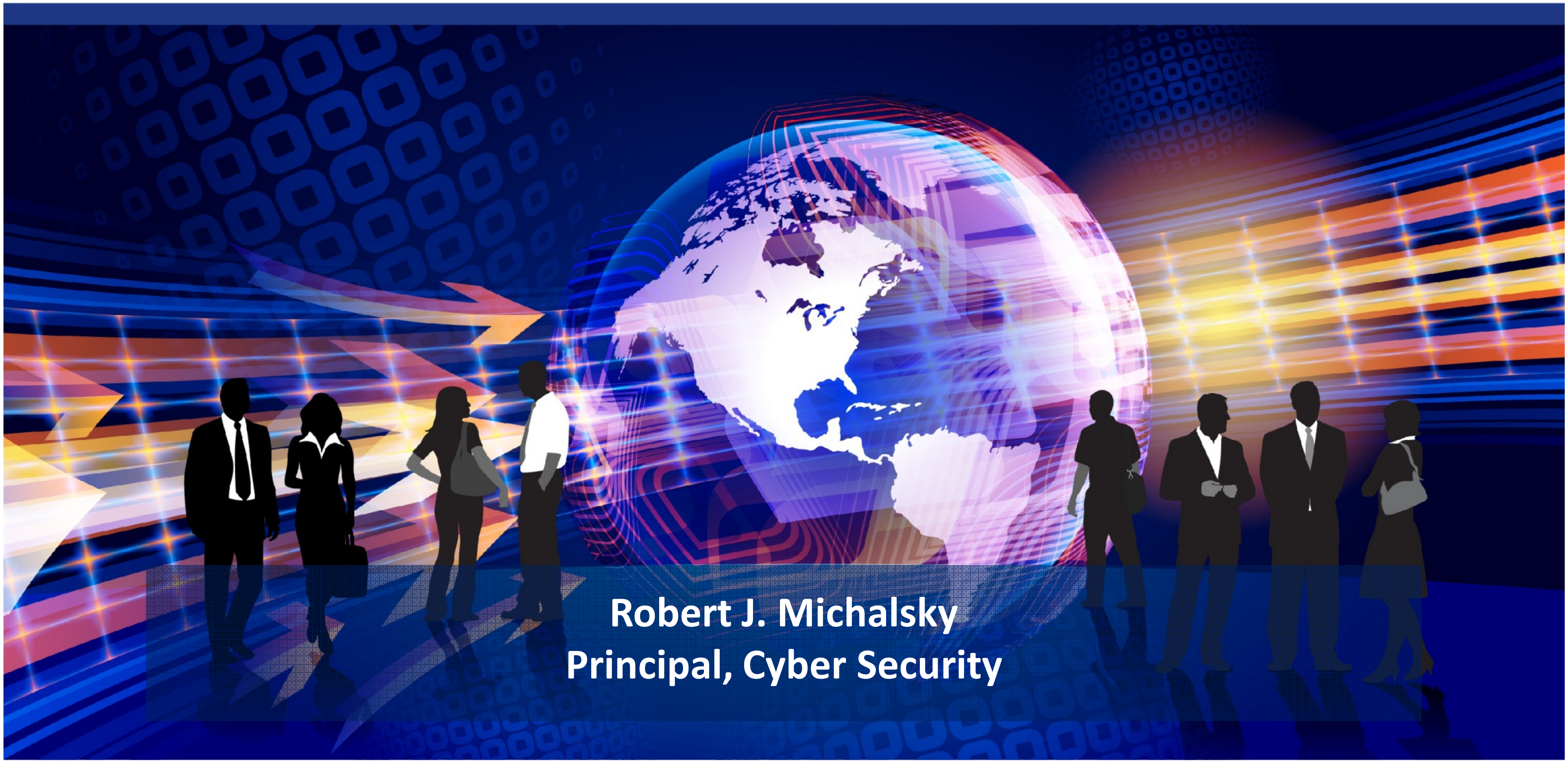
NJVC
Driven by Your Mission®

Cyber Security Metrics

Dashboards & Analytics

Feb, 2014



Robert J. Michalsky
Principal, Cyber Security

Agenda

- Healthcare Sector Threats
- Recent History
- Security Metrics
- Cyber Dashboards
  - Components
  - Visualization
- Analytics
  - Risk Management
  - Breach detection

Healthcare Sector Threats

- Exploits – Wide Attack Profile
  - Personal Health Information (PHI) breaches
  - Medical Identity theft
  - Medical device intrusions
  - Insurance / Medicare / Medicaid fraud
  - Supply Chain corruption
  - Third party payment processor breaches
  - Supplier networks / Insurance vendors
  - Corruption of health records
  - Insurance / Medicare / Medicaid fraud
  - Public network access to records
  - Web application break ins
  - Account Takeovers

- Attack Methods – Varied and evolving
  - Social Engineering
  - Wireless Interception (Bluetooth)
  - Spear phishing, e-mail spoofing
  - Mobile device exploitation (BYOD)
  - Links to infected websites
  - Malware – keyloggers, trojans, worms, data sniffers etc.
  - Spyware, Ransomware (CryptoLocker)
  - Insider threat
  - Man-in-the-middle attacks
  - Zero Day Exploits
  - Distributed Denial of Service (DDoS)
  - Rainbow tables

Adversaries are always looking for "the weakest link"

Recent History

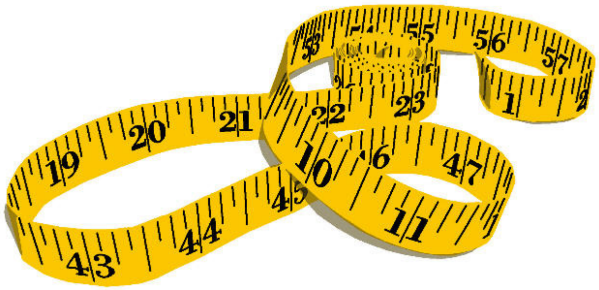
- 32,500 patients of Cottage Health System in CA had personal and health information exposed on Google for 14 months (Oct 2012 – Dec 2013) – because of Business Associate lapse in server protection
  - Discovered via a voice mail message
- Hackers break into FDA servers used to submit proprietary and confidential information – Oct 2013
  - Potential exposure: Drug manufacturing data, clinical trial data for 14,000 accounts
- Boston Convention Center Nov 2013
  - American Public Health Association
  - America Society of Human Genetics
    - Credit card info stolen for over 21,000 attendees
    - No data breach source identified

Goal of using security metrics?

