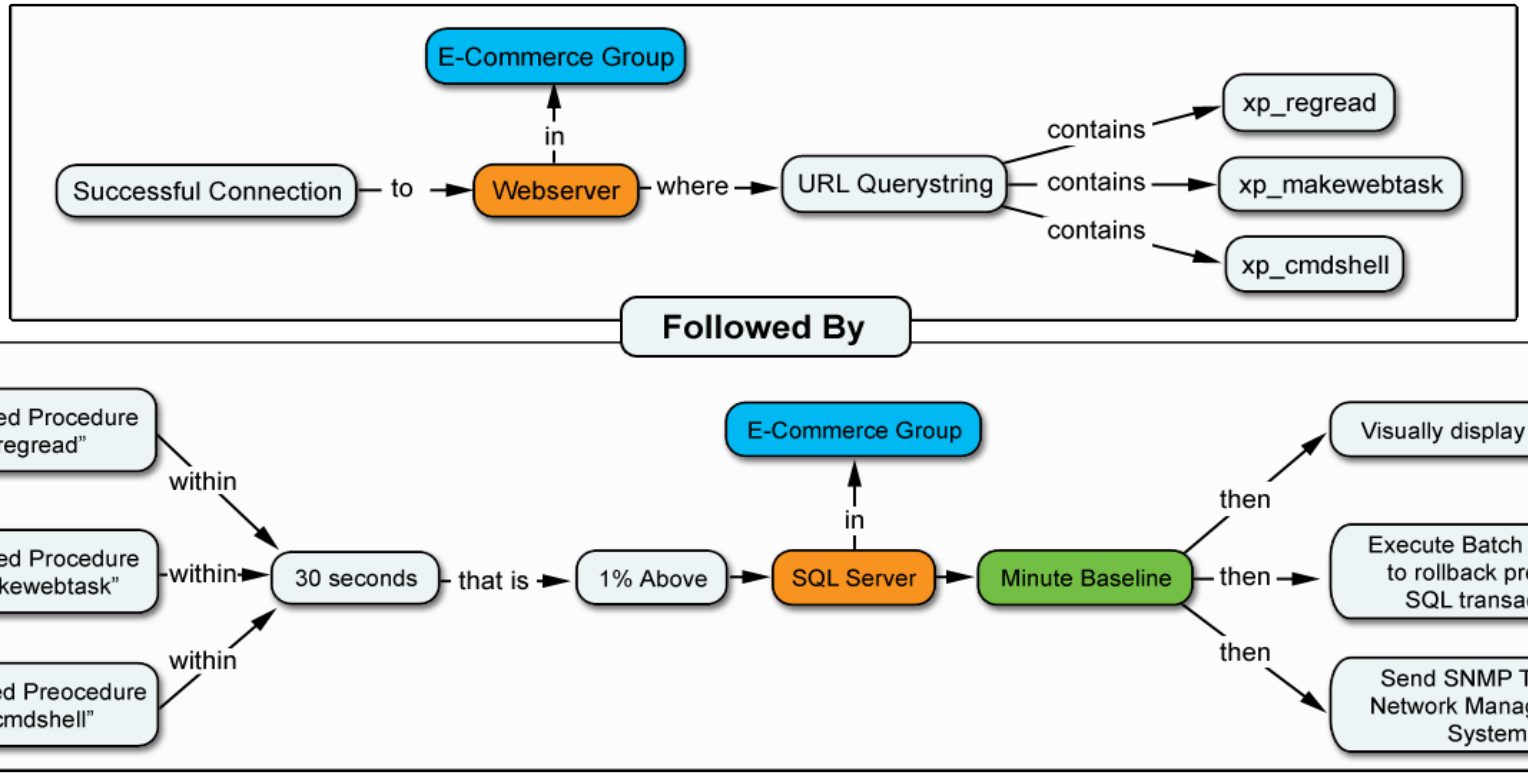
The goal of this rule is to detect Blaster worm variants as well as other malicious code by analyzing network traffic patterns.



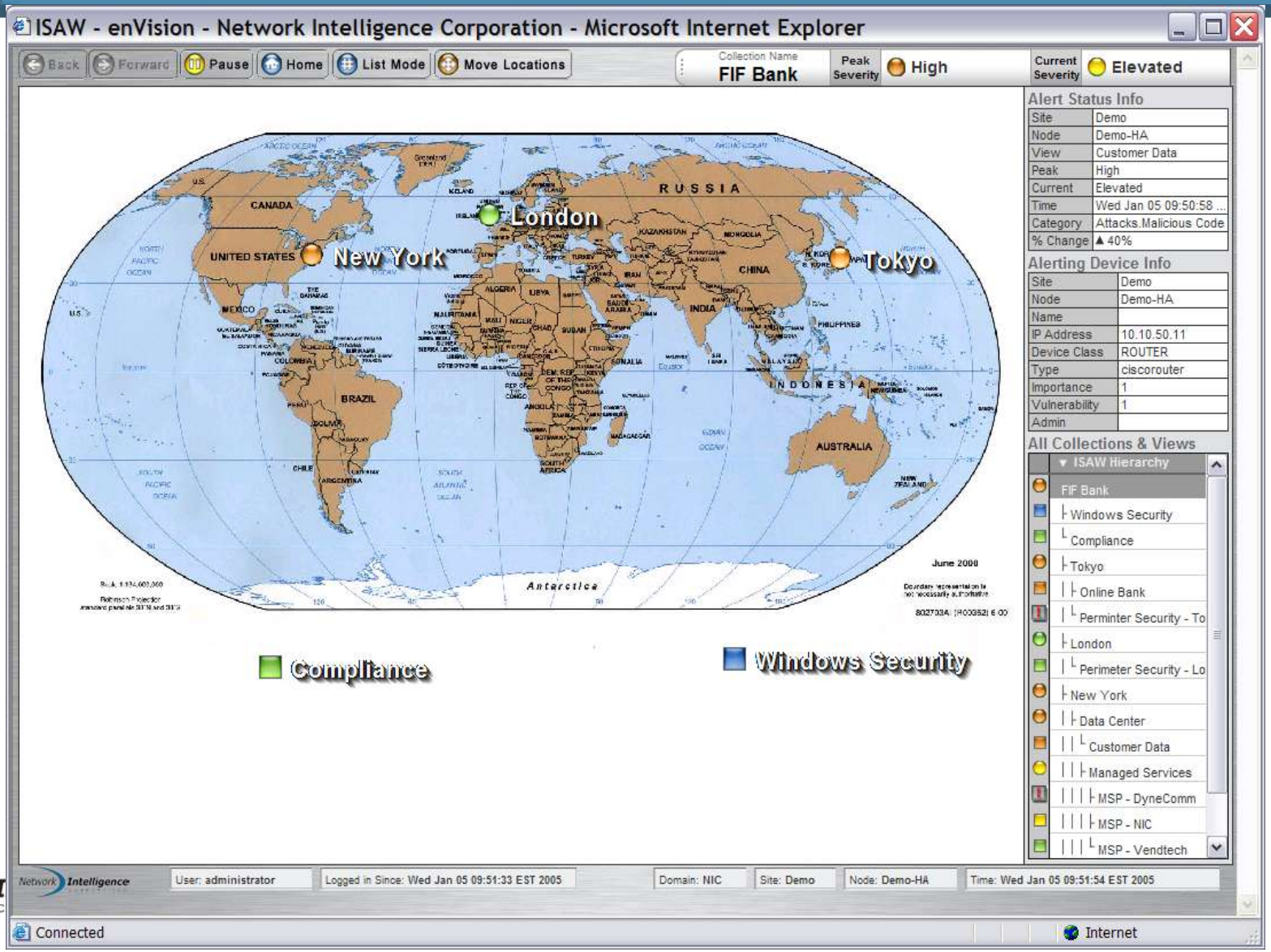
Analysis: Correlation Example – Website Attack

