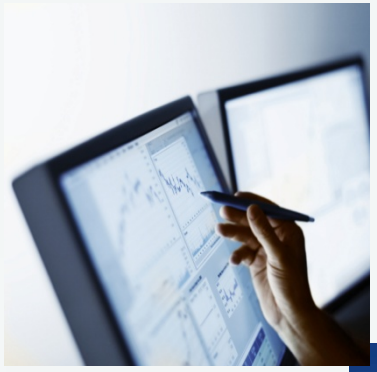
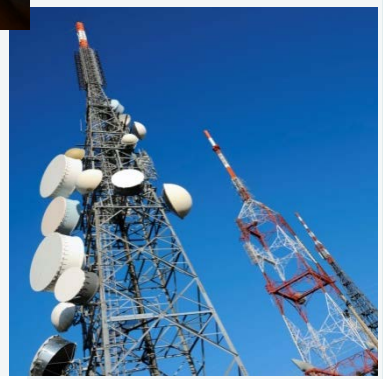
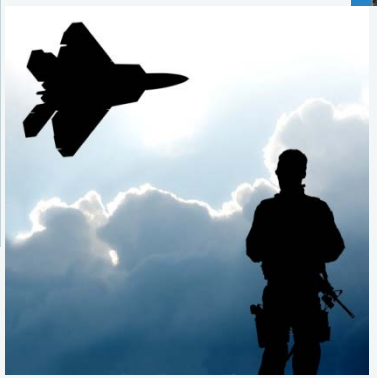






SENSAGE

Massive-Scale Event Data Collection in Threat Management for Government Agencies

Joe Gottlieb

President and CEO, Sensage

Joe Gottlieb

Joe is well known as an enterprise security thought leader. A respected technology veteran, Joe helped Sensage build and rapidly expand the web's first open security intelligence community, as well as increase consecutive quarterly revenues. Prior to becoming president and CEO in 2011, Joe led all marketing and business development activities, building partnerships and developing new opportunities to drive growth.

Joe joined Sensage from McAfee, where he was Vice President of Corporate Strategy and Technology Alliances. He brings a proven track record of innovative business strategies, including building the Security Innovation Alliance partner ecosystem for the industry's first open security management platform. Prior to McAfee, Joe held executive positions leading product and business strategy for such companies as Nokia and META Group.

CREDIT CARD FRAUD

PROBLEM:

1) RECURRING
2) EVOLUTIONARY
3) COSTLY

SOLUTION:

1) BIG DATA MASTERY
2) SEMI-AUTOMATED FILTERING
3) EVOLUTIONARY PROCESS

STATUS:

1) EXPECTED
2) CONTROLLED

A SIMPLE COMPARISON…

INFORMATION SECURITY

PROBLEM:

1) RECURRING
2) EVOLUTIONARY
3) COSTLY

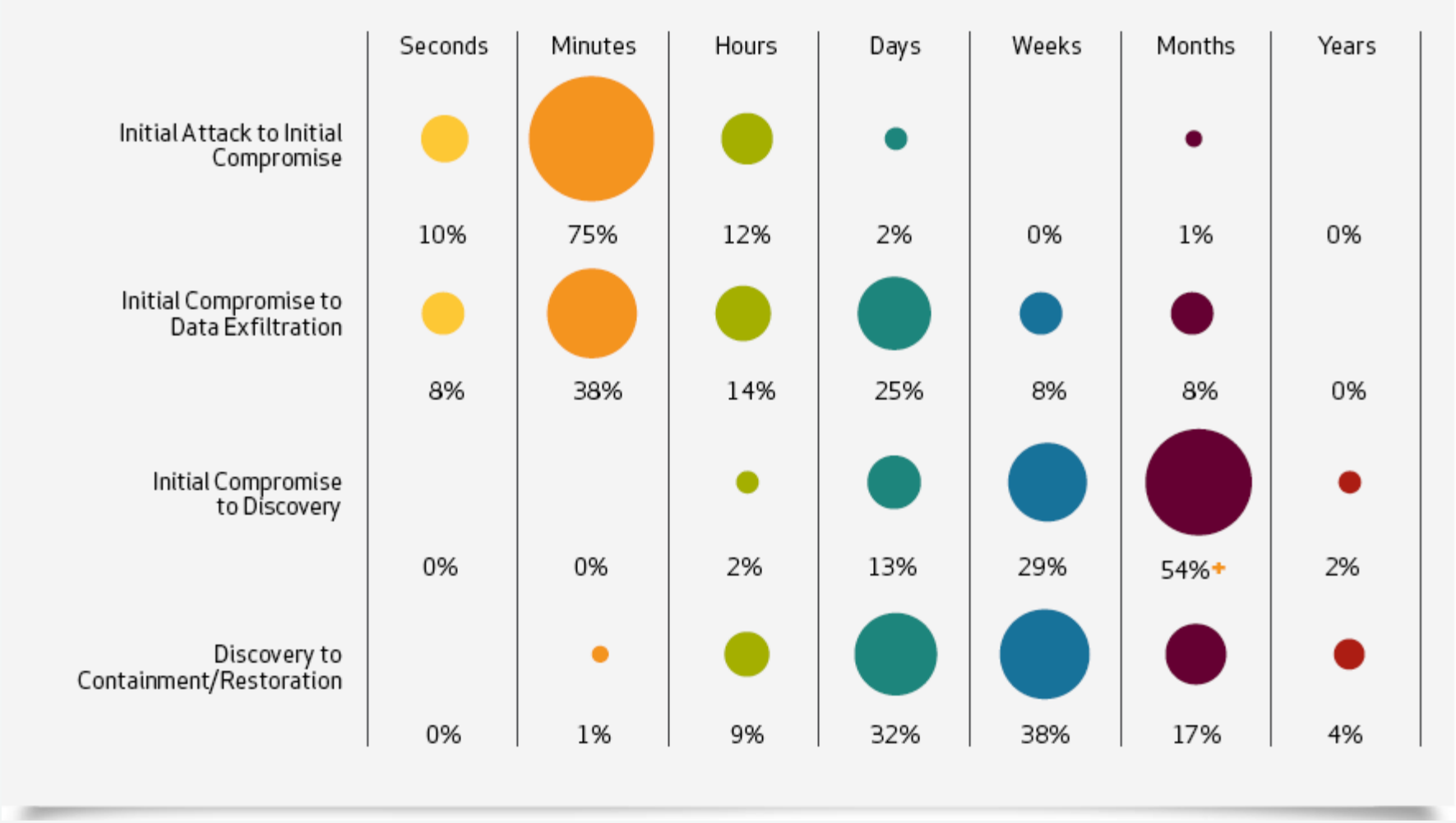
SOLUTION:

1) WEAK/INCOMPLETE DATA MANAGEMENT
2) REAL-TIME FAÇADE + MANUAL PROBING
3) HEROIC CRAFTSMEN

STATUS:

1) INCREASING THREAT
2) BLEAK PROGNOSIS

Why Information Security is So Challenging… It's Not Happening in Real Time



SOURCE: Verizon Business, *2012 Data Breach Investigations Report*

SENSAGE

…Even More Challenging for the U.S. Government…

10110010010110011000110100
11111101110001100111011001 1
11010110111101111100001100 0
11101110001110111011001100 10
11010001101111000100110110
11001011010001101111000100
10011110110001000101100100
10110010011110110001000010
01001110111101100100101

More Users
More Diversity

Biggest Target

Highest Degree of Operational Complexity

With More Compliance Pressures and Scrutiny

U.S. Securities and Exc

Division of Corporation Finance
Securities and Exchange Commission

CF Disclosure Guidance: Topic No. 2

Cybersecurity

OPINION | July 19, 2012, 7:15 p.m. ET

Taking the Cyberattack Threat Seriously

In a future conflict, an adversary unable to match our military suprem might seek to exploit our computer vulnerabilities here at home.

Article | Comments (270)

Email

By BARACK O

Last month I intelligence a carrying indu several state fall ill.

Concept of Operations (CONOPS)

FedRAMP SM

Office of Management

About | OMBlog | The Budget | Management

REGULATION & INFORMATION POLICY

About OIRA

Information Policy

Federal Collection of

Information Policy

tandards Policy

nformation Quality Government-wide Initi

MB-Specific Information Quality Web pa

nformation Policy Documents

NISTIR 7359

Information Security Guide For Government Executives

Pauline Bowen
Elizabeth Chew
Joan Hash

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

January 2007

er / Vol. 76, No. 198 / Thursday, October 13, 2011 / Presidential Documents 63811

Presidential Documents

Executive Order 13587 of October 7, 2011

Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information

By the authority vested in me as President by the Constitution and the laws of the United States of America and in order to ensure the responsible sharing and safeguarding of classified national security information (classified

FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) IMPLEMENTATION PROJECT

Protecting the Nation's Critical Information Infrastructure

Our Vision

To promote the development of key security standards and guidelines to support the implementation of and compliance with the Federal Information Security Management Act including:

Data Proves It

855 incidents

81% utilized some form of hacking

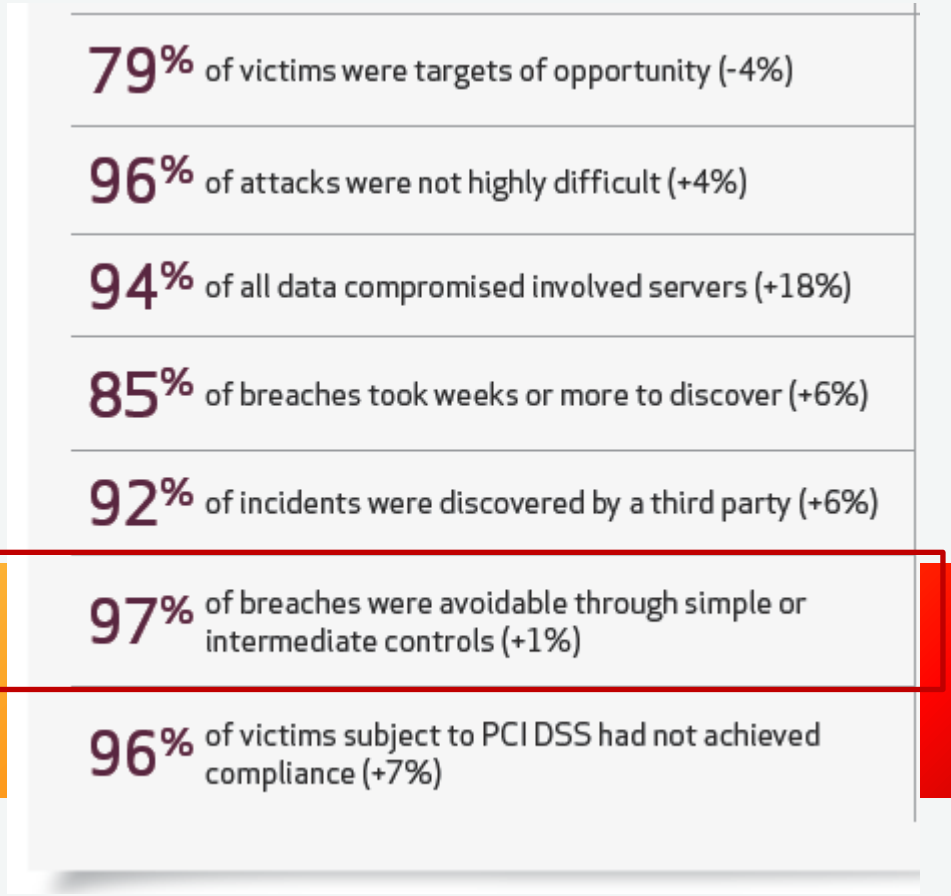
69% incorporated malware

174 million compromised records

SOURCE: Verizon Business, *2012 Data Breach Investigations Report*

SENSAGE

97% of breaches were avoidable…



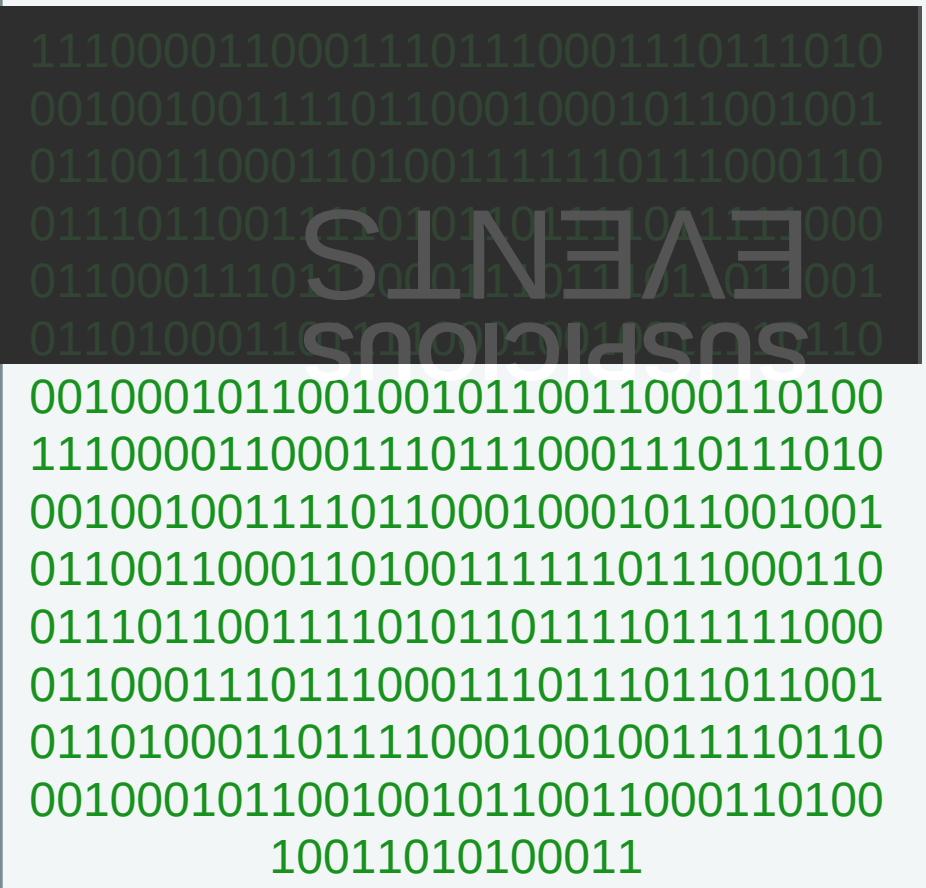
SOURCE: Verizon Business, *2012 Data Breach Investigations Report*

