



Comprehensive, On-Demand Security.

7 Top Data Sources for Security Monitoring

Peter Bybee, CISSP, CISA

President/CEO

February 2009

- **Security On-Demand**

- Founded 2001
- “On-Demand” Managed Security Services

- **Peter Bybee, President/CEO**

- CISSP, CISA, San Diego ISSA Chapter President
- Speaker, Lecturer, Published Author & Security Expert
- Expertise with Small, Medium, & Enterprise & able to address multiple Compliance Areas (SOX, HIPAA, PCI, GLBA, etc.)

- **Security On-Demand**

- Over 1000 Security Devices being actively managed
- Client base consisting of Banks, Credit Unions, Healthcare, biotechnology, retail, e-commerce, etc.
- Compliance Management for PCI, HIPAA, SOX, GLBA, etc.

- **Operations**

- SAS-70 Certification
- 24x7x365 Staffing
- PCI Certified ASV
- Worldwide Coverage
- Redundant Data Centers
- Certified Security Analysts



- **Monitoring means**

1. Centrally collecting events from critical systems, applications, & security devices in real time
2. Performing analysis of traffic, data, and events in real time
3. Deciding on what actions to take or not take based on established policy
4. Responding according the Security Incident Response Plan

- **What connection between monitoring & Logging?**

- Monitoring is NOT Logging
- Log Data from various data sources is *part* of the overall monitoring & risk management process

- **Why Should you Monitor?**

- Protect Sensitive Company Data Assets
- Required by Compliance & Regulatory Bodies
- Business Disruption Cost
- Legal Liability for Data Replacement
- Reputation Loss
- Fines for a Data Breach (PCI, HIPAA, SB-1386, etc.)

- **If I didn't do it before, Why do I need it now?**

- Regulatory Requirements have changed
- Standard of Due Care – Considered prudent today
- Evolving Threats & Increased Risk to Financial Exploits

- **In September of 2007, Robert Moore pleaded guilty to conspiracy to commit computer fraud & was sentenced to 2 years in Federal prison**
- **He broke into 15 telecommunications companies and hundreds of businesses worldwide**
- **Moore scanned more than 6 million computers just between June and October of 2005. AT&T reported to the court that Moore ran in excess of 6 million scans on its network alone.**

How did he do it?

- **He purchased 2 GB of data on corporate IP ranges for \$800**
- **He then scanned the IPs looking for specific devices he wanted to exploit**
- **Using recon techniques & simple network probing & mapping he looked for specific vulns**
- **Then ran exploits for unpatched code, known vulns & dictionary attacks against weak passwords**
- **70% of all the companies he scanned were insecure, and 45% to 50% of VoIP providers were insecure.**

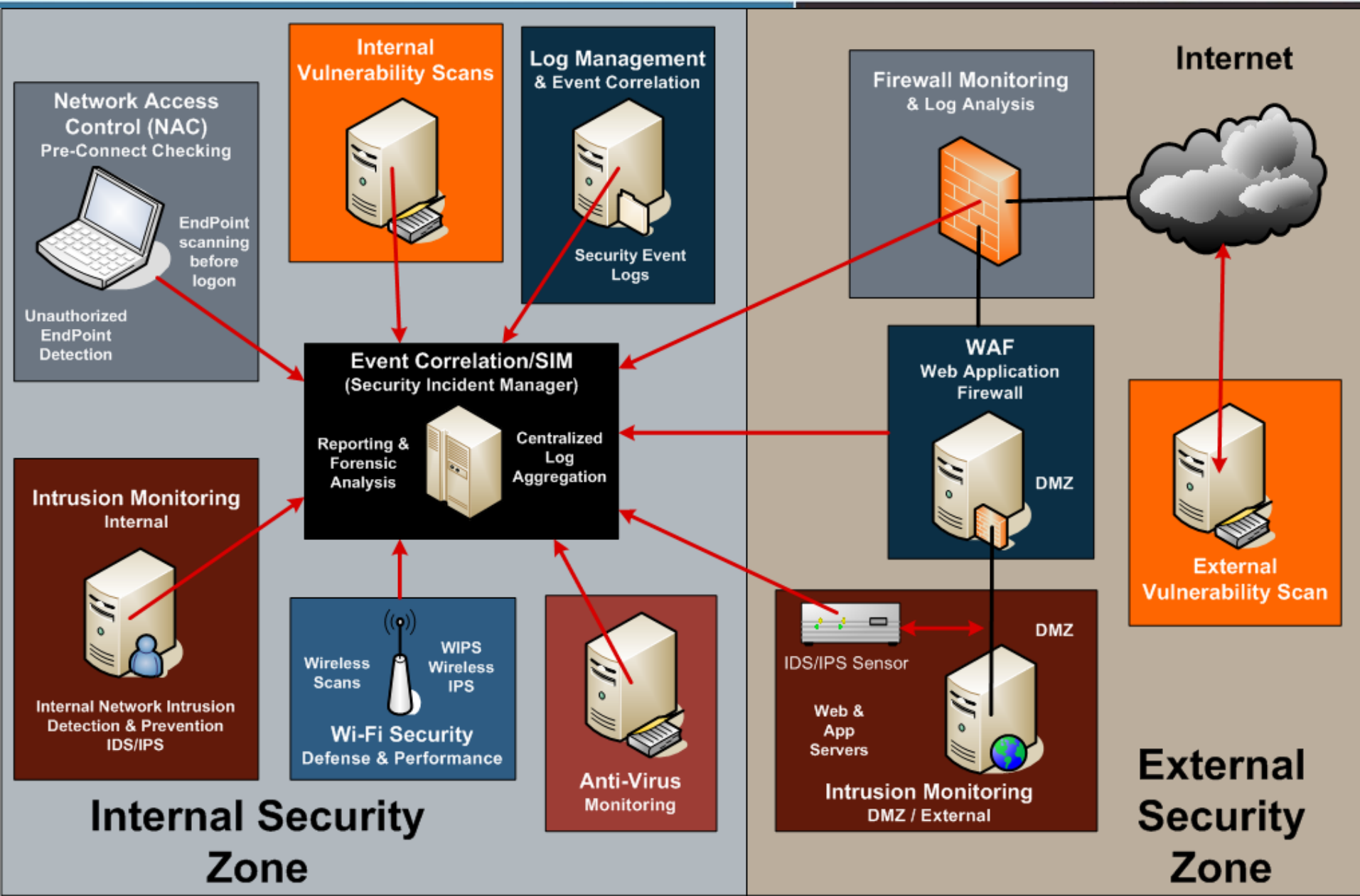
- **Moore said it would have been easy for IT and security managers to detect him in their companies' systems... if they'd been looking.**
- **The problem was that, generally, no one was paying attention.**
- **He further commented:**
 - "If they were just monitoring their boxes and keeping logs, they could easily have seen us logged in there,"
 - "If they had an intrusion detection system set up, they could have easily seen that these weren't their calls."

