SIEM

Understanding the Difference Between Noise & Intelligence

CSOHIMSS Spring Conference

OCLC Conference Center, Dublin, OH | May 20, 2016

Lynn R. Child

Education

AA – Tiffin University
BA – Ohio Northern University
MA – Bowling Green State University
MA – George Washington University

Experience

Principal Founder, President &
Chairman - CentraComm
CEO - Aardvark Inc.

Inc. 5000 AMERICA'S FASTEST GROWING PRIVATE COMPANIES

Certified WBENC Women's Business Enterprise

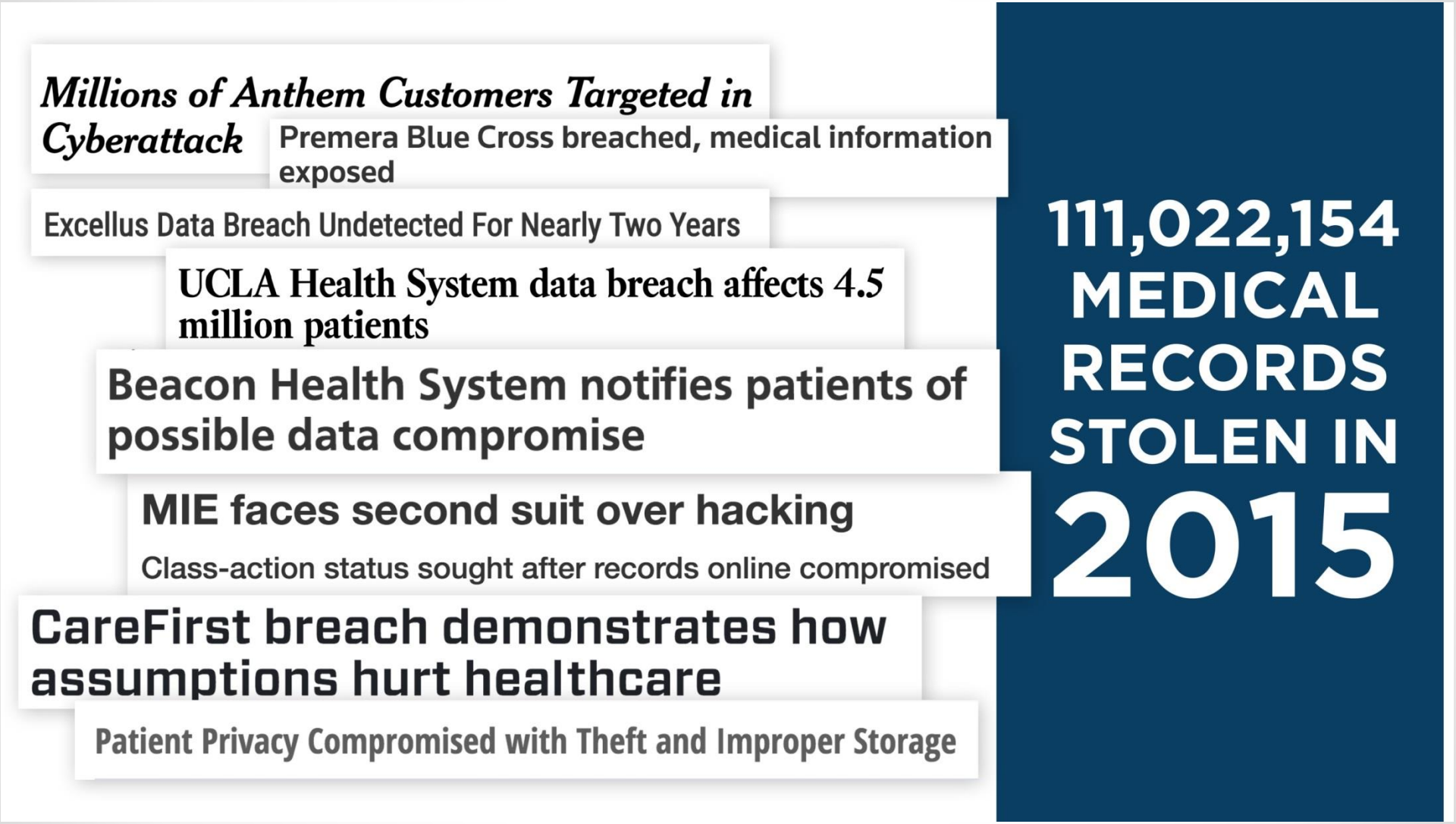
Joanne White

CIO
HIPAA Privacy & Security Officer

Wood County Hospital

Agenda of Topics

- Define Internet of Things (IoT)
- Explain Ways IoT Improves Healthcare
- Define Big Data Analytics
- Define SIM + SEM = SIEM
- Explain SIEM Components per Gartner
- Provide Business Cases for Use of SIEM in Healthcare
- Show Examples of SIEM at Wood County Hospital
- Q & A


Millions of Anthem Customers Targeted in Cyberattack
Premera Blue Cross breached, medical information exposed
Excellus Data Breach Undetected For Nearly Two Years
UCLA Health System data breach affects 4.5 million patients
Beacon Health System notifies patients of possible data compromise
MIE faces second suit over hacking
Class-action status sought after records online compromised
CareFirst breach demonstrates how assumptions hurt healthcare
Patient Privacy Compromised with Theft and Improper Storage
111,022,154 MEDICAL RECORDS STOLEN IN 2015