1. Quantify data to facilitate insight
   - People, process, technology
2. Mitigate existing vulnerabilities
   - Unforeseen flaws in IT infrastructure or application software that can be exploited
   - Evade security controls

Classes of Vulnerabilities (2013 Defense Science Board Report)

- ❖ Tier 1: Known vulnerabilities
- ❖ Tier 2: Unknown vulnerabilities (zero-day exploits)
- ❖ Tier 3: Adversary-created vulnerabilities (APT)



✶ Potential Categories

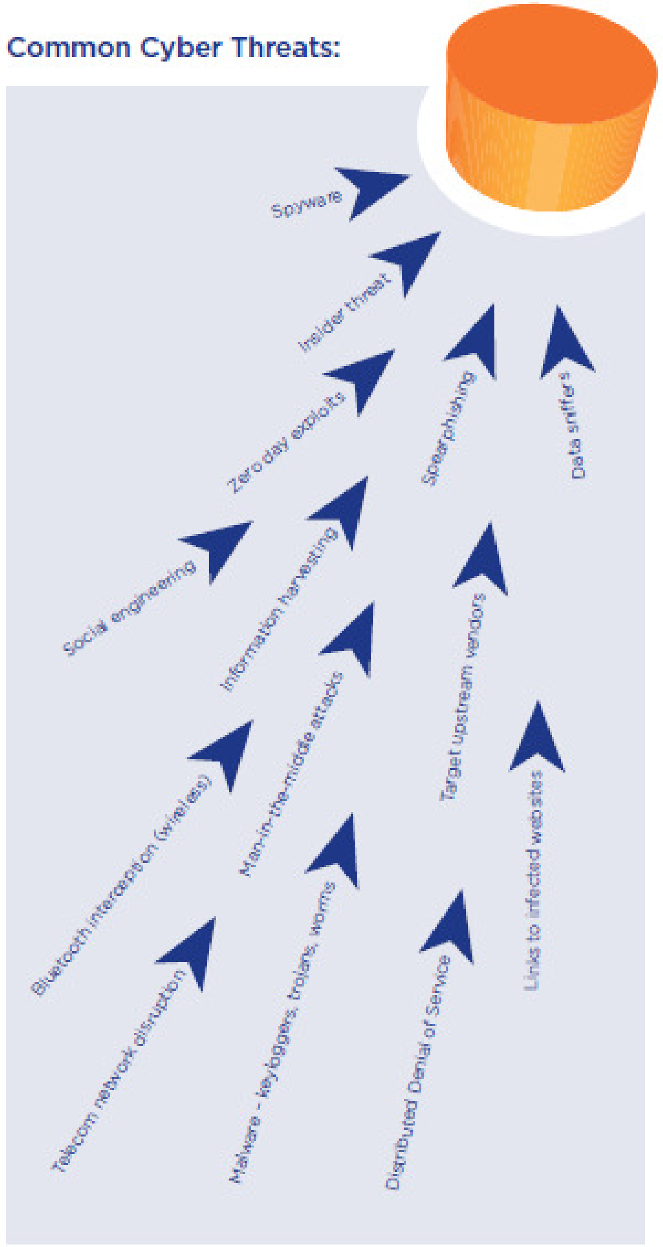
- Application Security
- Network infrastructure
- End Devices
- Operations
- Help Desk / Support
- End Users
- Servers

What makes a good metric?

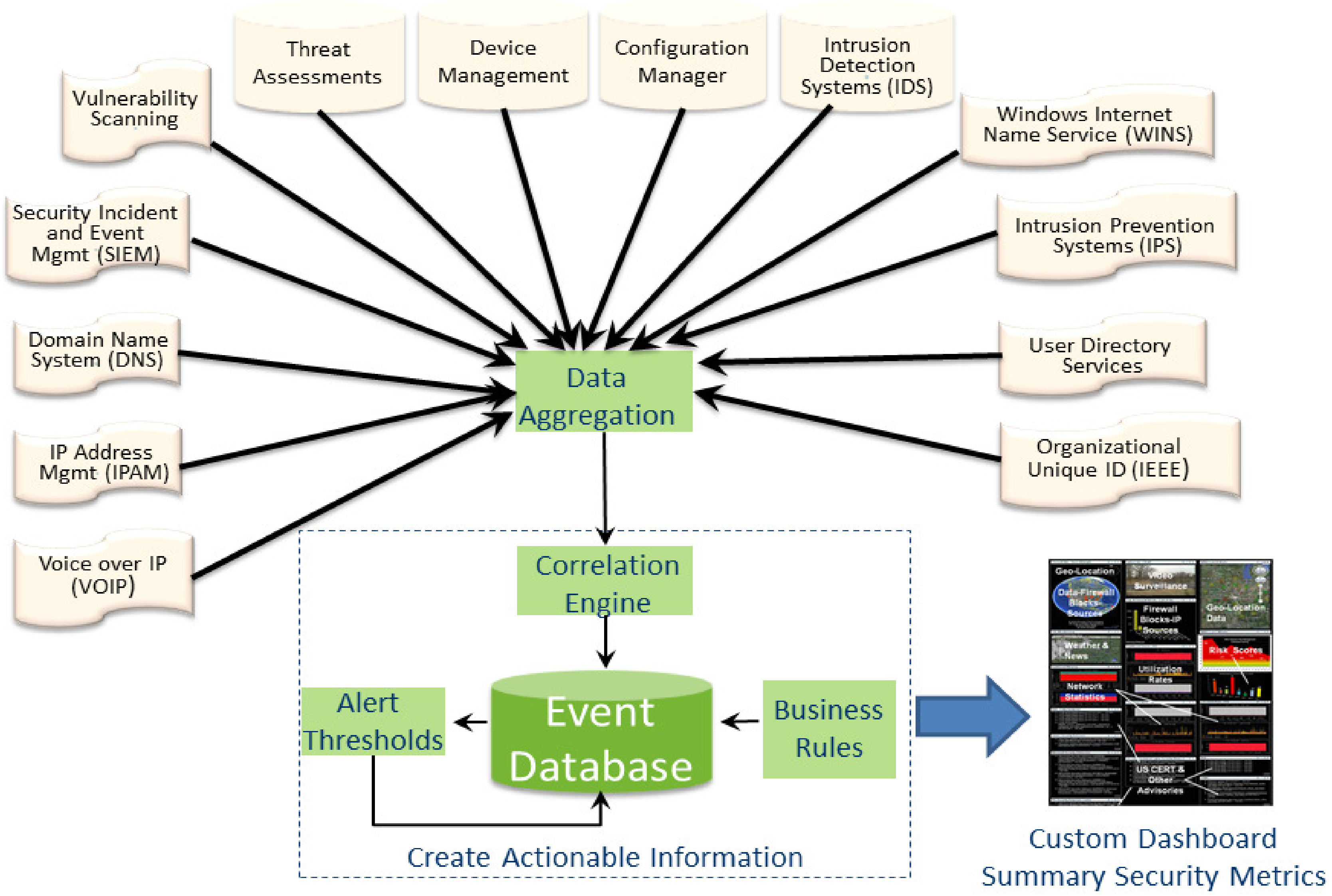
- Consistent collection methodology
- Common definition – across an enterprise
- Standard of ***measurement*** – clear, not ambiguous
- Improves organization security posture
- Supports comparisons over time
- Enables comparison with peer companies
- Effort to collect consistent with results
- Enables decision making
- Supports forensics as needed
- Cheap / easy to collect