- **What is the Ideal Monitoring Scenario?**
- **Monitor Everything!!**
 - However - Impractical due to resource constraints
 - Monitor Select Devices & Sources – Will only give you a partial picture

Where is Security Data Found?

- Virtually all systems on the corporate network contain security data
- **What data sources are most valuable?**
- **How to determine what data sources & devices to include and exclude?**

Security Architecture Model



- **Fundamental Questions**

- What data sources are most valuable to monitor?
- How do you determine what data sources & devices to include and exclude?
- How do you get a handle on understanding the risk or severity level associated with a monitoring alert?

5 Data Monitoring Challenges

- 1. Security Context**
- 2. Information Overload (Too Much Data)**
- 3. “Siloed” Security information**
- 4. Lack of Information about “Bad Guys”**
- 5. Process, Documentation, & Reporting**

1. Security Context

- **What is Context?**
 - Prioritizes value of each data monitoring source
 - Depends on the source's ability to help you make decisions
 - Is specific to each organization
- **All systems/data sources do *not* provide equally valuable Security Context.**
 - The more relevant security context you have, the more likely it is you will successfully detect real security incidents while weeding out false positives
- **Incorporating Security Context means focusing on areas of risk to the organization**
 - Risk is primarily comprised of threat, vulnerability, Asset Value and Impact (or potential impact)

- **Conduct security architecture context review**
 - Understand where critical data is being stored & transmitted (data at rest, data in transit)
 - Help determine what data sources are most important based on overall risk to business
- **Identify other data sources that can be integrated with new or existing security layers**
 - Newer Services, such as WAF, NAC, Wireless, etc.
- **Help Consolidate Security Layers & reduce complexity (e.g. IPS combined with NAC, etc.)**
- **Ensure that Compliance Requirements are met**

- 1. Network IDS/IPS Alerts**
- 2. Firewall Alerts**
- 3. Host & Client Based Alerts**
- 4. Network Devices with ACLs**
- 5. Server & Application Logs**
- 6. Wireless Alert Data**
- 7. Vulnerability Scan Data**
- 8. Unauthorized Access or Use**

Determining Risk through Event Triage

- **Looking at Alerts outside of a risk context is a waste of Time**
- **Understand the asset value**
- **Instantly Understanding the severity of a threat is critical when determining what action to take**
- **The alert severity should be higher if there is an attack against a vulnerability that the network is susceptible**

- **The Problem of Too Much Data**

- Monitoring too much data and/or irrelevant data means you will have lots of false positives
- Security Architectures (IDS, IPS sensors, Firewalls, etc.) are designed to “Sense”, not analyze, sift, or filter

- **Event Correlation**

- Developing Correlation Rules in SIM products is hard & requires constant tuning, new rule creation

- **Million Dollar Question –**

- How do you use information being reported or logged, to improve your security posture (e.g. tune or change a rule in your firewall or IDS)

2. Filtering Suggestions

- **Eliminate Unnecessary & Excess Data**
 - Use Sensors that filter out excess data using alert thresholds that are tuned to the company environment
 - Alert Data that has exceeded analysis criteria and should be further analyzed and followed up on
- **Optimized Alert Architecture**
 - Filter out excess data at the edge (sensor) before it's processed & analyzed by the SIM (event correlation engine)
 - Monitoring a small subset of relevant data means it's easier to detect and understand real threats