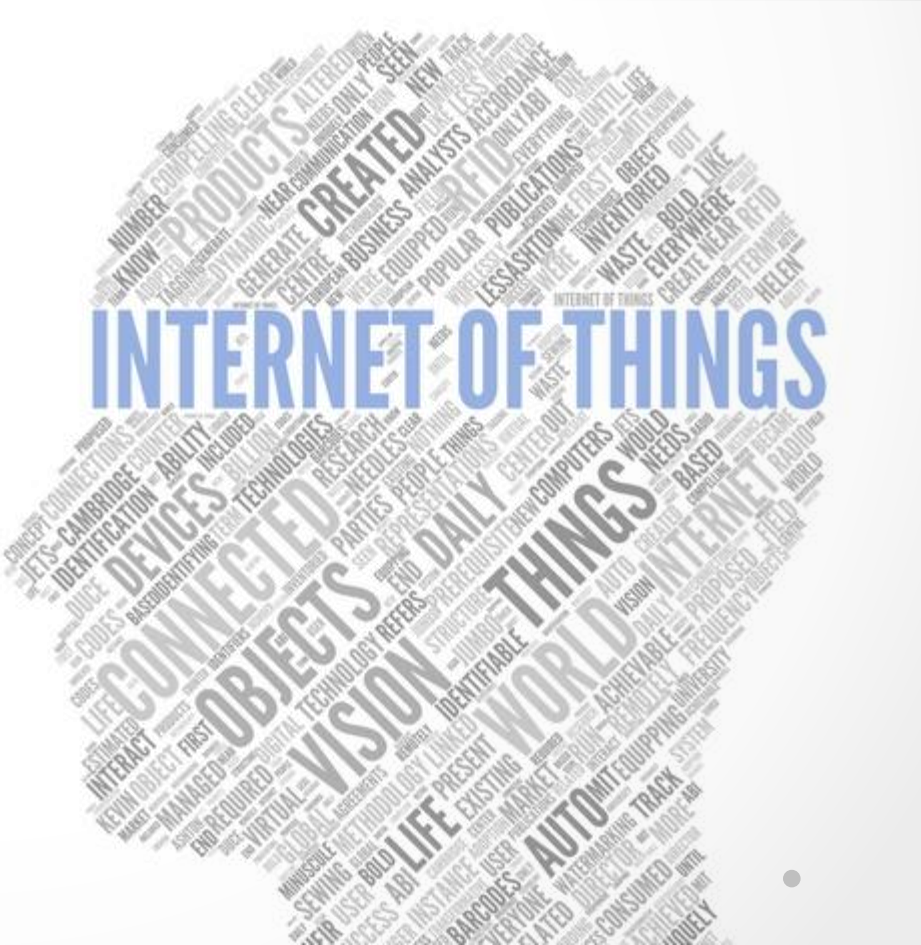
Population of

California – 38.8m
Texas – 27m
Pennsylvania – 12m
Illinois – 12m
Ohio – 11 m
Michigan – 10m

Combined

What is the Internet of Things

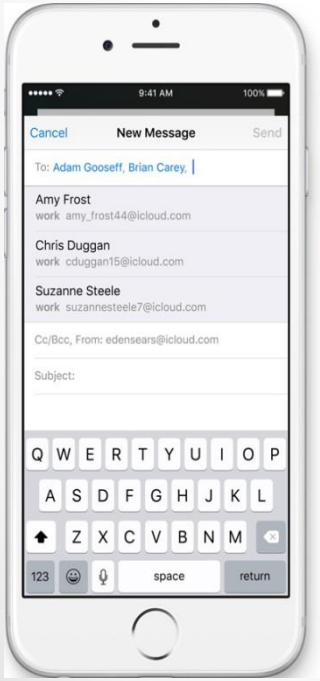
- **The Internet of Things** is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.