Toolset

- SIEM (Security Incident and Event Monitor)
  - Raw data collection
  - Collect into central repository
- NIST documents
  - Special Publication (SP) 800-39
    - Managing Info Security Risk
  - SP 800-30
    - Guide for Conducting Risk Assessments
- Threat Assessment Services
- Vulnerability Scanners


Common Cyber Threats:
Spyware
Insider threat
Zero day exploits
Spearphishing
Data sniffers
Social engineering
Information harvesting
Target upstream vendors
Bluetooth interception (wireless)
Man-in-the-middle attacks
Links to infected websites
Telecom network disruption
Malware - keyloggers, trojans, worms
Distributed Denial of Service

Sample Security Metrics Architecture



Vulnerability Scanning

Threat Assessments

Device Management

Configuration Manager

Intrusion Detection Systems (IDS)

Windows Internet Name Service (WINS)

Security Incident and Event Mgmt (SIEM)

Intrusion Prevention Systems (IPS)

Domain Name System (DNS)

User Directory Services

IP Address Mgmt (IPAM)

Organizational Unique ID (IEEE)

Voice over IP (VOIP)

Data Aggregation

Correlation Engine

Alert Thresholds

Event Database

Business Rules

Create Actionable Information

Custom Dashboard
Summary Security Metrics

CYBER DASHBOARDS

Enable Complete Picture of Network Assets – Aggregation, Correlation

Situation

No enterprise view of the risk profile exists to enable a robust and resilient cyber defense posture

Solution

1. Gather and correlate existing data on systems
2. Identify complete set of IT assets
3. Store and display information in central location

Data is fused into a single picture of network devices based on inputs from multiple authoritative security and management sources

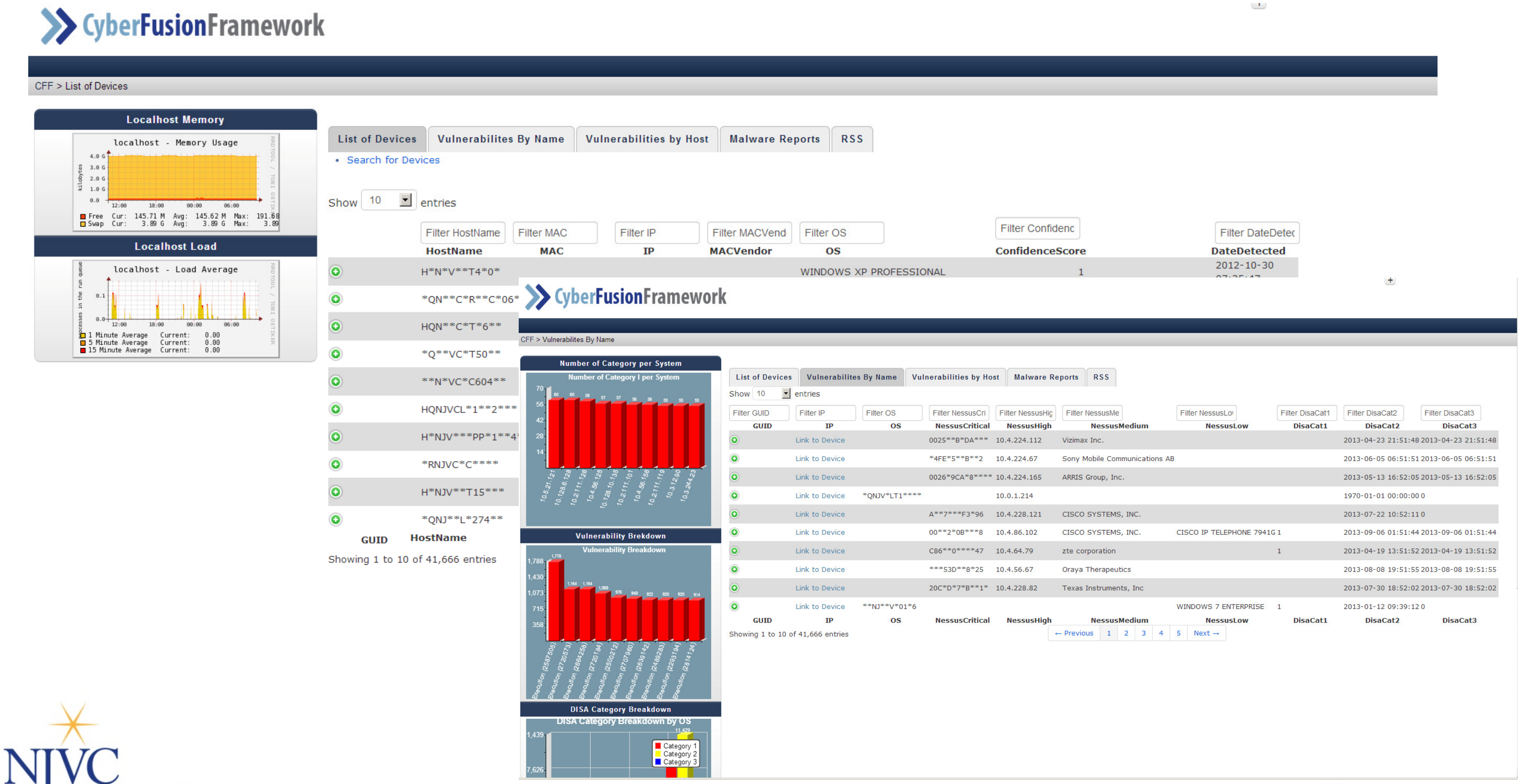
- Actionable Data – Enable the network operators and security analysts
- Provide data in near real time as well as trending data over time