3. “Siloed” Security Information

- **Where do information security silos exist?**
 - Scan data (PCI Scans, vulnerability scans)
 - Risk Assessments
 - Audit & Compliance Reports on Internal Controls
 - Defenses & Countermeasures
 - Performance Mechanisms & Data
 - Service Providers – ISPs, etc.
 - Flows - Routing & Switching Infrastructure
 - Audit & Event Logs
 - People – IT Staff, consultants, business partners, 3rd party vendors

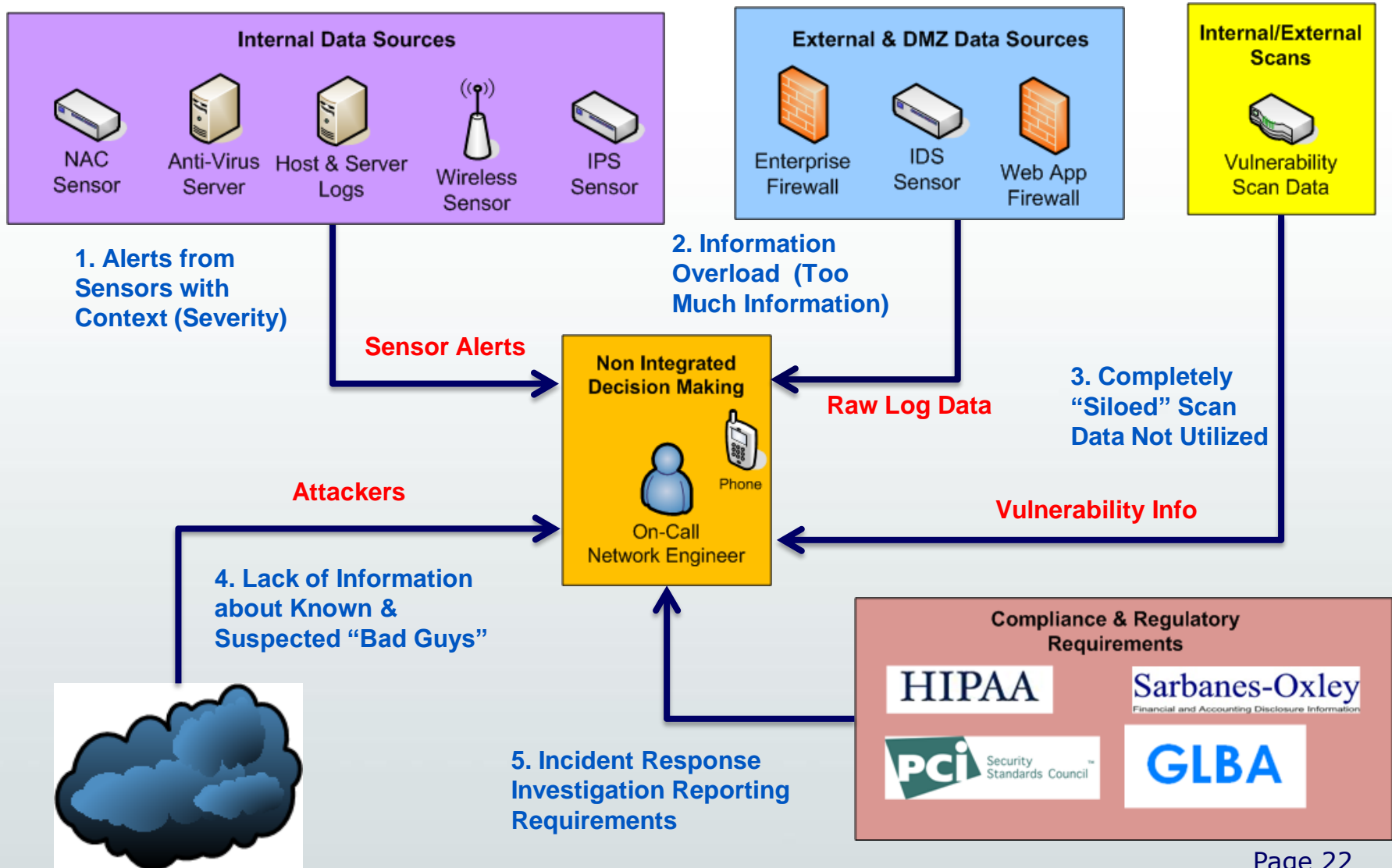
4. Research on “Bad Guys”

- **In 2003 ISS published some research they had gathered**
- **They reported that among all reported/known successful attacks exploiting data and committing credit card theft, 50% of the attacks originated from IP addresses that were previously published as known fraudulent or suspected attacker IPs**
- **Today there are lots of good sources for information on the internet that can provide help**
 - **Dshield.org, CyberTA, CERT, & Others**