Correlation Rule Name: SQL Injection Attack

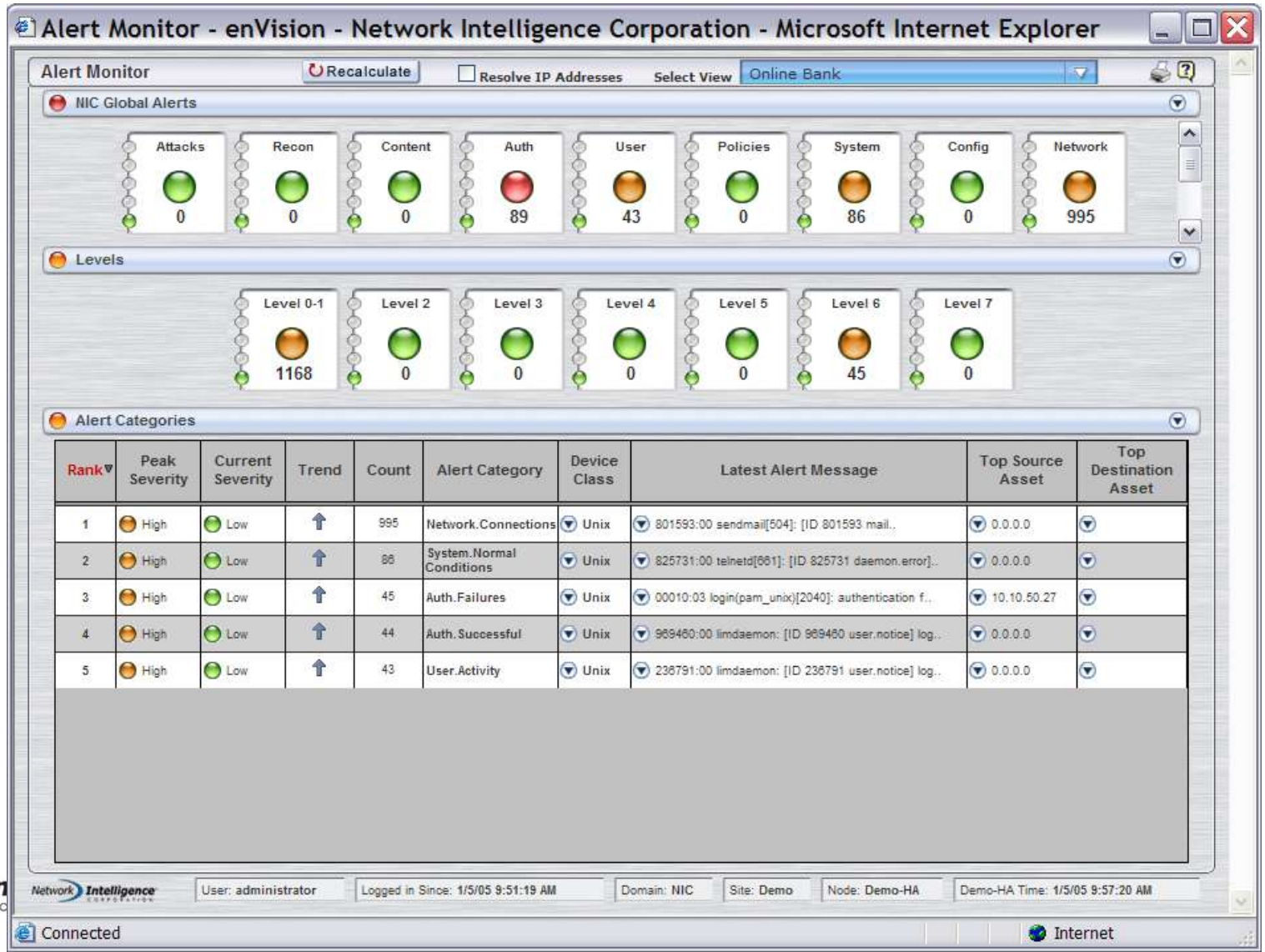
The goal of this rule is to detect information theft from E-Commerce websites through the exploitation of the trusted connection between the web server and the database.