Benefit

- ✶ Enables continuous monitoring
- ✶ Provides real time visualization of security posture of enterprise
- ✶ Reduces the time between detect and react
- ✶ Empowers incident prevention through anomalous behavior detection and trending analysis

Data Collection Components

List of Devices	RSS Data Feeds	Host Names
Vulnerabilities by Name	Malware severity rating	Operating Systems
Vulnerabilities by Host	IP Addresses in use	Unauthorized software
Malware Threat List	MAC Addresses in use	PHI timestamps



CFF > List of Devices

List of Devices | Vulnerabilites By Name | Vulnerabilities by Host | Malware Reports | RSS

- Search for Devices

Show 10 entries

GUID	HostName	MAC	IP	MACVendor	OS	ConfidenceScore	DateDetected
	Filter HostName	Filter MAC	Filter IP	Filter MACVend	Filter OS	Filter Confidenc	Filter DateDetec
●	H*N*V**T4*0*				WINDOWS XP PROFESSIONAL	1	2012-10-30
●	*QN**C*R**C*06*						
●	HQN**C*T*6**						
●	*Q**VC*T50**						
●	**N*VC*C604**						
●	HQNJVCL*1**2***						
●	H*NJV***PP*1**4						
●	*RNJVC*C****						
●	H*NJV**T15***						
●	*QNJ**L*274**						

Showing 1 to 10 of 41,666 entries

CyberFusionFramework

CFF > Vulnerabilites By Name

List of Devices | Vulnerabilites By Name | Vulnerabilities by Host | Malware Reports | RSS

Show 10 entries

GUID	IP	OS	NessusCritical	NessusHigh	NessusMedium	NessusLow	DisaCat1	DisaCat2	DisaCat3
Filter GUID	Filter IP	Filter OS	Filter NessusCri	Filter NessusHig	Filter NessusMe	Filter NessusLo	Filter DisaCat1	Filter DisaCat2	Filter DisaCat3
●	Link to Device		0025**B*DA***	10.4.224.112	Vizimax Inc.			2013-04-23 21:51:48	2013-04-23 21:51:48
●	Link to Device		*4FE*5**B**2	10.4.224.67	Sony Mobile Communications AB			2013-06-05 06:51:51	2013-06-05 06:51:51
●	Link to Device		0026*9CA*8****	10.4.224.165	ARRIS Group, Inc.			2013-05-13 16:52:05	2013-05-13 16:52:05
●	Link to Device	*QNJV*LT1****		10.0.1.214				1970-01-01 00:00:00	0
●	Link to Device		A**7***F3*96	10.4.228.121	CISCO SYSTEMS, INC.			2013-07-22 10:52:11	0
●	Link to Device		00**2*0B***8	10.4.86.102	CISCO SYSTEMS, INC.	CISCO IP TELEPHONE 7941G	1	2013-09-06 01:51:44	2013-09-06 01:51:44
●	Link to Device		C86**0****47	10.4.64.79	zte corporation		1	2013-04-19 13:51:52	2013-04-19 13:51:52
●	Link to Device		***53D**8*25	10.4.56.67	Oraya Therapeutics			2013-08-08 19:51:55	2013-08-08 19:51:55
●	Link to Device		20C*D*7*B**1*	10.4.228.82	Texas Instruments, Inc			2013-07-30 18:52:02	2013-07-30 18:52:02
●	Link to Device	**NJ**V*01*6				WINDOWS 7 ENTERPRISE	1	2013-01-12 09:39:12	0