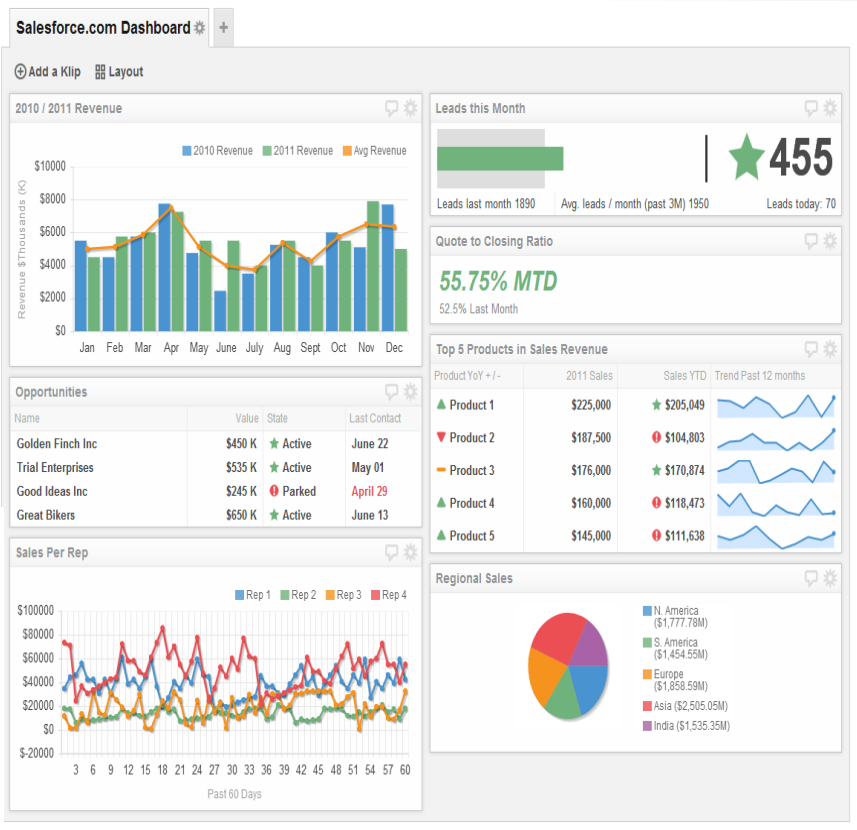


Some Examples of the IoT Devices

IFTTT

More Examples of the IoT Devices





Even Rail Cars Create Data

A Connected Society

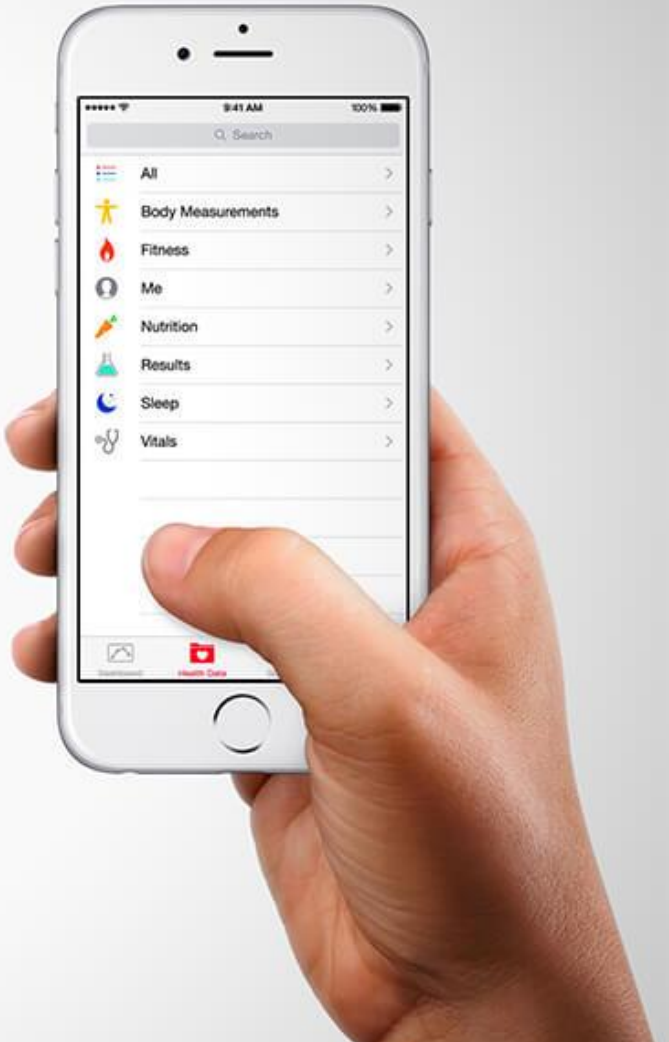
List of countries by IoT devices online per 100 inhabitants as published by the OECD* in 2015.

Rank	Country	Devices online	Relative size
1	South Korea	37.9	
2	Denmark	32.7	
3	Switzerland	29.0	
4	United States	24.9	
5	Netherlands	24.7	
6	Germany	22.4	
7	Sweden	21.9	
8	Spain	19.9	
9	France	17.6	
10	Portugal	16.2	
11	Belgium	15.6	
12	United Kingdom	13.0	
13	Canada	11.6	
14	Italy	10.2	
15	Brazil	9.2	
16	Japan	8.2	
17	Australia	7.9	
18	Mexico	6.8	
19	Poland	6.3	
20	China	6.2	
21	Colombia	6.1	
22	Russia	4.9	
23	Turkey	2.3	
24	India	0.6	

*Organisation_for_Economic_Co-operation_and_Development

IoT in Healthcare

IoT is the interplay between bedside monitors, smartwatches and fitness trackers, implanted medical devices, and any other object that transmits or receives a signal containing data that must be accessed or stored somewhere else.



Medical IoT Devices

Sources of Medical IoT Data

3 Ways IoT improves Healthcare

➢ Increase Operational Efficiency

- Track Patients
- Manage Inventory & Time
- Manage Equipment

➢ Improve Patient Care

- Incorporate Mobile Devices
- Access Data from Wearable Technologies
- Integrate Electronic Medical Records

➢ Support Leadership and Leverage Innovation

- Capture and Analyze Data
- Improve Performance and Quicken Innovation
- Enhance Time Dedicated to Patient Care and Building Strategies
- Improve Overall Operations

http://www.himss.org/News/NewsDetail.aspx?ItemNumber=40536

IoT Creates Big Data - Big Data Comes from Machines

Volume | Velocity | Variety | Variability

GPS,
RFID,
Hypervisor,
Web Servers,
Email, Messaging,
Clickstreams, Mobile,
Telephony, IVR, Databases,
Sensors, Telematics, Storage,
Servers, Security Devices, Desktops
Medical Appliances & Devices