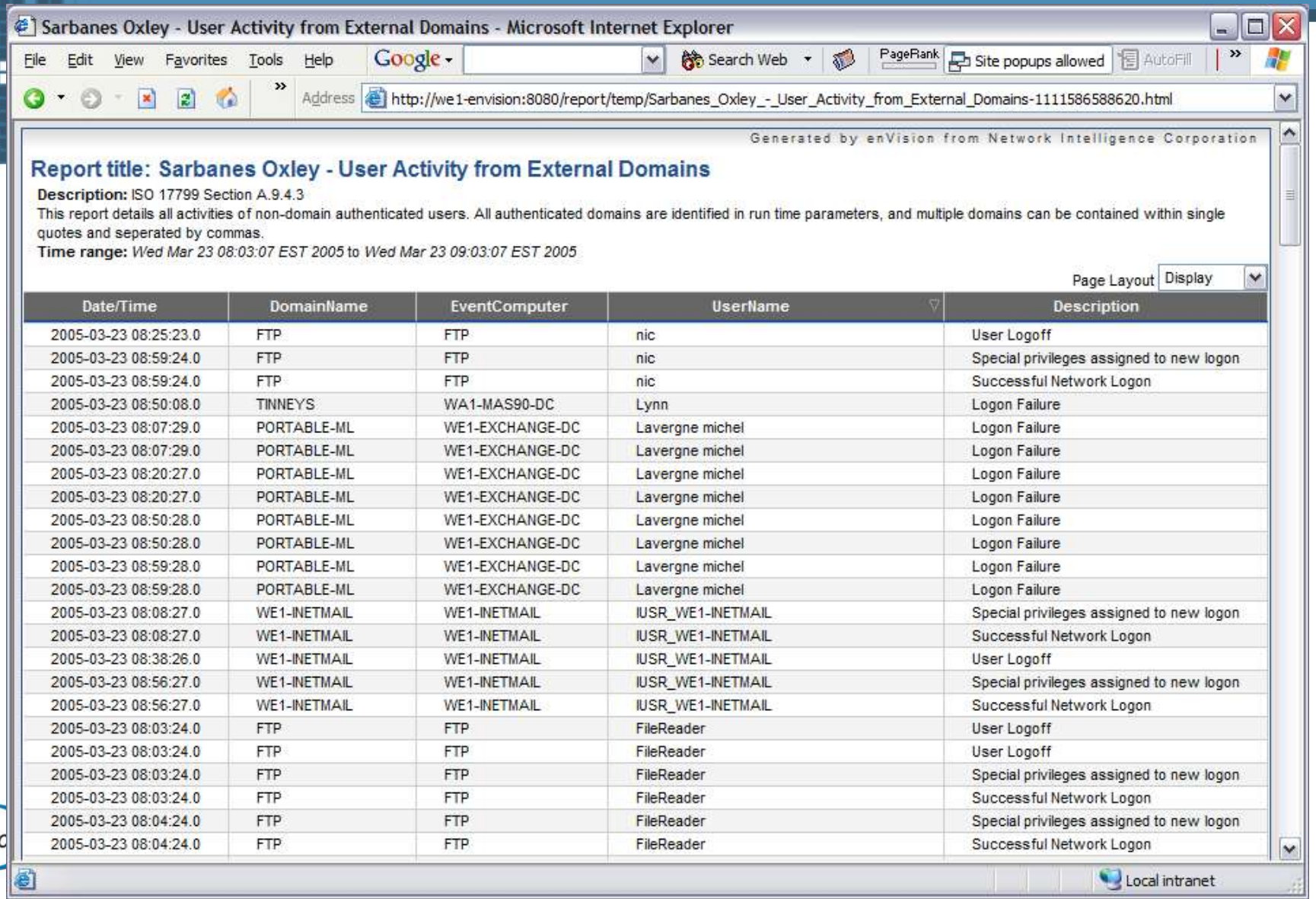
Analysis: Real-time Threat Analysis



Analysis: Real-time Threat Analysis

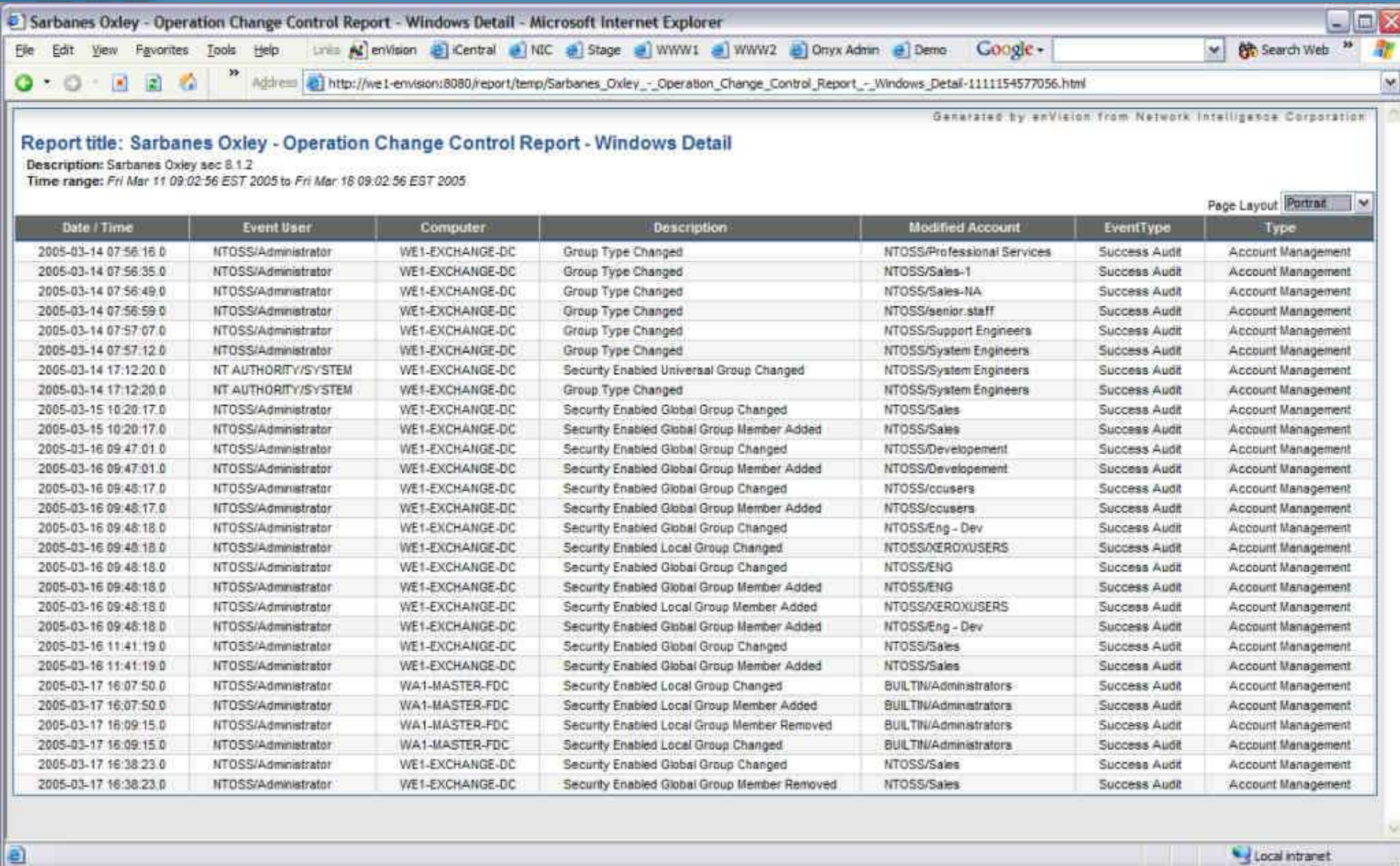


Analysis: Reporting
User Activity from External Domains



Date/Time	DomainName	EventComputer	UserName	Description
2005-03-23 08:25:23.0	FTP	FTP	nic	User Logoff
2005-03-23 08:59:24.0	FTP	FTP	nic	Special privileges assigned to new logon
2005-03-23 08:59:24.0	FTP	FTP	nic	Successful Network Logon
2005-03-23 08:50:08.0	TINNEYS	WA1-MAS90-DC	Lynn	Logon Failure
2005-03-23 08:07:29.0	PORTABLE-ML	WE1-EXCHANGE-DC	Lavergne michel	Logon Failure
2005-03-23 08:07:29.0	PORTABLE-ML	WE1-EXCHANGE-DC	Lavergne michel	Logon Failure
2005-03-23 08:20:27.0	PORTABLE-ML	WE1-EXCHANGE-DC	Lavergne michel	Logon Failure
2005-03-23 08:20:27.0	PORTABLE-ML	WE1-EXCHANGE-DC	Lavergne michel	Logon Failure
2005-03-23 08:50:28.0	PORTABLE-ML	WE1-EXCHANGE-DC	Lavergne michel	Logon Failure
2005-03-23 08:50:28.0	PORTABLE-ML	WE1-EXCHANGE-DC	Lavergne michel	Logon Failure
2005-03-23 08:59:28.0	PORTABLE-ML	WE1-EXCHANGE-DC	Lavergne michel	Logon Failure
2005-03-23 08:59:28.0	PORTABLE-ML	WE1-EXCHANGE-DC	Lavergne michel	Logon Failure
2005-03-23 08:08:27.0	WE1-INETMAIL	WE1-INETMAIL	IUSR_WE1-INETMAIL	Special privileges assigned to new logon
2005-03-23 08:08:27.0	WE1-INETMAIL	WE1-INETMAIL	IUSR_WE1-INETMAIL	Successful Network Logon
2005-03-23 08:38:26.0	WE1-INETMAIL	WE1-INETMAIL	IUSR_WE1-INETMAIL	User Logoff
2005-03-23 08:56:27.0	WE1-INETMAIL	WE1-INETMAIL	IUSR_WE1-INETMAIL	Special privileges assigned to new logon
2005-03-23 08:56:27.0	WE1-INETMAIL	WE1-INETMAIL	IUSR_WE1-INETMAIL	Successful Network Logon
2005-03-23 08:03:24.0	FTP	FTP	FileReader	User Logoff
2005-03-23 08:03:24.0	FTP	FTP	FileReader	User Logoff
2005-03-23 08:03:24.0	FTP	FTP	FileReader	Special privileges assigned to new logon
2005-03-23 08:03:24.0	FTP	FTP	FileReader	Successful Network Logon
2005-03-23 08:04:24.0	FTP	FTP	FileReader	Special privileges assigned to new logon
2005-03-23 08:04:24.0	FTP	FTP	FileReader	Successful Network Logon

Analysis: Reporting
Operational Change Control


Sarbanes Oxley - Operation Change Control Report - Windows Detail - Microsoft Internet Explorer

File Edit View Favorites Tools Help Links enVision iCentral NIC Stage WWW1 WWW2 Onyx Admin Demo Google Search Web

Address http://we1-envision:8080/report/temp/Sarbanes_Oxley_-_Operation_Change_Control_Report_-_Windows_Detail-1111154577056.html