Showing 1 to 10 of 41,666 entries

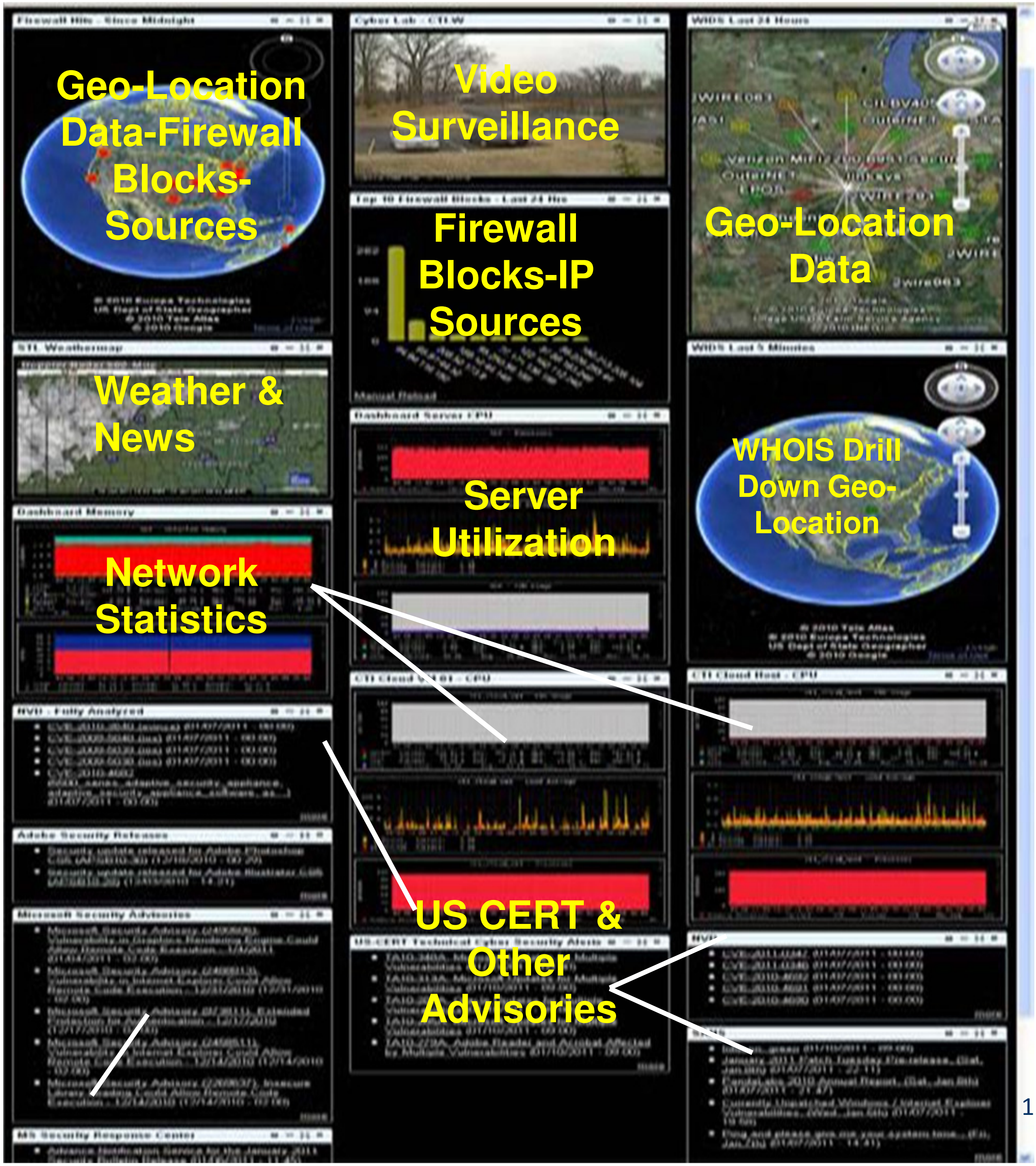
← Previous | 1 | 2 | 3 | 4 | 5 | Next →

NJVC
Driven by Your Mission®

www.njvc.com/healthcare-it

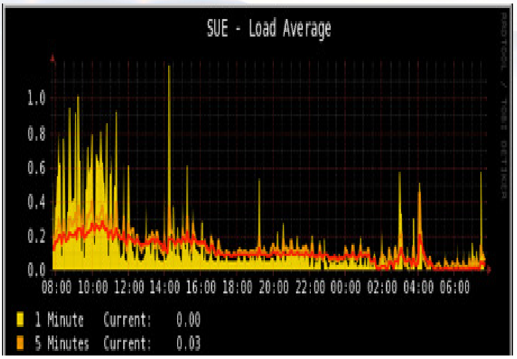
Cyber Dashboard

- Enterprise capable
  - Configure sensors in environment as appropriate
- User focused
  - Able to be tailored for each stakeholder
- Visual display of data feeds
  - Accepts feeds from external sources
  - Vendor neutral
- Automated device interrogation
  - Periodic updates
- Display aggregation

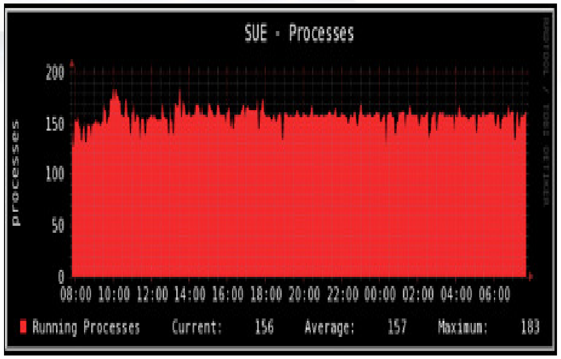

Geo-Location Data-Firewall Blocks-Sources
Video Surveillance
Geo-Location Data
Firewall Blocks-IP Sources
Weather & News
Server Utilization
WHOIS Drill Down Geo-Location
Network Statistics
US CERT & Other Advisories

System Status & Performance at a Glance

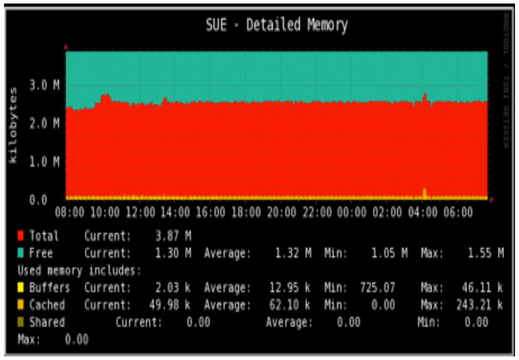
- Evaluate configuration changes
- Perform root cause analysis
- Plan network enhancements
- Detect suspicious activity
- Process alerts
  - Data exfiltration
  - Resource performance thresholds
  - Denial of Service attacks