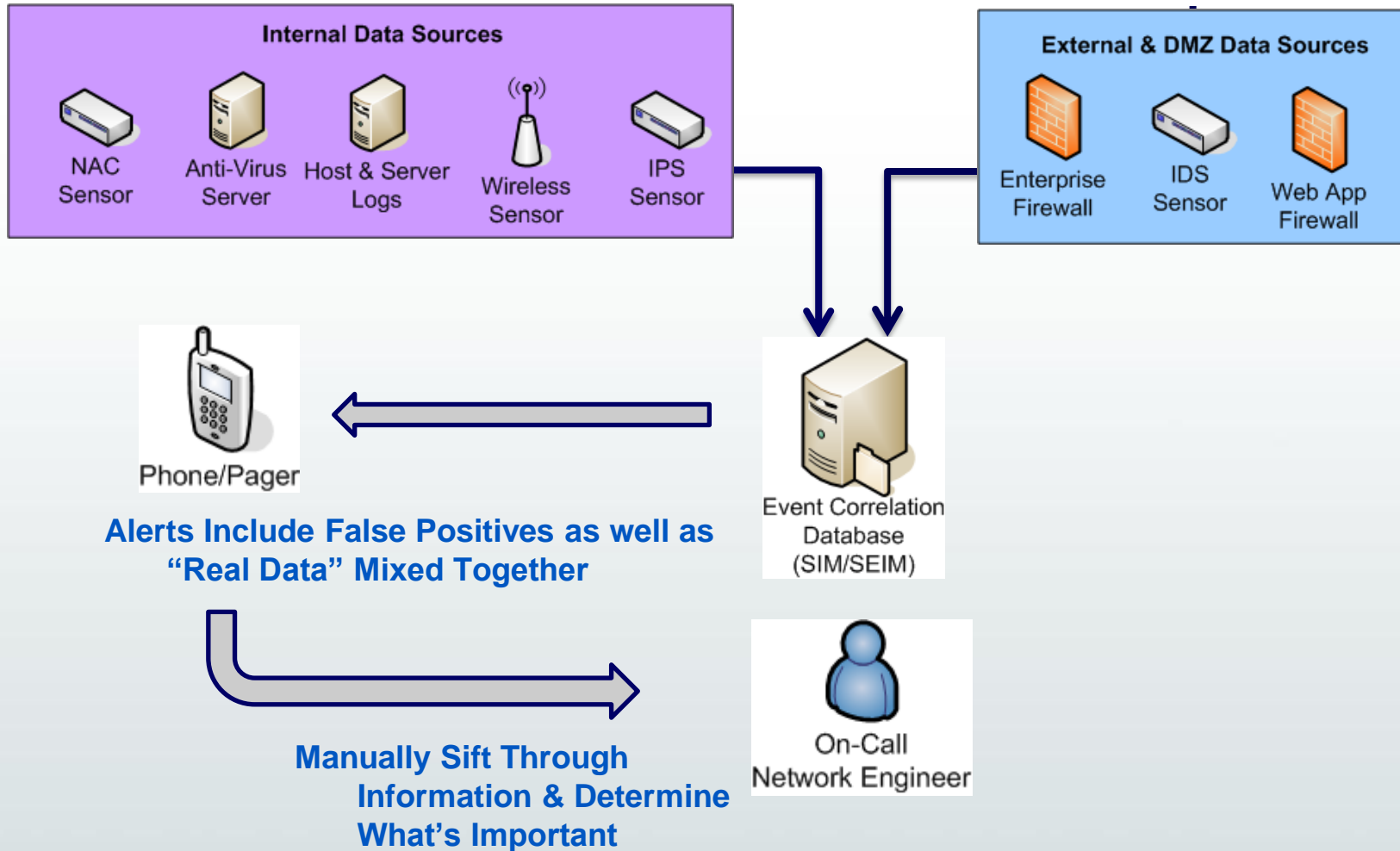
5. Reporting & Process

- **For most compliance initiatives, it's not enough to wait for a confirmed successful penetration**
- **In order to defend against legal liability, you need to demonstrate that your company, management, culture, etc. actually cares by showing that a minimum standard of Due Diligence is maintained**
- **You need to log and report on suspected and attempted violations of computer policy (attacks, or unauthorized attempts to access data)**
- **Needs to address internal as well as outsider attacks (employee insider)**