Generated by enVision from Network Intelligence Corporation

Report title: Sarbanes Oxley - Operation Change Control Report - Windows Detail

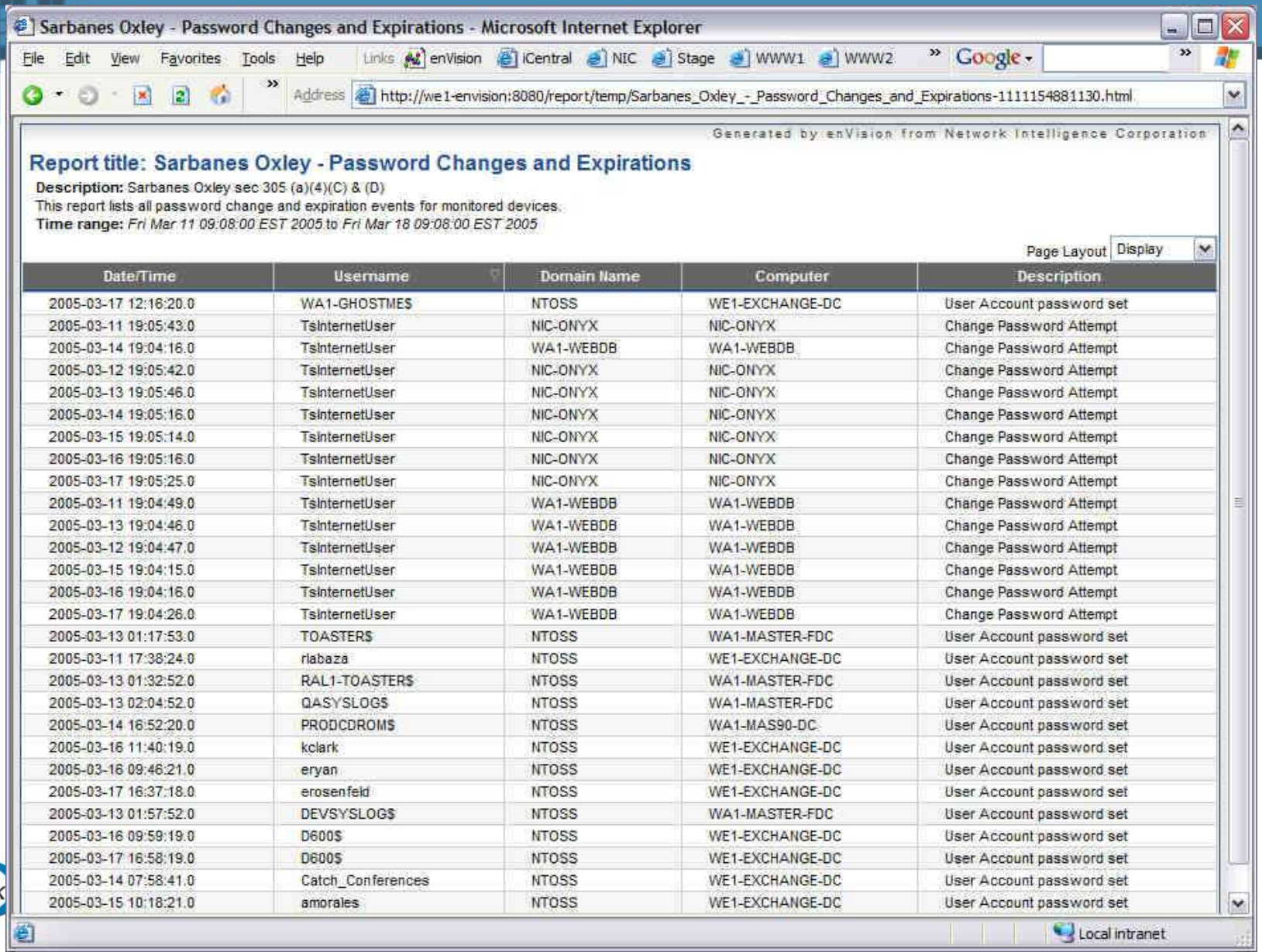
Description: Sarbanes Oxley sec 8.1.2
Time range: *Fri Mar 11 09:02:56 EST 2005* to *Fri Mar 18 09:02:56 EST 2005*

Page Layout Portrait

Date / Time	Event User	Computer	Description	Modified Account	EventType	Type
2005-03-14 07:56:16.0	NTOSS/Administrator	WE1-EXCHANGE-DC	Group Type Changed	NTOSS/Professional Services	Success Audit	Account Management
2005-03-14 07:56:35.0	NTOSS/Administrator	WE1-EXCHANGE-DC	Group Type Changed	NTOSS/Sales-1	Success Audit	Account Management
2005-03-14 07:56:49.0	NTOSS/Administrator	WE1-EXCHANGE-DC	Group Type Changed	NTOSS/Sales-NA	Success Audit	Account Management
2005-03-14 07:56:59.0	NTOSS/Administrator	WE1-EXCHANGE-DC	Group Type Changed	NTOSS/senior staff	Success Audit	Account Management
2005-03-14 07:57:07.0	NTOSS/Administrator	WE1-EXCHANGE-DC	Group Type Changed	NTOSS/Support Engineers	Success Audit	Account Management
2005-03-14 07:57:12.0	NTOSS/Administrator	WE1-EXCHANGE-DC	Group Type Changed	NTOSS/System Engineers	Success Audit	Account Management
2005-03-14 17:12:20.0	NT AUTHORITY/SYSTEM	WE1-EXCHANGE-DC	Security Enabled Universal Group Changed	NTOSS/System Engineers	Success Audit	Account Management
2005-03-14 17:12:20.0	NT AUTHORITY/SYSTEM	WE1-EXCHANGE-DC	Group Type Changed	NTOSS/System Engineers	Success Audit	Account Management
2005-03-15 10:20:17.0	NTOSS/Administrator	WE1-EXCHANGE-DC	Security Enabled Global Group Changed	NTOSS/Sales	Success Audit	Account Management
2005-03-15 10:20:17.0	NTOSS/Administrator	WE1-EXCHANGE-DC	Security Enabled Global Group Member Added	NTOSS/Sales	Success Audit	Account Management
2005-03-16 09:47:01.0	NTOSS/Administrator	WE1-EXCHANGE-DC	Security Enabled Global Group Changed	NTOSS/Developement	Success Audit	Account Management
2005-03-16 09:47:01.0	NTOSS/Administrator	WE1-EXCHANGE-DC	Security Enabled Global Group Member Added	NTOSS/Developement	Success Audit	Account Management
2005-03-16 09:48:17.0	NTOSS/Administrator	WE1-EXCHANGE-DC	Security Enabled Global Group Changed	NTOSS/ccusers	Success Audit	Account Management
2005-03-16 09:48:17.0	NTOSS/Administrator	WE1-EXCHANGE-DC	Security Enabled Global Group Member Added	NTOSS/ccusers	Success Audit	Account Management
2005-03-16 09:48:18.0	NTOSS/Administrator	WE1-EXCHANGE-DC	Security Enabled Global Group Changed	NTOSS/Eng - Dev	Success Audit	Account Management
2005-03-16 09:48:18.0	NTOSS/Administrator	WE1-EXCHANGE-DC	Security Enabled Local Group Changed	NTOSS/XEROXUSERS	Success Audit	Account Management
2005-03-16 09:48:18.0	NTOSS/Administrator	WE1-EXCHANGE-DC	Security Enabled Global Group Changed	NTOSS/ENG	Success Audit	Account Management
2005-03-16 09:48:18.0	NTOSS/Administrator	WE1-EXCHANGE-DC	Security Enabled Global Group Member Added	NTOSS/ENG	Success Audit	Account Management
2005-03-16 09:48:18.0	NTOSS/Administrator	WE1-EXCHANGE-DC	Security Enabled Local Group Member Added	NTOSS/XEROXUSERS	Success Audit	Account Management
2005-03-16 09:48:18.0	NTOSS/Administrator	WE1-EXCHANGE-DC	Security Enabled Global Group Member Added	NTOSS/Eng - Dev	Success Audit	Account Management
2005-03-16 11:41:19.0	NTOSS/Administrator	WE1-EXCHANGE-DC	Security Enabled Global Group Changed	NTOSS/Sales	Success Audit	Account Management
2005-03-16 11:41:19.0	NTOSS/Administrator	WE1-EXCHANGE-DC	Security Enabled Global Group Member Added	NTOSS/Sales	Success Audit	Account Management
2005-03-17 16:07:50.0	NTOSS/Administrator	WA1-MASTER-FDC	Security Enabled Local Group Changed	BUILTIN/Administrators	Success Audit	Account Management
2005-03-17 16:07:50.0	NTOSS/Administrator	WA1-MASTER-FDC	Security Enabled Local Group Member Added	BUILTIN/Administrators	Success Audit	Account Management
2005-03-17 16:09:15.0	NTOSS/Administrator	WA1-MASTER-FDC	Security Enabled Local Group Member Removed	BUILTIN/Administrators	Success Audit	Account Management
2005-03-17 16:09:15.0	NTOSS/Administrator	WA1-MASTER-FDC	Security Enabled Local Group Changed	BUILTIN/Administrators	Success Audit	Account Management
2005-03-17 16:38:23.0	NTOSS/Administrator	WE1-EXCHANGE-DC	Security Enabled Global Group Changed	NTOSS/Sales	Success Audit	Account Management
2005-03-17 16:38:23.0	NTOSS/Administrator	WE1-EXCHANGE-DC	Security Enabled Global Group Member Removed	NTOSS/Sales	Success Audit	Account Management