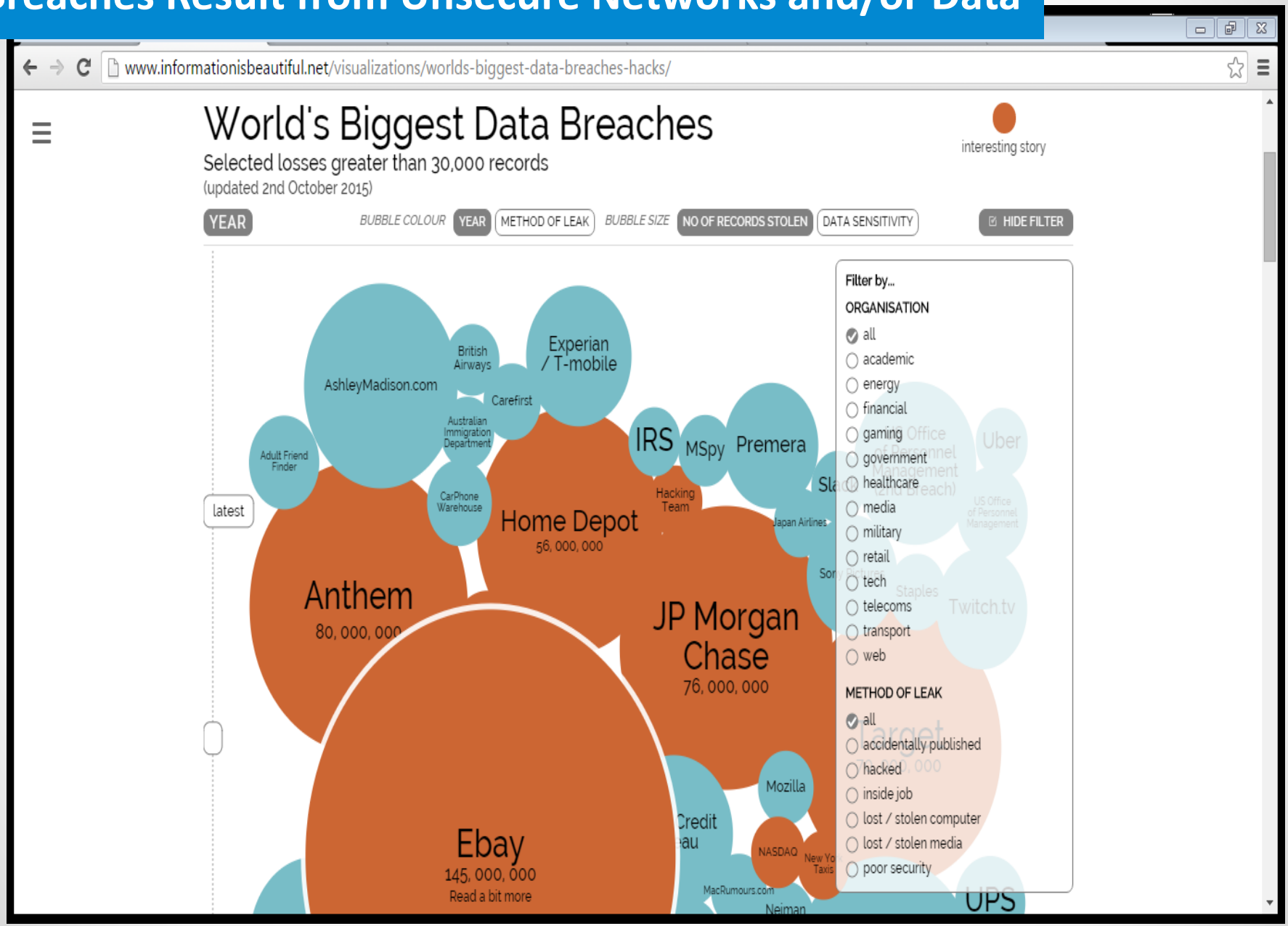
Value comes from Big Data Analysis

Big data analytics is the process of examining large data sets containing a variety of data types -- i.e., big data -- to uncover hidden patterns, unknown correlations, market trends, customer preferences and other useful business information.

All of this data must be secure!

http://searchbusinessanalytics.techtarget.com/definition/big-data-analytics

Breaches Result from Unsecure Networks and/or Data



SIEM: An effective security tool

Security information and event management **(SIEM)** is an approach to security management that seeks to provide a holistic view of an organization's information technology (IT) security.

http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM

SIM + SEM = SIEM

SIM - long-term storage as well as analysis and reporting of log data
SEM - real-time monitoring, correlation of events, notifications and console view
SIEM - real-time analysis of security alerts generated by network hardware and applications

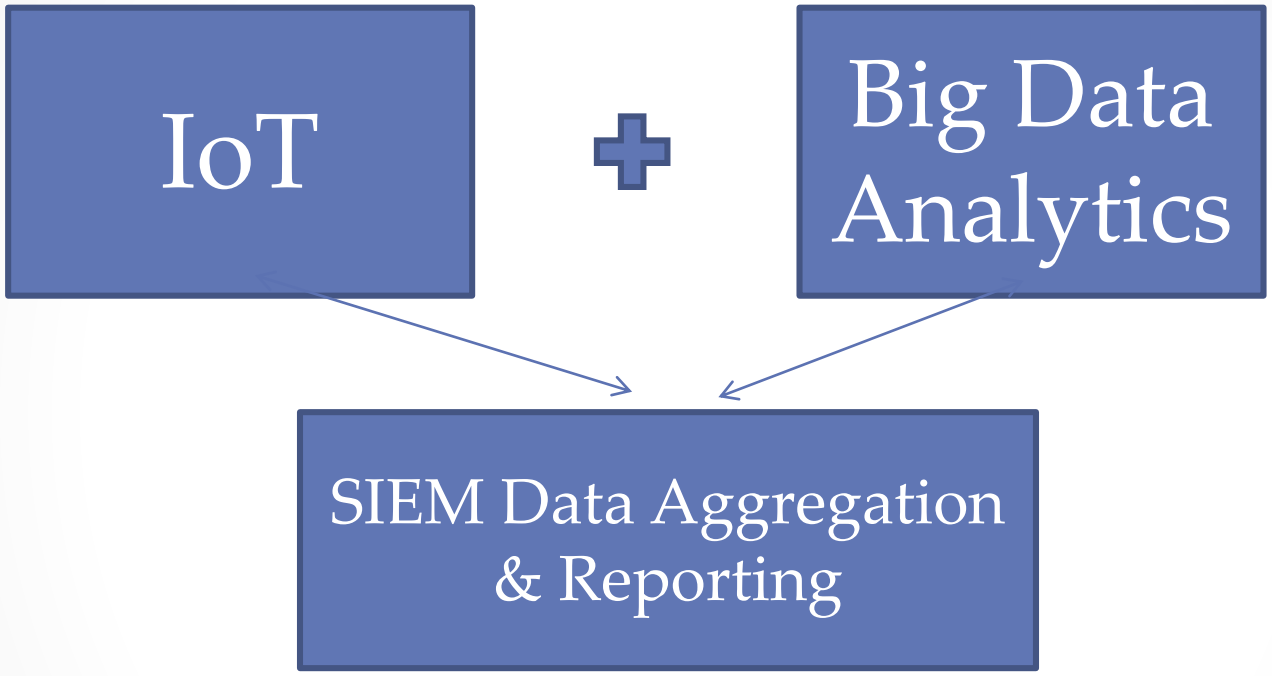
https://en.wikipedia.org/wiki/Security_information_and_event_management