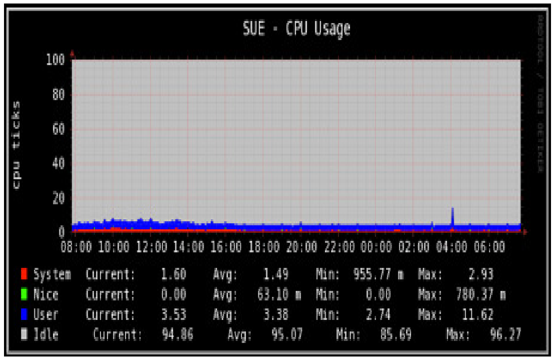
```
1 Minute   Current:   0.00
5 Minutes  Current:   0.03
```



```
Running Processes   Current:   156   Average:   157   Maximum:   183
```



```
Total    Current:   3.87 M
Free     Current:   1.30 M  Average:   1.32 M  Min:    1.05 M  Max:    1.55 M
Used memory includes:
Buffers  Current:   2.03 k  Average:  12.95 k  Min:  725.07    Max:   46.11 k
Cached   Current:  49.98 k  Average:  62.10 k  Min:    0.00    Max:  243.21 k
Shared        Current:    0.00        Average:    0.00        Min:    0.00
Max:    0.00
```



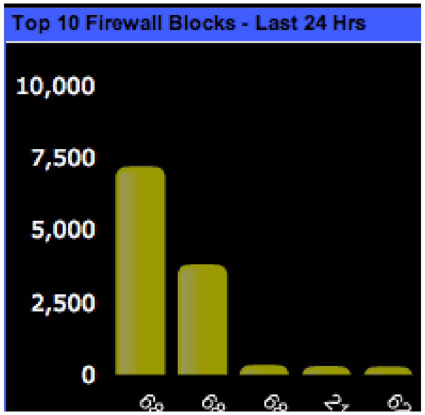
```
System  Current:   1.60   Avg:    1.49    Min:  955.77 m  Max:    2.93
Nice    Current:   0.00   Avg:   63.10 m  Min:    0.00    Max:  780.37 m
User    Current:   3.53   Avg:    3.38    Min:    2.74    Max:   11.62
Idle     Current:  94.86    Avg:   95.07     Min:   85.69     Max:   96.27
```

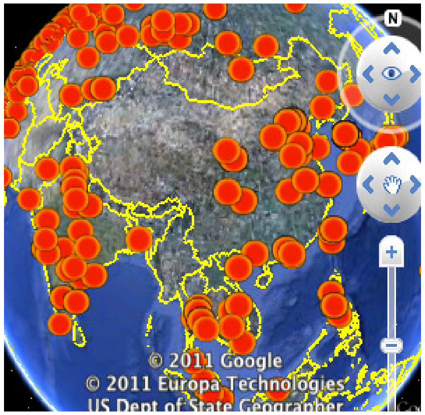
- Mobile Device status
- Authorized apps installed
- Remote wipe capability
- Summary usage statistics

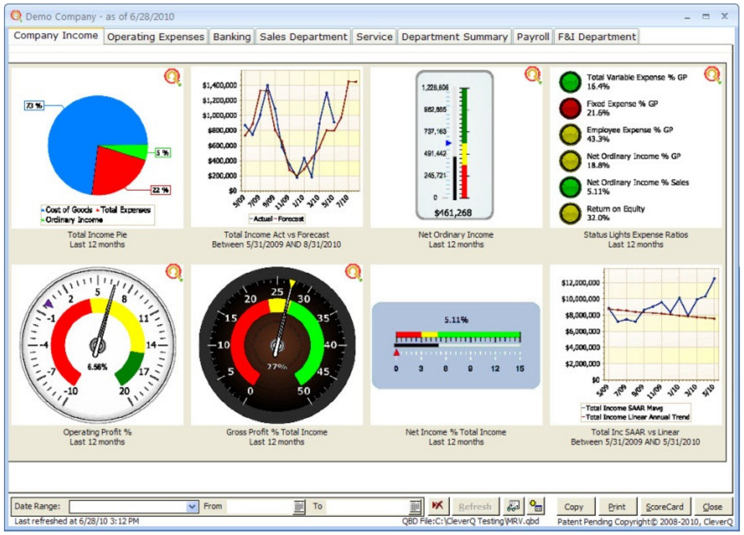
Cyber Dashboard - Event Analysis and Reporting

- The same data set can be viewed in multiple formats
- Different perspectives help tell the full story and readily aid in identifying appropriate response priorities

- One depiction will readily identify the most aggressive attackers
- Another view of the same data can be rendered to show geographic dispersion and density