Local intranet

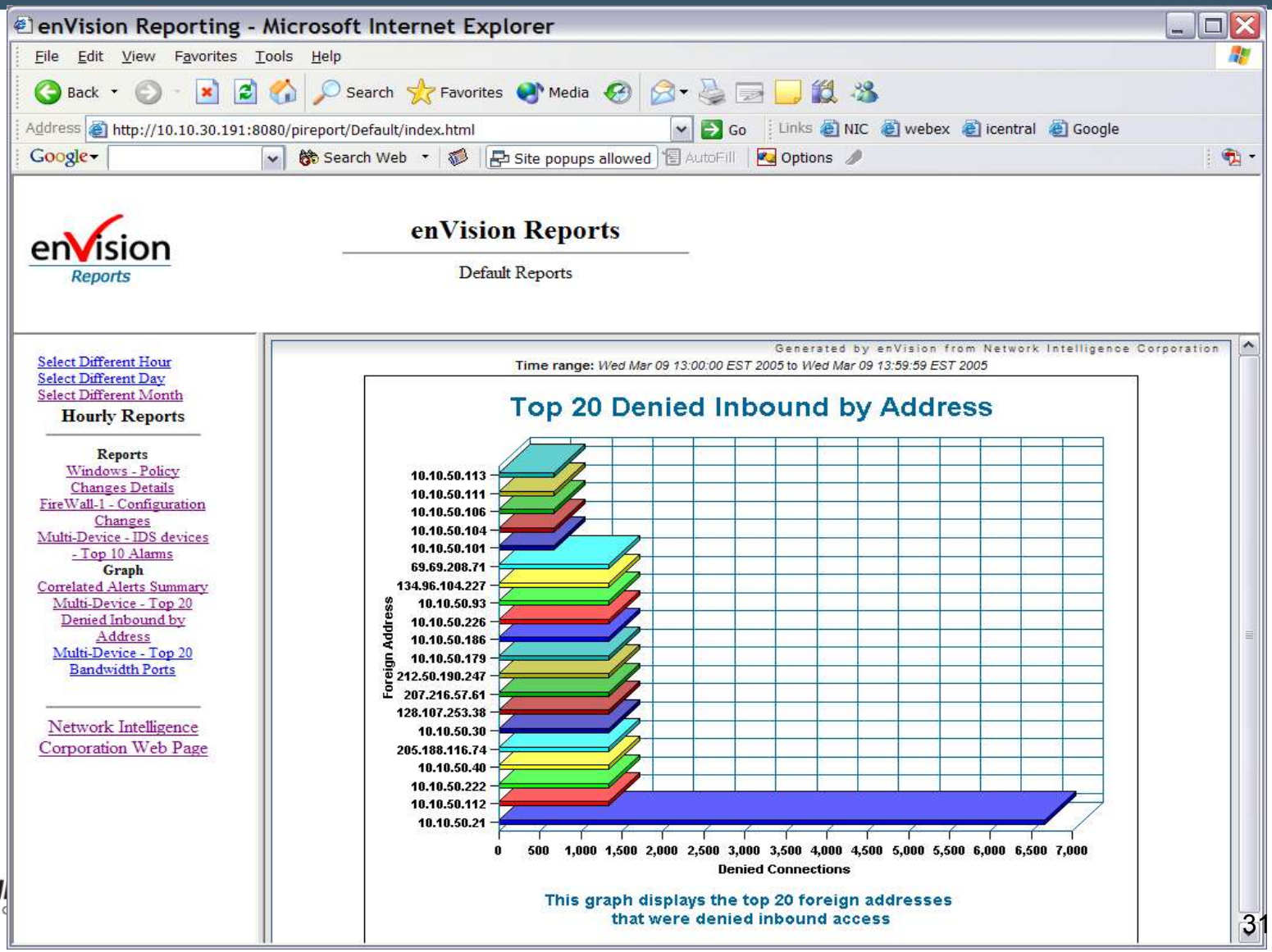
Analysis: Reporting
Password Changes and Expirations



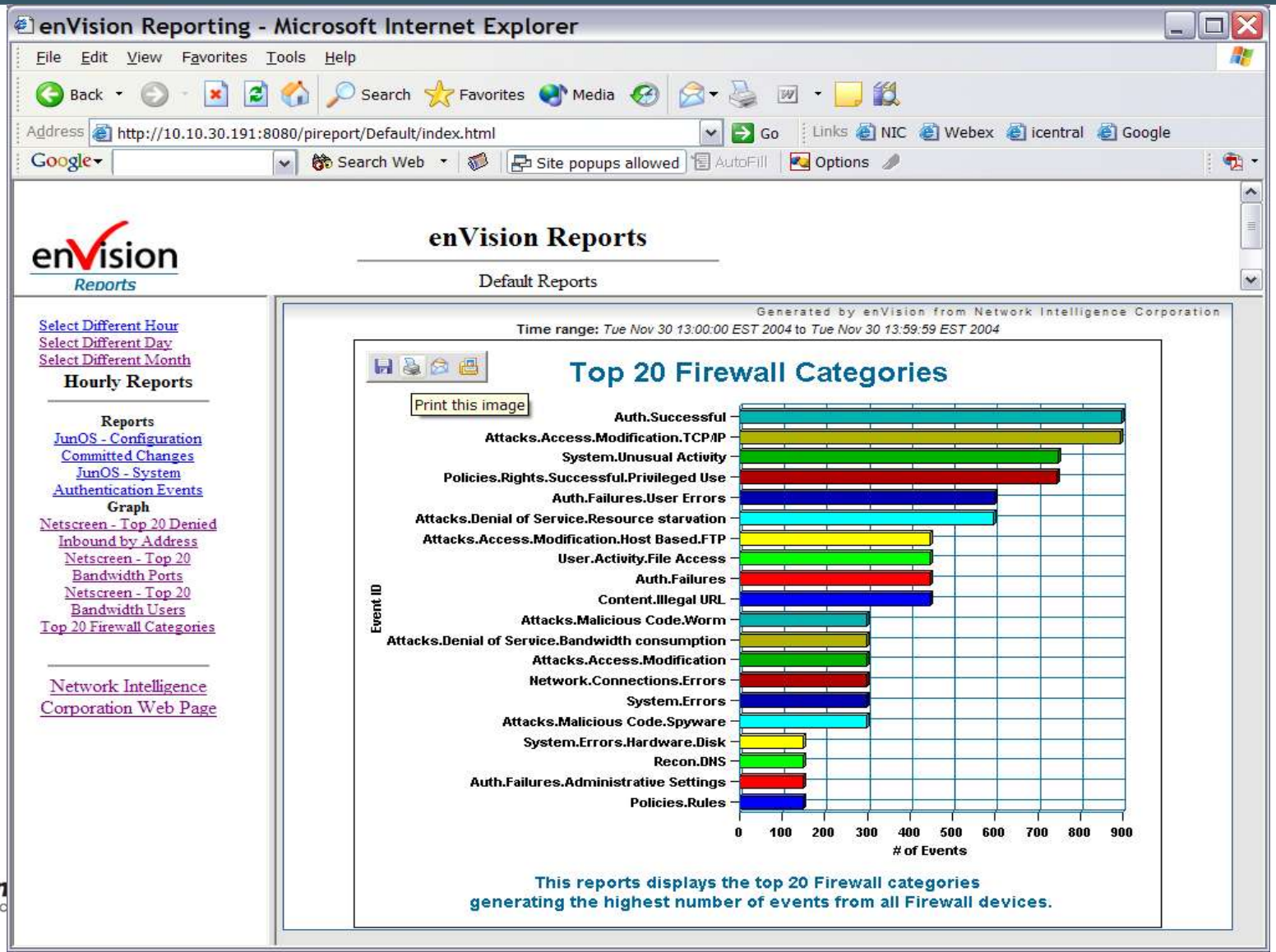
Date/Time	Username	Domain Name	Computer	Description
2005-03-17 12:16:20.0	WA1-GHOSTME$	NTOSS	WE1-EXCHANGE-DC	User Account password set
2005-03-11 19:05:43.0	TsInternetUser	NIC-ONYX	NIC-ONYX	Change Password Attempt
2005-03-14 19:04:16.0	TsInternetUser	WA1-WEBDB	WA1-WEBDB	Change Password Attempt
2005-03-12 19:05:42.0	TsInternetUser	NIC-ONYX	NIC-ONYX	Change Password Attempt
2005-03-13 19:05:46.0	TsInternetUser	NIC-ONYX	NIC-ONYX	Change Password Attempt
2005-03-14 19:05:16.0	TsInternetUser	NIC-ONYX	NIC-ONYX	Change Password Attempt
2005-03-15 19:05:14.0	TsInternetUser	NIC-ONYX	NIC-ONYX	Change Password Attempt
2005-03-16 19:05:16.0	TsInternetUser	NIC-ONYX	NIC-ONYX	Change Password Attempt
2005-03-17 19:05:25.0	TsInternetUser	NIC-ONYX	NIC-ONYX	Change Password Attempt
2005-03-11 19:04:49.0	TsInternetUser	WA1-WEBDB	WA1-WEBDB	Change Password Attempt
2005-03-13 19:04:46.0	TsInternetUser	WA1-WEBDB	WA1-WEBDB	Change Password Attempt
2005-03-12 19:04:47.0	TsInternetUser	WA1-WEBDB	WA1-WEBDB	Change Password Attempt
2005-03-15 19:04:15.0	TsInternetUser	WA1-WEBDB	WA1-WEBDB	Change Password Attempt
2005-03-16 19:04:16.0	TsInternetUser	WA1-WEBDB	WA1-WEBDB	Change Password Attempt
2005-03-17 19:04:26.0	TsInternetUser	WA1-WEBDB	WA1-WEBDB	Change Password Attempt
2005-03-13 01:17:53.0	TOASTER$	NTOSS	WA1-MASTER-FDC	User Account password set
2005-03-11 17:38:24.0	rlabaza	NTOSS	WE1-EXCHANGE-DC	User Account password set
2005-03-13 01:32:52.0	RAL1-TOASTER$	NTOSS	WA1-MASTER-FDC	User Account password set
2005-03-13 02:04:52.0	QASYSLOG$	NTOSS	WA1-MASTER-FDC	User Account password set
2005-03-14 16:52:20.0	PRODCDROM$	NTOSS	WA1-MAS90-DC	User Account password set
2005-03-16 11:40:19.0	kclark	NTOSS	WE1-EXCHANGE-DC	User Account password set
2005-03-16 09:46:21.0	eryan	NTOSS	WE1-EXCHANGE-DC	User Account password set
2005-03-17 16:37:18.0	erosenfeld	NTOSS	WE1-EXCHANGE-DC	User Account password set
2005-03-13 01:57:52.0	DEVSYSLOG$	NTOSS	WA1-MASTER-FDC	User Account password set
2005-03-16 09:59:19.0	D600$	NTOSS	WE1-EXCHANGE-DC	User Account password set
2005-03-17 16:58:19.0	D600$	NTOSS	WE1-EXCHANGE-DC	User Account password set
2005-03-14 07:58:41.0	Catch_Conferences	NTOSS	WE1-EXCHANGE-DC	User Account password set
2005-03-15 10:18:21.0	amorales	NTOSS	WE1-EXCHANGE-DC	User Account password set