SIEM Components

- Gathers, analyzes and presents information from network and security devices
- Includes identity and access-management applications
- Incorporates vulnerability management and policy-compliance tools
- Supports operating-system, database and application logs
- Includes external threat data

https://www.gartner.com/doc/480703/improve-it-security-vulnerability-management

Turning Noise into Intelligence



Better, Quicker, Safer & More Effective
IT & Business Decision Making

Data Powers Business Decisions

Real-time transaction volume across all tiers.

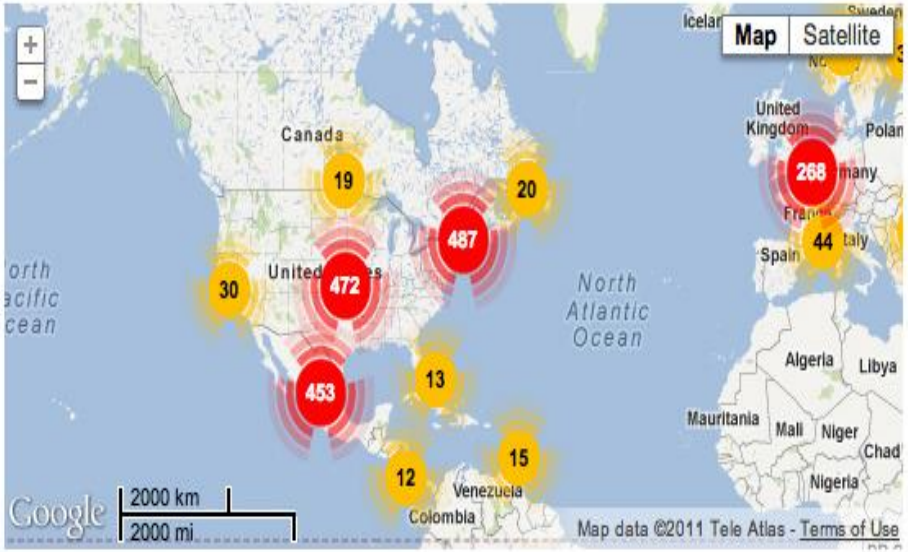
Real-time average shopping cart values.

Real-time concurrent users browsing website.

60

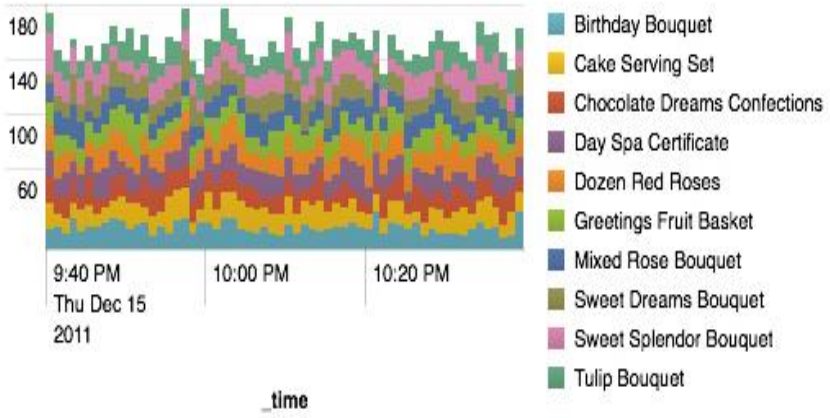
Visitor Location

3m ago



Top Items Sold

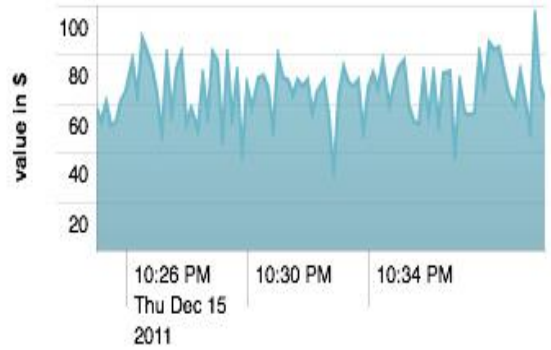
5m ago



Abandoned Baskets

5m ago

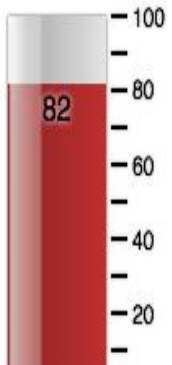
Average value of abandoned shopping carts on website via logout or expired sessions over the last 60 minutes.



% Coupon Usage

real-time

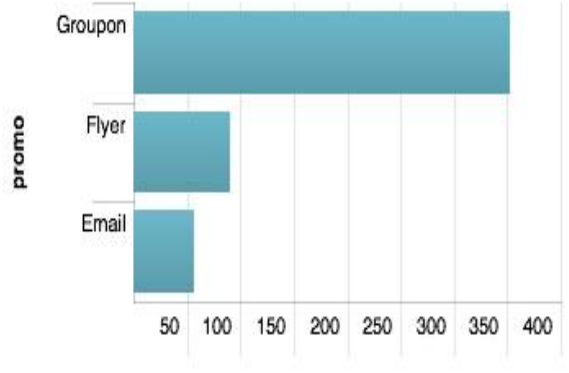
Real-time percentage of shoppers using coupons vs paying full price.