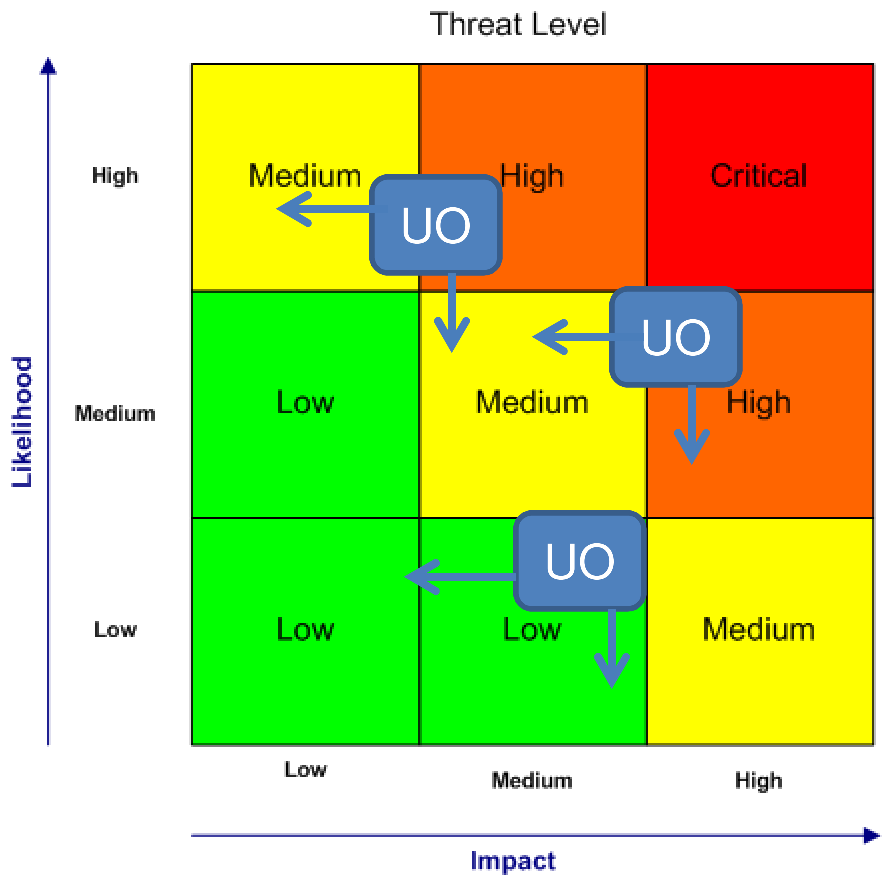




NJVC Driven by Your Mission®

ANALYTICS

Risk Management Methodology



Threat Level

	Low	Medium	High
High	Medium	High	Critical
Medium	Low	Medium	High
Low	Low	Low	Medium

Quantify and create a mitigation for each risk

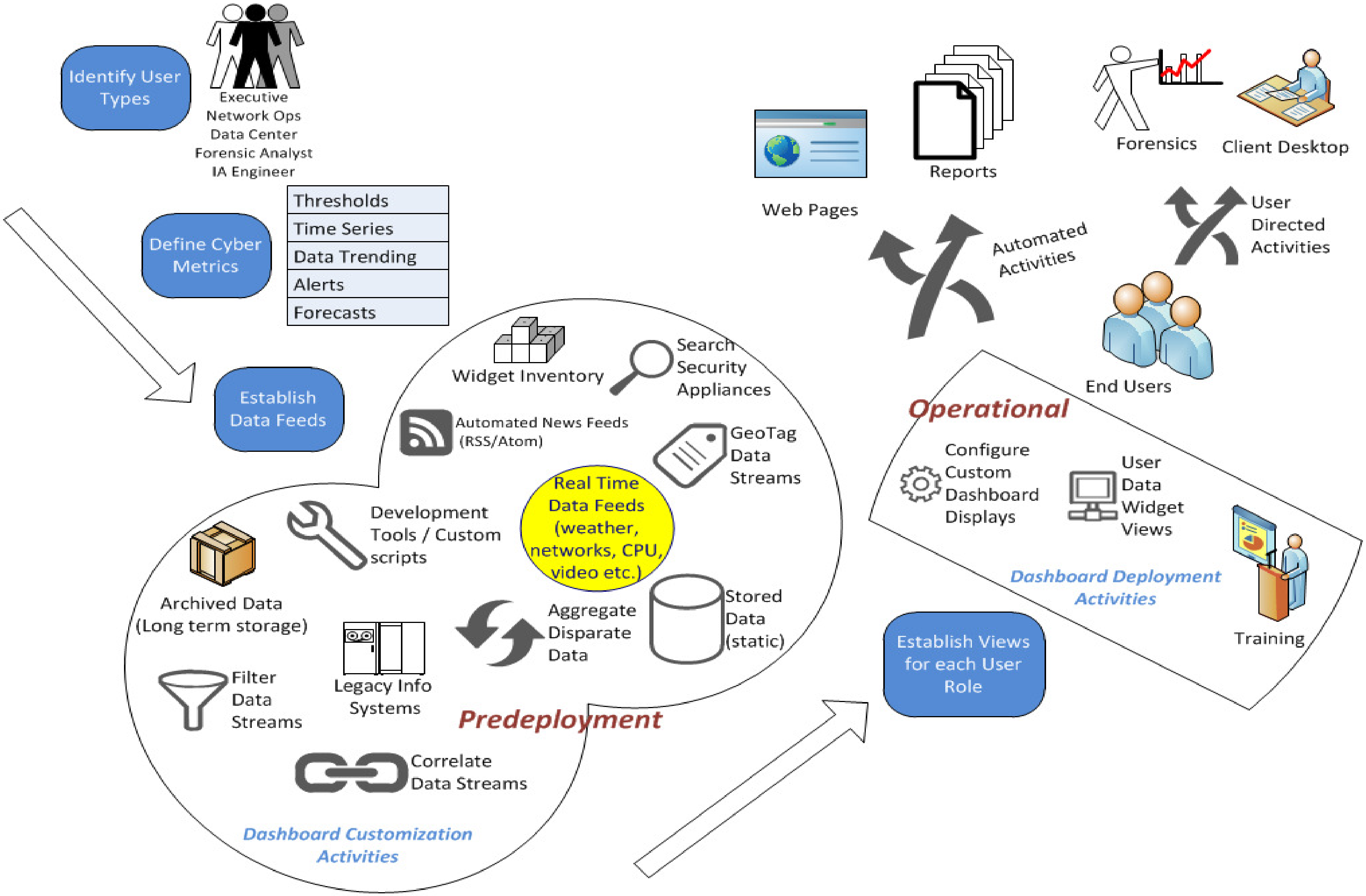
- Start with Risk Matrix
- Define Unwanted Outcomes (UO)
  - System breaches
  - Data egress
  - Unauthorized account access
  - Malware intrusion
  - Privilege escalations
  - Patches out of date
  - System downtime
  - Unauthorized data alterations
  - Network unavailability etc. etc.
- Map UO onto Matrix
  - Look to reduce likelihood
    - (Frequency of event)
  - Look to reduce impact
    - (Magnitude of harm)

Breach Detection

- Passive
  - Unusual system behavior
    - First time events
    - Login failures
    - Data replication
    - Data movement
    - DNS server configuration changes
    - DNS query failures
    - User privilege escalations
  - Many vendor analysis tools exist – but sifting through Big Data – and uncovering threats at line speeds requires ***automation***

- Active
  - Log detection
  - Human review of pre-filtered, pre-screened data.
  - Needle in a haystack – need to point the analyst where to look…
  - Aggregate volumes of data into a summary format
  - Stop data egress once infiltration is identified (minimize damage even if you have been breached)
  - Data Loss Prevention (DLP) products

Cybersecurity Analytics Service



Identify User Types

Executive
Network Ops
Data Center
Forensic Analyst
IA Engineer

Define Cyber Metrics

Thresholds
Time Series
Data Trending
Alerts
Forecasts

Establish Data Feeds

Widget Inventory

Search Security Appliances

Automated News Feeds (RSS/Atom)

GeoTag Data Streams

Development Tools / Custom scripts

Real Time Data Feeds (weather, networks, CPU, video etc.)