Network

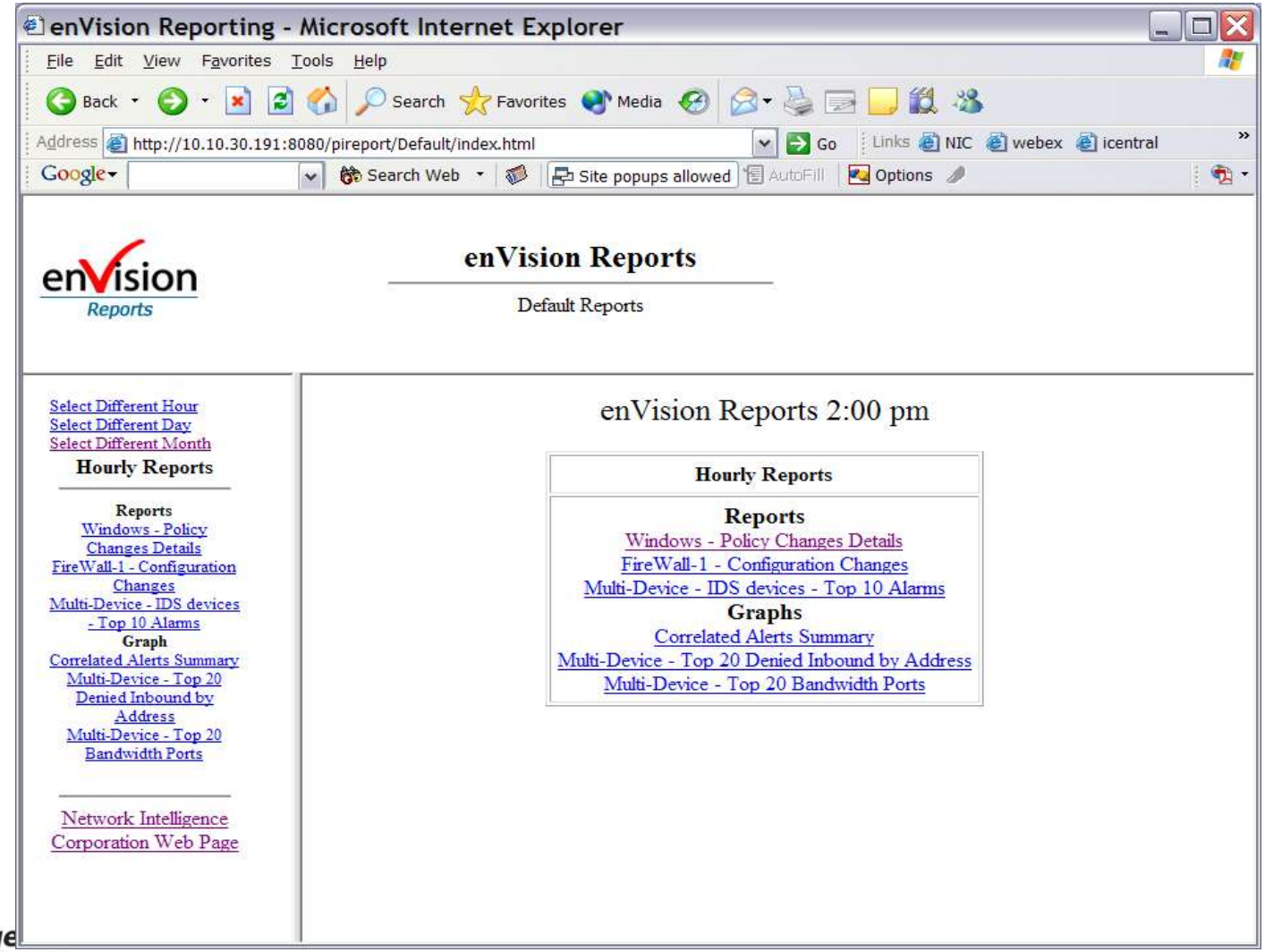
Analysis: Reporting
Top 20 Denied Inbound



Analysis: Reporting
Top 20 Firewall Categories (Taxonomy)