Top Promotions

3m ago

Promotional program popularity over the past 24 hours.



Wood County Hospital Concerns

- Networks…and threats are becoming more complex
- IT security roles are becoming increasingly specialized / minimal staff
- Continuous monitoring of inventories and vulnerabilities is the new norm
- Even smaller healthcare facilities must correlate and analyze big data
- Most aren't prepared to survive a cyber attack

Wood County Hospital Desired Solution

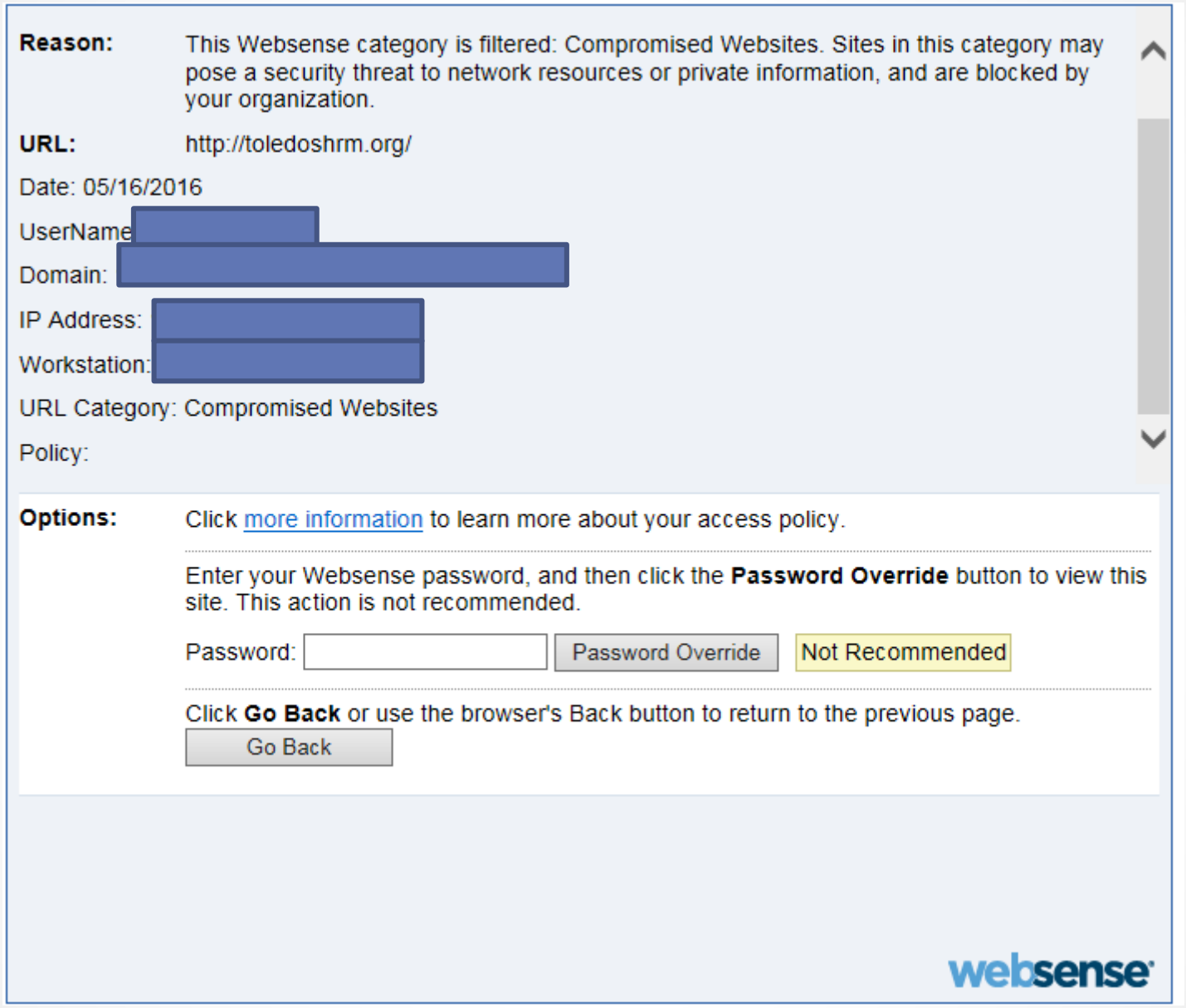
- Cloud-based SIEM based on Elasticsearch, big data and machine learning
- Monthly Vulnerability Assessments
- Personalized service managed by a dedicated security engineer
- Continuous monitoring, analysis and correlations of events, logs and user information
- Custom alerts, response management and reporting
- Filter out false-positive incident alerts
- Ensure proactive detection and response to threats, intrusions and attacks

Wood County Hospital Solution External

- Cloud-based SIEM 24x7 continuous monitoring of external threats
- Currently includes logs from the firewalls and Forcepoint
- Forcepoint includes url filtering, email encryption, DLP, and malware

Problem Detected

- Our training department complained that a website was blocked
- The reason was found in our log
- The owner of the website was unaware they had 41 malicious links on their site.
- We were able to send them a copy of the log to take corrective action
- Note: To date they have not resolved these issues


Reason:
This Websense category is filtered: Compromised Websites. Sites in this category may pose a security threat to network resources or private information, and are blocked by your organization.
URL:
http://toledoshrm.org/
Date: 05/16/2016
UserName
Domain:
IP Address:
Workstation:
URL Category: Compromised Websites
Policy:
Options:
Click more information to learn more about your access policy.
Enter your Websense password, and then click the Password Override button to view this site. This action is not recommended.
Password:
Password Override
Not Recommended
Click Go Back or use the browser's Back button to return to the previous page.
Go Back
websense

ACE Insight Report
Generated **2016-02-25** at **7:40:51 PM UTC Input:** **http://toledoshrm.org**

Analysis for: http://toledoshrm.org

Link detection summary:

Shows the actual name and type of the security threat.