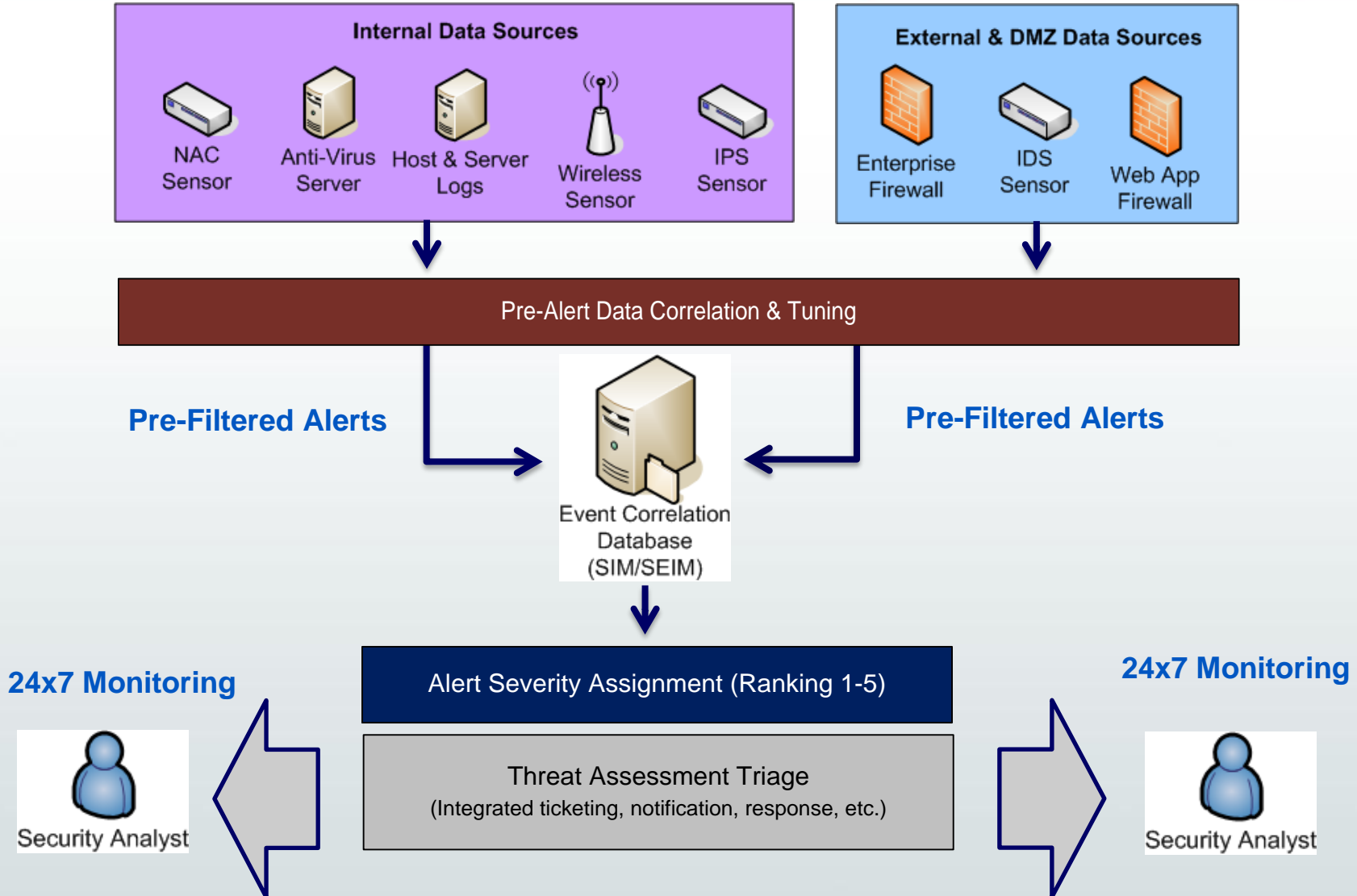
Frequent Pain Points



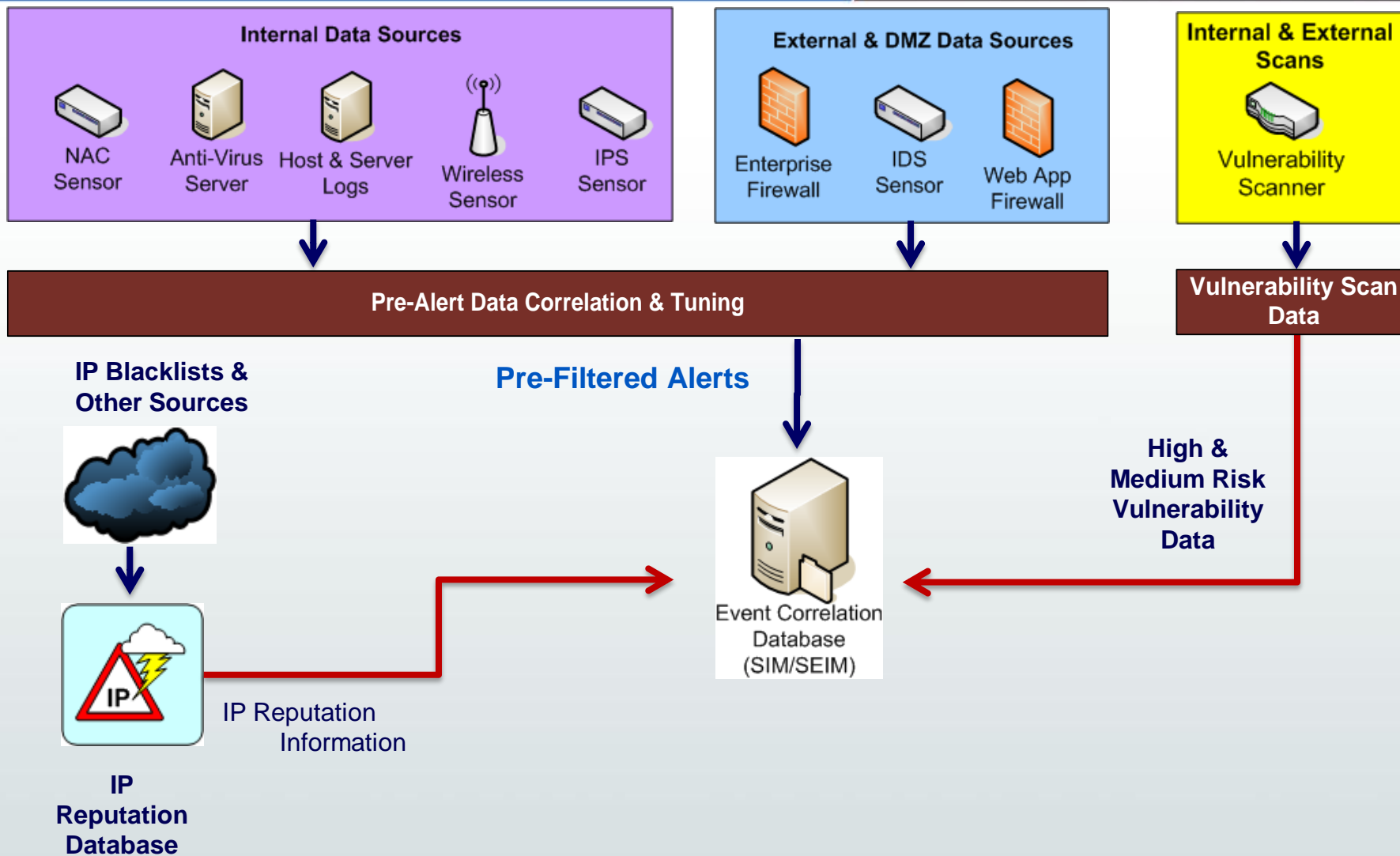
Traditional Monitoring Solution



Architecture Recommendations



Scan Data & IP Blacklists



7 Top Monitoring Priorities

- 1. Network IDS/IPS Alerts**
- 2. Firewall Alerts**
- 3. Host & Client Based Alerts**
- 4. Network Devices with ACLs**
- 5. Server & Application Logs**
- 6. Wireless Alert Data**
- 7. Vulnerability Scan Data**

1. Network IDS/IPS

- **Typically Signature Based – Requires Constant Updates that should be Contextual**
 - Only signatures pertinent to your environment should be applied
 - What signatures to apply should be specific to your Company Profile
- **Performing full packet inspection of network traffic at the perimeter or across key network segments**
- **Most NIDS/NIPS devices provide detailed alerts that help to detect:**
 - Known vulnerability exploit attempts
 - Known Trojan activity
 - Anomalous behavior (depending on the IDS/IPS)
 - Port and Host scans

2. Firewalls

- **Some firewalls also have basic IPS signatures to detect security events.**
 - Firewall IPS events should also be Monitored (Smart Defense)
- **Monitoring firewall logs and alerts helps to detect:**
 - New and unknown threats, such as custom Trojan activity
 - Port and Host scans
 - Worm outbreaks
 - Minor anomalous behavior
 - Most any activity denied by firewall policy

- **Includes Host-based Intrusion Detection and Prevention Systems (HIDS/HIPS)**
 - Signature Based
- **Network Access Control**
 - Behavior Based - This approach is far superior to the HIDS/HIPS Approach
 - NAC Alerts exist in the form of Policy Violations
- **Monitoring Host & Client based alerts helps to detect:**
 - Known vulnerability exploit attempts
 - Console exploit attempts
 - Exploit attempts performed over encrypted channels
 - Password grinding (manual or automated attempts to guess passwords)
 - Anomalous behavior by users or applications

4. Network Devices

- **Includes Network Devices with Access Control Lists (ACLs)**