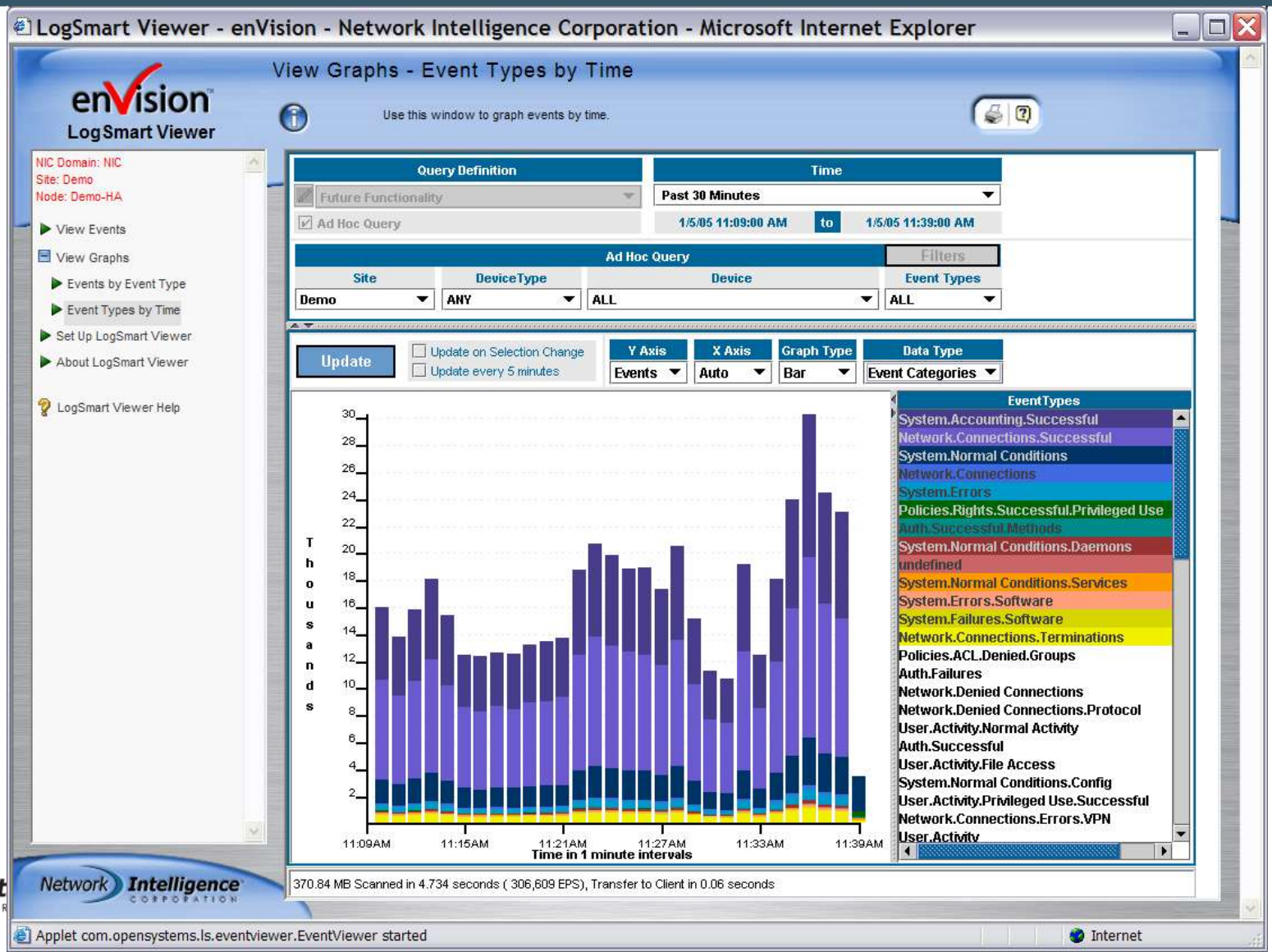


Analysis: Reporting
Scheduled Reports

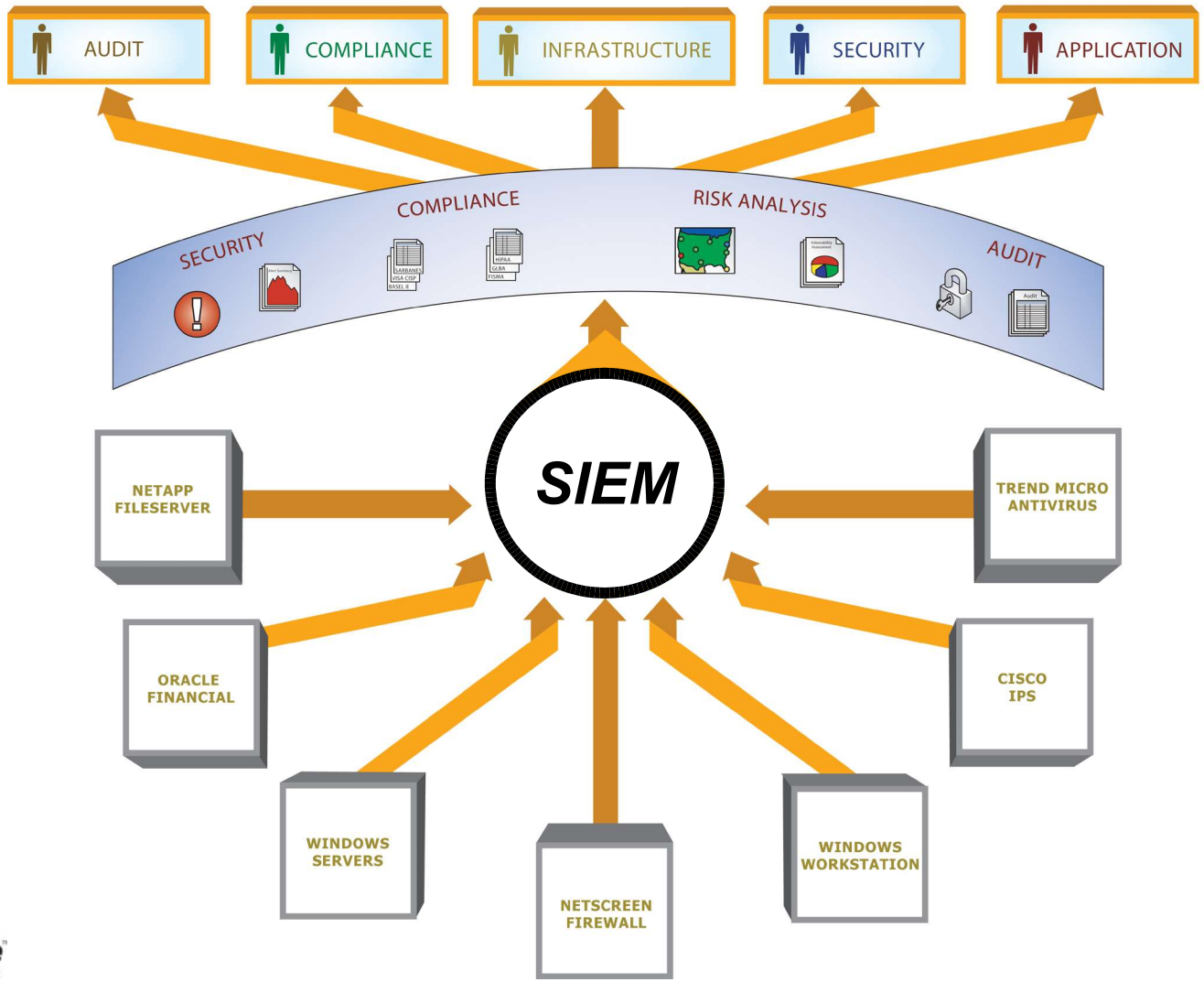


Analysis: Real-time Event Viewer

Data Mining in Real-time or Historically

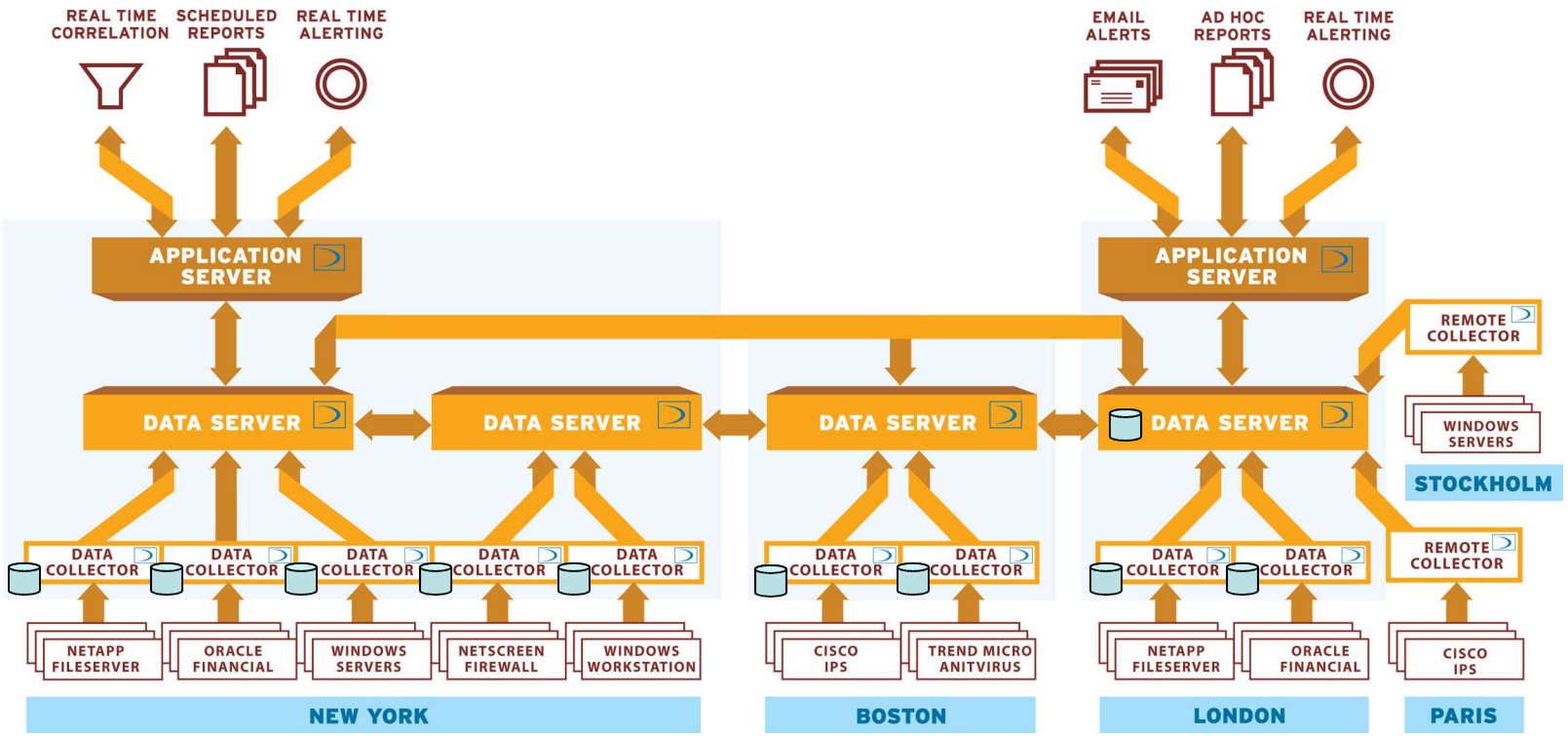


An Enterprise Platform for Compliance and Security



Network Intelligence CORPORATION

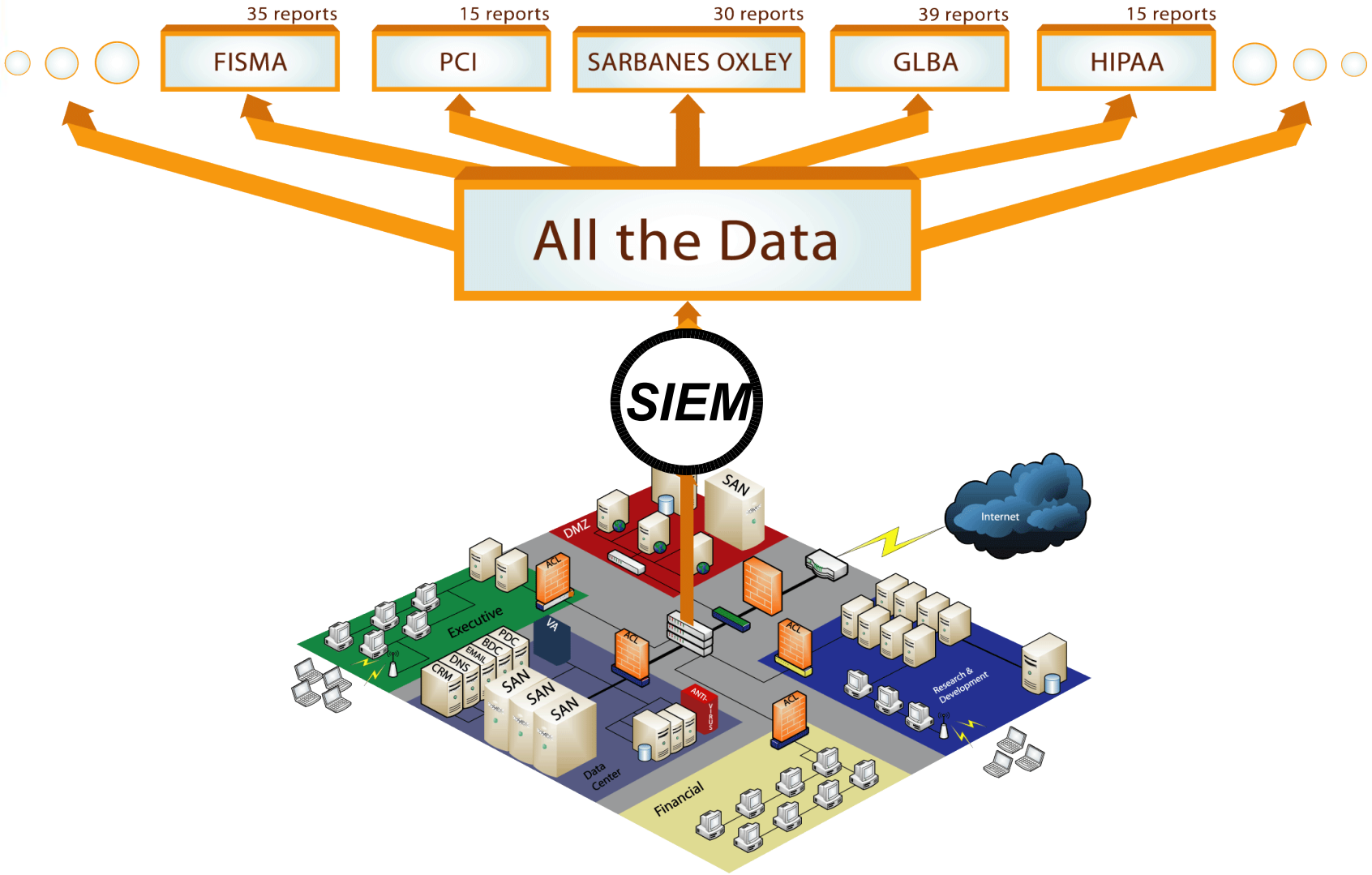
Example SIEM Architecture



- Patent-pending scaleable, distributed architecture for enterprises and global organizations.
- Local collection and storage of event data with true global analysis across multiple DBs.
- Leveraging local and remote collectors and a distributed DB, global organizations can collect and process over 300,000 EPS from up to 30,000 devices.
- Capture, analyze, and manage >26 Billion events per day per distributed DB.

Network Intelligence CORPORATION

ISO 17799: A Content Framework for IT Compliance



Best Practices

- Don't Try to filter the logs at the source
  - Predicting what is useful or not is like playing Russian Roulette
  - It's much easier to purge information you don't need vs. never having it
  - Good event logging systems will capture 100% and let you purge later
- Determine Reporting Time Periods
  - 1 week, 1 month, 90 days - more?
  - Reporting Periods will drive event data retention policies.
  - Plan to store data at least 2 complete reporting intervals
  - If you purge old data – be sure you have proper archives…
- Archive Key Logs to Long Life Media
  - CD-ROM, DVD-RW, etc
- Use a centralized, standard time source
  - When event logs are "time aligned" life is much easier
- Be cautious of sensitive event log content
  - Many logs are sent "in the clear" – leverage a VPN for WANs
  - Be sure that centralized logging facility is "secure"

Best Practices

- Don't Alert on Everything – Take it Slow
  - Prioritize on what You REALLY want to be alerted on
- Leverage Correlation to Weed Out False Positives
  - Rules-based correlation techniques can reduce the chatter
  - Correlated reporting will let get a more "holistic view" of the network
- Test Your Logging Facility
  - Are you REALLY capturing all the logs? REALLY?
- Encourage Your Teams to Analyze the Data
  - Determine your "standard" reports – develop baselines – look for exceptions
- If You Didn't Log It, Then It Never Happened