Threat Name	**Threat Type**	**Description**
Injection.Black_SEO.Web.RTSS	Injection	Black_SEO

Shows the total number of links and the number of links that point to malicious destinations. **Total Number of Links 250** **Malicious Links 41**

URL link detection Review analysis of all links within the target URL or IP address, including detailed link properties

Threat Severity	**Real-time Security Analysis**	**URL**
Medium	Compromised Websites	http://toledoshrm.org/images/Ads/11/11-PWMGlogo_TAHRAHOMEPAGE.jpg
Medium	Compromised Websites	http://creativeindoorplay.co.uk/config.php?page=70-412.html
Medium	Compromised Websites	http://socialmediarodeo.com/config.php?page=/comptia/220-801-ex
Medium	Compromised Websites	http://creativeindoorplay.co.uk/config.php?page=1Z0-051.html
Medium	Compromised Websites	http://www.toledoshrm.org/documents/meetings/DianaBioasof

Problem Detected

- Another case where the SIEM log alerted us to take corrective action
- We received an email alert and phone call
- This server is located at a hosting facility

Corrective Action

- The log identified Bedep Malware on one of our Terminal Servers
- We ran Sophos on it but contained rootkit and would not boot in safe mode
- The server had to be re-imaged

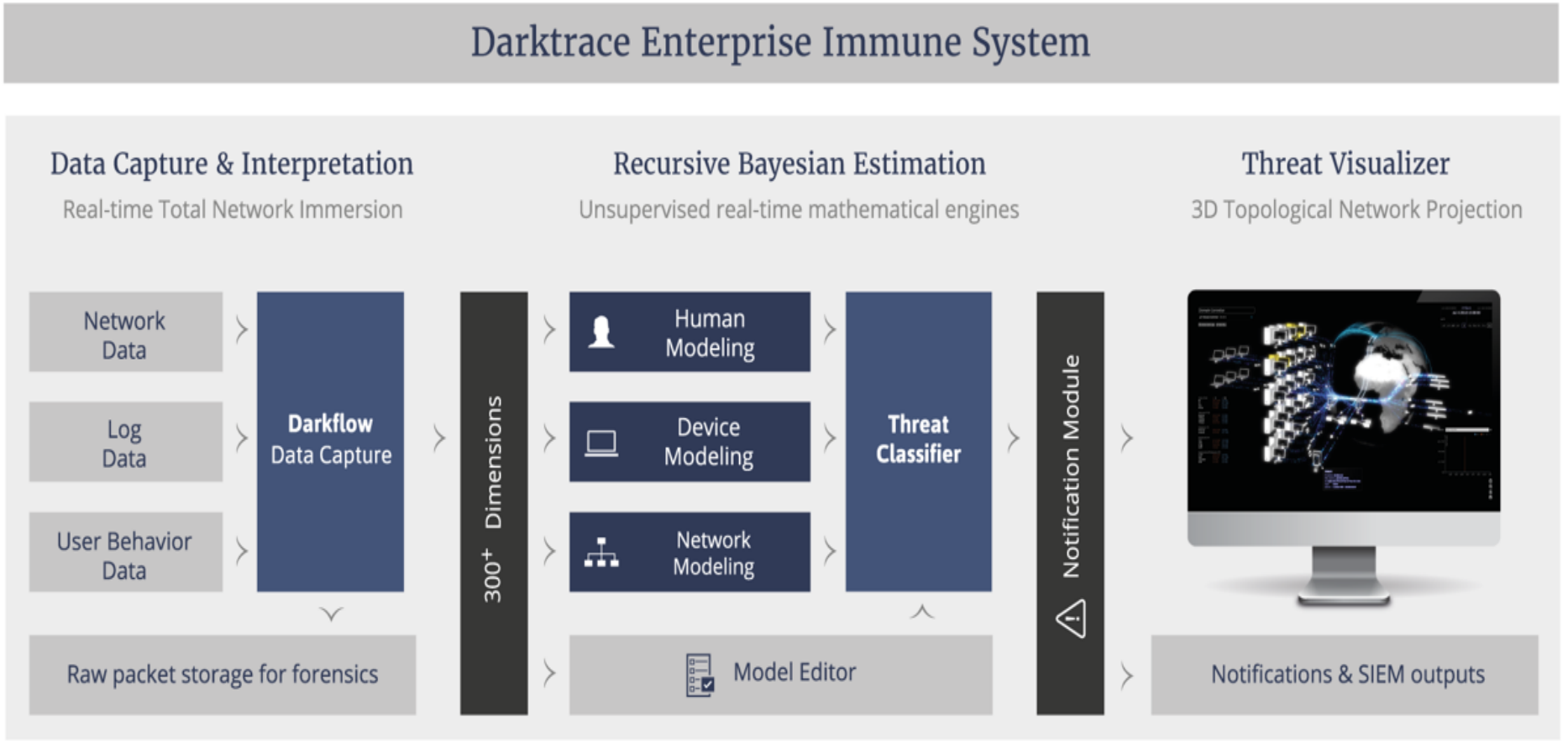
Incident Type: Incident
Systems Impacted: whcts3
Description:
The system whcts3 (xx.xx.xx.xx) appears to be infected with Bedep Malware. We have evidence of traffic to known malware control sites on the internet subsequent to a visit to an exploit page.
IDS Signatures hit:
Bedep HTTP POST CnC Beacon
Possible Compromised Host Sinkhole Cookie Value Snkz
Possible Bedep Connectivity Check
Possible Angler EK Payload June 16 2015 M2
Possible Angler EK Landing URI Struct Jul 15 M1 T1
Possible Angler EK IE DHE Post M3
Possible Angler EK Flash Exploit June 16 2015 M1
Angler or Nuclear EK Flash Exploit M2
Angler or Nuclear EK Flash Exploit (IE) Jun 16 M1 T2
Angler EK Landing URI Struct Oct 12

Recommended Actions:
The system whcts3 should have AV scanners run on it, or it should be re-imaged depending on your virus policies.