- **Network devices that can use ACLs,**
 - such as routers and VPN servers,
 - have the ability to control network traffic based on permitted networks and hosts.
- **Monitoring logs from devices with ACLs helps to detect:**
 - New and unknown threats, such as custom Trojan activity
 - Port and Host scans
 - Minor anomalous behavior
 - Most anything denied by the ACL's
- **This is Primarily log monitoring, NAC can do a better job of identifying anomalous behavior.**

5. Server & Application Logs

- **Many types of servers and applications log events such as login attempts and user activity.**
- **Depending on the extent of logging capabilities, monitoring server and application logs can help to detect:**
 - Known and unknown exploit attempts
 - Password Grinding
 - Anomalous behavior by users or applications
- **Event Correlation/SIM Technology can help**

6. Wireless Data

- **Defending the Airspace**
 - Detection of rogue Devices
 - Drive By & Passive Scanning
 - Prevent Users from Circumventing Internal Controls

- **Client Protection**
 - Client Mis-association
 - Zero Config Policies on Mobile Devices
 - Enforcing User Policy when Remote
 - Bridging the internal network from wired to wireless

7. Vulnerability Scan Data

- **Proactive in Nature**
- **Is More Powerful with Correlated with**
 - CVE Information
 - IP Reputation
 - Vulnerability Signatures
 - Threat & Database Resources
- **Nirvana – Integration of Threat Information with Vulnerability Data specific to the Client environment**
 - Vulnerabilities
 - O/S
 - Open Ports
 - Applications

- Incremental value of a data source will vary from situation to situation.
- A source's purpose, its location in your network and the quality of the data it provides are a few of the many variables that must be considered when planning your security monitoring strategy.
- By monitoring the assets that provide the highest security context value, eliminating excess "noise", and assigning alerts to risk levels, you can optimize your security monitoring efforts.