Archived Data (Long term storage)

Aggregate Disparate Data

Stored Data (static)

Filter Data Streams

Legacy Info Systems

Predeployment

Correlate Data Streams

Dashboard Customization Activities

Web Pages

Reports

Forensics

Client Desktop

Automated Activities

User Directed Activities

End Users

Operational

Configure Custom Dashboard Displays

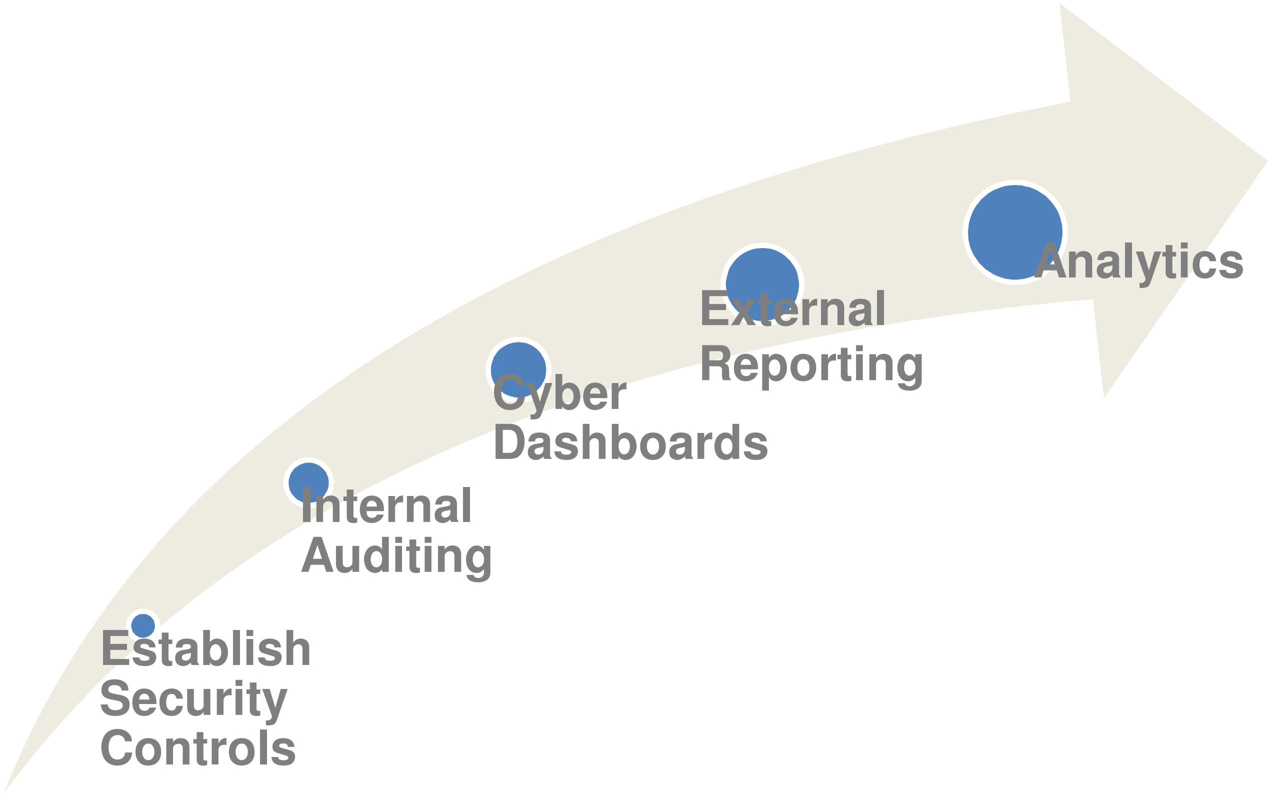
User Data Widget Views

Training

Dashboard Deployment Activities

Establish Views for each User Role

Moving to Continuous Diagnostics and Mitigation



Establish Security Controls

Internal Auditing

Cyber Dashboards

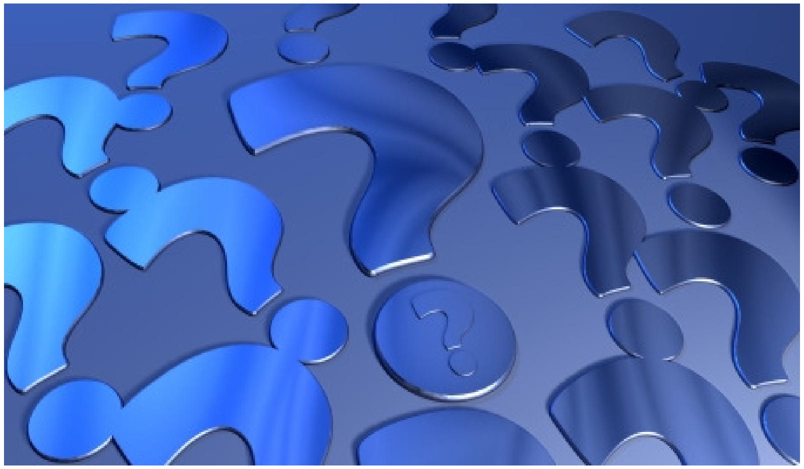
External Reporting

Analytics

Cyber Command

DHS CyberScope

THANK YOU



QUESTIONS?

Robert.michalsky@njvc.com

Twitter: RobertMichalsky

NJVC cyber security blog posts: http://www.njvc.com/blog

White paper series on healthcare: http://www.njvc.com/resource-center/white-papers-and-case-studies