Wood County Hospital Solution Internal

- Cloud-based SIEM 24x7 continuous monitoring of internal threats
- Darktrace appliance on-site for POC

Technology Architecture



Threat Intelligence Report

Darktrace has detected an internal device exhibiting very unusual behaviour. Firstly, it remotely controlled an external device which is a new destination for the network. While in remote control, the device downloaded an anomalous amount of data. Following this activity, the internal device was observed broadcasting an anomalously high level of traffic on a particular channel that attackers have used to observe and exploit network and device credentials. Darktrace recommends investigating to see whether or not these activities are related. If they are, they could be evidence of malicious behaviour.

A device is sending unencrypted messages to an external network, messages which contain sensitive information about the configuration and security of the network. If an attacker was able to intercept these communications, then they would have had little difficulty accessing this information and potentially exploiting it. The company may wish to use a more secure communications channel when sending information externally.

Darktrace has observed a device downloading software that enables one device to take remote control of another. This device later gained remote control over an internal device. The company may wish to confirm that the download and use of this software was expected and authorised, as the software could be leveraged by a malicious actor to move laterally through the network or to harvest data.

Incident Details

1. External RDP:

An internal device has remotely controlled and downloaded data from an external network for purposes that are not clear. No other device has connected to this external network; this is the only connection observed during the reporting period. Interestingly the source has not made any other remote desktop connections, to other external or internal devices.

Figure Two illustrates the spike in sustained internal Link-Local Multicast Name Resolution (LLMNR) broadcast activity following the RDP event which is signified by the orange dot.

LLMNR is used to resolve host names on a subnet; a host will broadcast a name query of a device it is trying to reach to all other devices on the subnet. Malicious attackers listen for this traffic and respond with their own device name as the answer. As a consequence, the source host will then initiate a connection to the attacker device passing authentication credentials.

Several open source and well documented tools such as the Metasploit framework and responder provide command interfaces to conduct these attacks. It is possible such utilities may have been brought across from the remote connection. Analysis of the packet streams indicate that a significant amount of broadcast traffic related to queries with no responses seen from this host. As such it is unlikely to relate to this specific attack. However, there remains the possibility that the remote connection may have seen attacker tools transferred and if this was not an expected activity it should be investigated.

The detection also serves as an example of how Darktrace identifies anomalies in the devices activity patterns and the combination of these activities that raise a devices threat profile.

3 Business Cases for SIEM in Healthcare

1. Streamline compliance reporting
2. Detect incidents that would otherwise not be detected
3. Improve the efficiency of incident handling activities

http://searchsecurity.techtarget.com/feature/Three-enterprise-benefits-of-SIEM-products

1) Streamline Compliance Reporting

- **Centralized Logging of Events:**
  - Transfer Log Data to SIEM Server by Many Hosts
  - Create Rich, Customized Reports based upon Data Aggregation
  - Create Rich, Customized Reports from Each Host that are Granular
  - Converts Operating Systems, Applications and Other Software that may be Proprietary into Single, Readable Report
  - Incorporates Built-In Support for Compliance Efforts such as HIPAA, PCI, Sarbanes-Oxley (SOX), etc.
  - Streamlines Ability to Meet Compliance Demands of Various Entities

2) Detect Hidden Incidents

- **Highlights Security Activity on Hosts that Do Not Have Built-In Incident Detection Capabilities**
  - Observation Occurs
  - Audit Logs Created
  - No Ability to Analyze to Detect Malicious Activity
  - Often Can Alert Someone but Cannot Proactively Address
- **Correlates Events Across Hosts**
  - Aggregates Data from Many Hosts Across the Enterprise
  - Sees Attacks from Different Hosts and can Reconstruct the Series of Events
  - Analyzes Events from Various Hosts to Determine the Nature of the Attack and Whether the Attack was Successful or Not
  - Remedial Action May Commence Immediately

3) Improve Efficiency of Incident Handling

- Provides a Single Interface for Viewing all the Security Log Data from Many Hosts/Sources
- Creates Efficiency in Handling Attacks
- Increases Speed of Incident Containment
- Reduces the Amount of Overall Damage
- Examples:
  - Rapidly ID Hosts Affected by an Attack
  - Quickly ID the Attack Route through the Enterprise and Remediate
  - Speedily Attempts to Stop Attacks While in Progress
  - Effectively Contains Compromised Hosts

Other Aspects of SIEM

- Does Not Take the Place of Enterprise Security Controls, i.e., IDP, Anti-virus, Firewalls, etc.
- SIEM uses Data Logs Generated from Other Pieces of Software and Does Not Generate its Own Data Logs
- SIEM has the Ability to Attempt to Stop an Attack that is Detected While the Attack is Still in Progress by Communicating with Other Network Devices such as Firewalls
- SIEM can Ingest Threat Intelligence Feeds from Trusted External Sources
- SIEM can Act to Terminate Connections or Disrupt Malicious Host Interaction with the Network to Prevent an Attack

Questions & Answers

Thank You for the Honor and Privilege of Presenting Today as We All Work Together to Keep our Worlds Safer.

• • •

Joanne White – Wood County Hospital
whitej@woodcountyhospital.org; 419-601-0711

Lynn R. Child – CentraComm
lchild@centracomm.net; 419-421-1284