Comprehensive, On-Demand Security.

Using Service Providers to Help You with Monitoring

Peter Bybee, CISSP, CISA

September 2008

Managed Services Evolution

- Carriers owned & controlled equipment
- Contract was outsource arrangement bundled with CPE
- Often Colocation Based

- Lots of M&A
- Simple Web Portals
- Offerings built around proprietary technology
- Managed on Client Premises
- Still used Outsourced Model

- Evolved Offerings
- Co-managed SLAs
- Services "In the Cloud"
- Security-as-a-Service
- Services Transparency
- Security Dashboards blend sensor data
- Reputation Analysis

Web 1.0 & ASP Era

Expanded e-Commerce and Web Apps Era

Web 2.0, SaaS & "On-Demand" Era

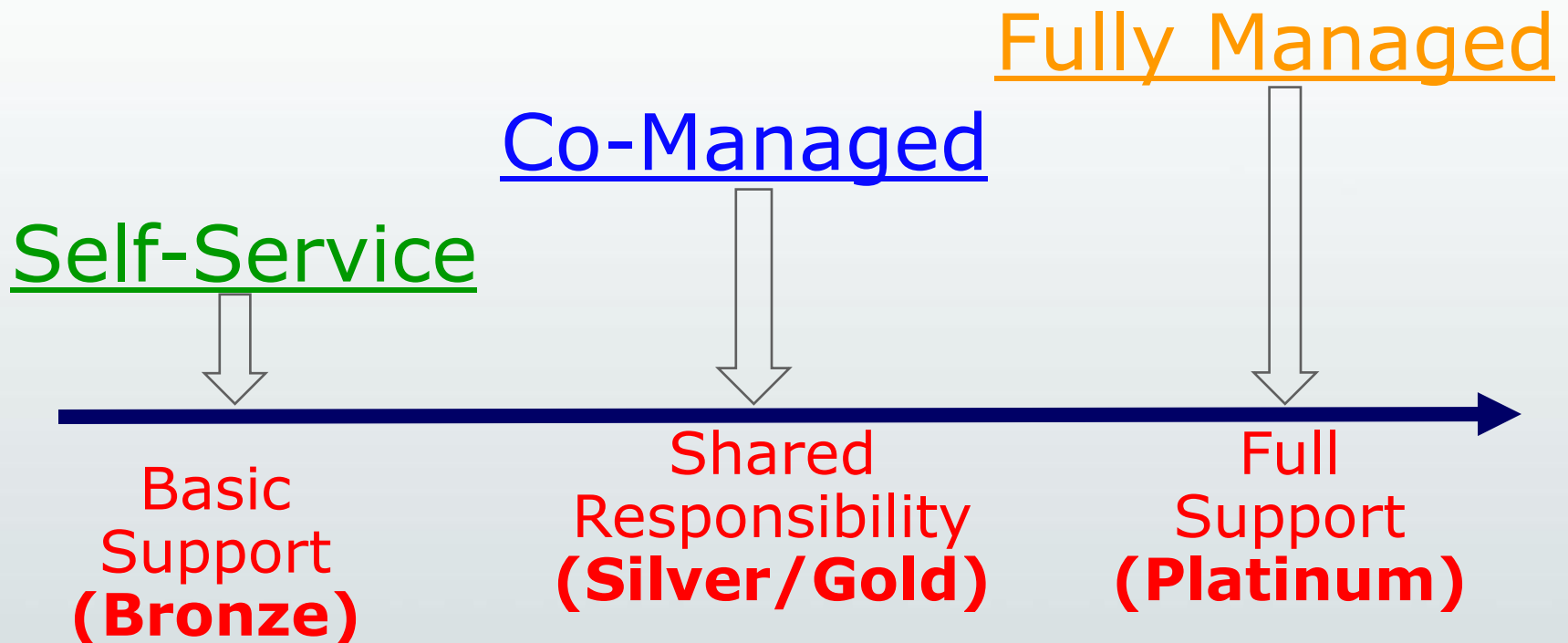
**1st Generation
1998 – 2002**

**2nd Generation
2002 – 2007**

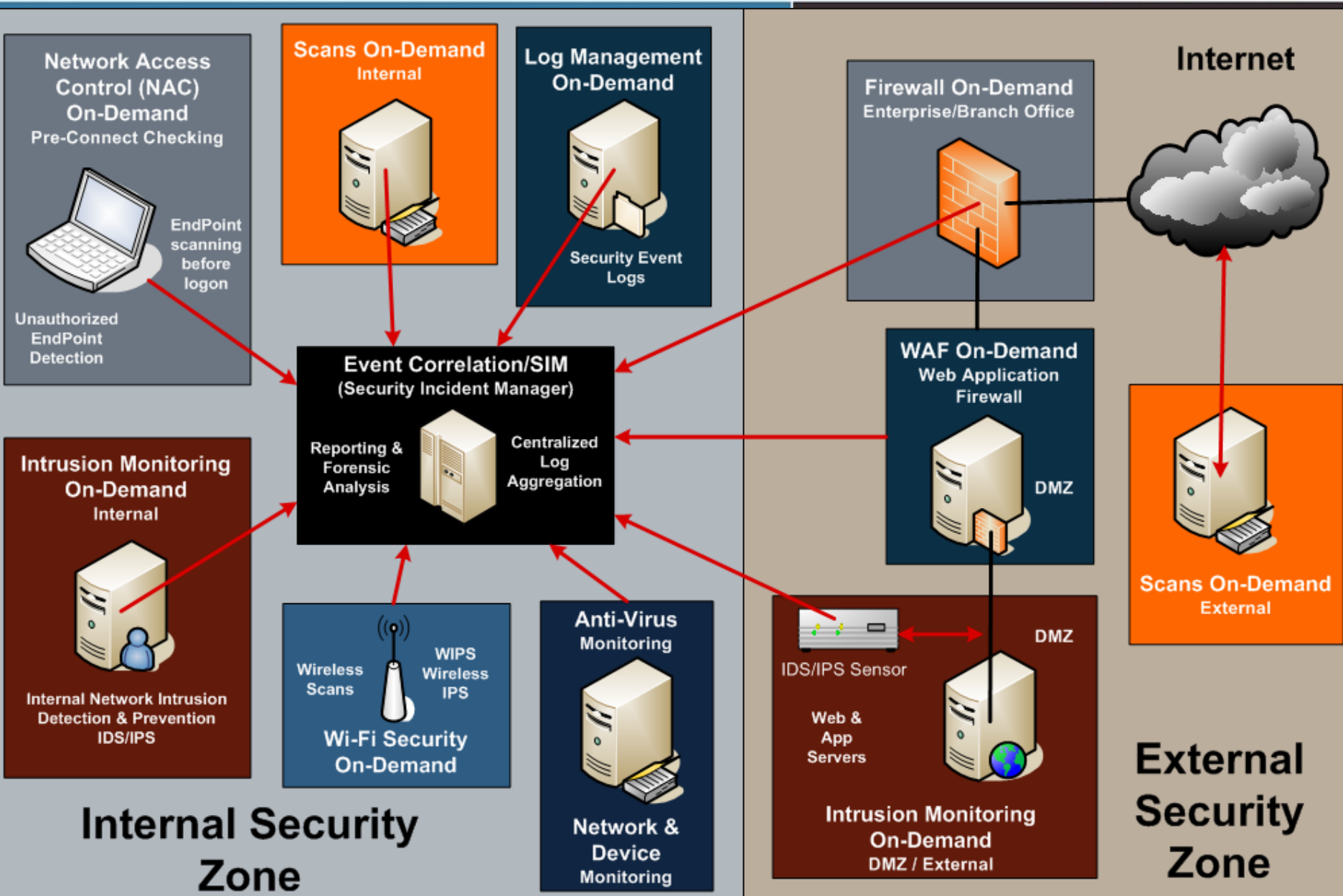
**3rd Generation
2008 -**

- **Knowledge, Training, & Experience**
 - Specialized Security Knowledge
 - Product Experience (Best Practices)
 - Speed time to Full Deployment
- **Staffing**
 - 7x24x365 Coverage for Monitoring & Alerting
- **Cost – Lower total cost of ownership**
- **Improve Security Process & People (not just Technology)**
 - Automates critical manual & tedious tasks (patching, signatures, etc.)
 - Leverage Operational Framework for Incident Triage & Response
- **Improve Return On Security Investment**
 - Typically costs 3-5 times or more to maintain a technology solution compared to the cost of the purchase

- **What Does “Management” Mean to You?**
- **Outsourcing vs. Software as a Service (On-Demand)**



Security Architecture Model



- **Deployment**

- Increase the speed & ease of deployment
- Plug into a pre-built security Platform (Utility Model)
- Minimize Disruption, Avoid being the technology Guinea Pig

- **Operations**

- **Best practices Management**
 - Leverage pre-built config in Tuning, Management, & Operations
 - Experts can help you define & implement your security policy
- **Staffing - Augment IT staff with subject matter experts**
- **Alert Triage - Accurately & efficiently differentiate between Security events vs. Security incidents**
- **Response - 7x24 Security Incident Handling & Mitigation**

1. **Training - Specialized Security Skills** required to monitor, evaluate, investigate potential security incidents, limit IT turnover expense
2. **Lack of Internal Staffing** for 7x24 monitoring, technology management, etc.
3. **Cost/Expense** – It’s fun to learn the new toys & cool to own all the technology, but who’s going to maintain, tune, and monitor?
4. **Provide guidance** in managing security incident response process and response protocols
5. **Augment your Computer Incident Response Team** with security professionals that can consult with you in the event of a real incident
6. **Service Level Agreements** – That can set written standards for appropriate response
7. **Mitigate Risk** – As a part of your Risk Management Program
8. **Utility Model** – Infrastructure already is built, just “plug in”
9. **Compliance** – More easily meet requirements for PCI, GLBA, etc.
10. **Reporting - Gain Visibility** to Events, investigations, responses, etc.

Thank You!

- **Peter Bybee, CISSP, CISA**
 - President/CEO
 - pbybee@securityondemand.com

- **For More Information**
 - www.securityondemand.com
 - info@securityondemand.com
 - 858-695-8676