SENSAGE

Problem:
Finding & Understanding Suspicious Events Buried in Big Data

In security monitoring, isolating the signal from the noise now requires big data digestion, storage and analysis

The Other Guys



Sensage

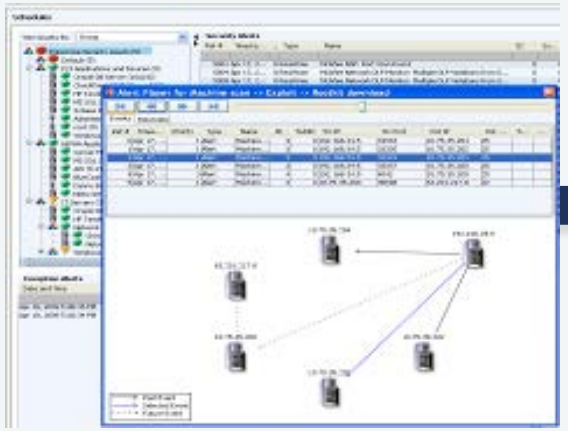
Sensage Unique Capabilities

Massive-scale security event data collection, aggregation, storage and analysis

- Automated auditing, threat management, continuous monitoring, forensic investigation to broad user community
- Columnar Database with strong data compression to reduce the amount of security event storage required
- Complex aggregation and statistical analytics across all user, system and network activities
- Role-based access controls, automated alerting functions, historical querying, bi-directional interoperability with real time event data correlation

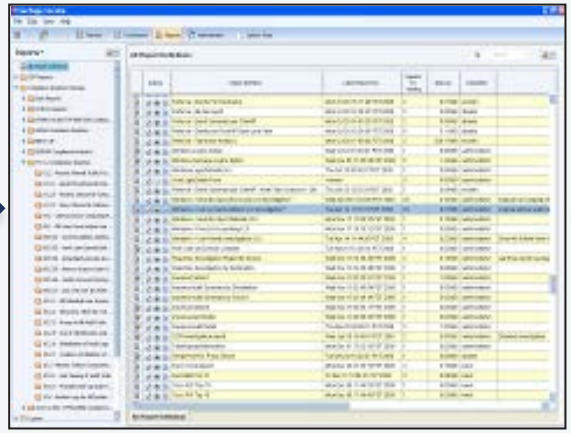
Sensage Solution – Analytics for Greater Security Intelligence

Real-time Monitoring



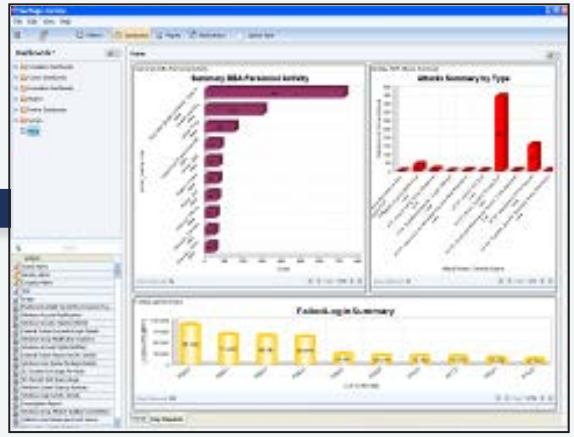
- Powerful real-time correlation
- Scenario-based analysis
- Integrated with historical correlation
- Easy to create and deploy template-based rules
- Dozens of common out-of-the-box rules

Forensic Investigation



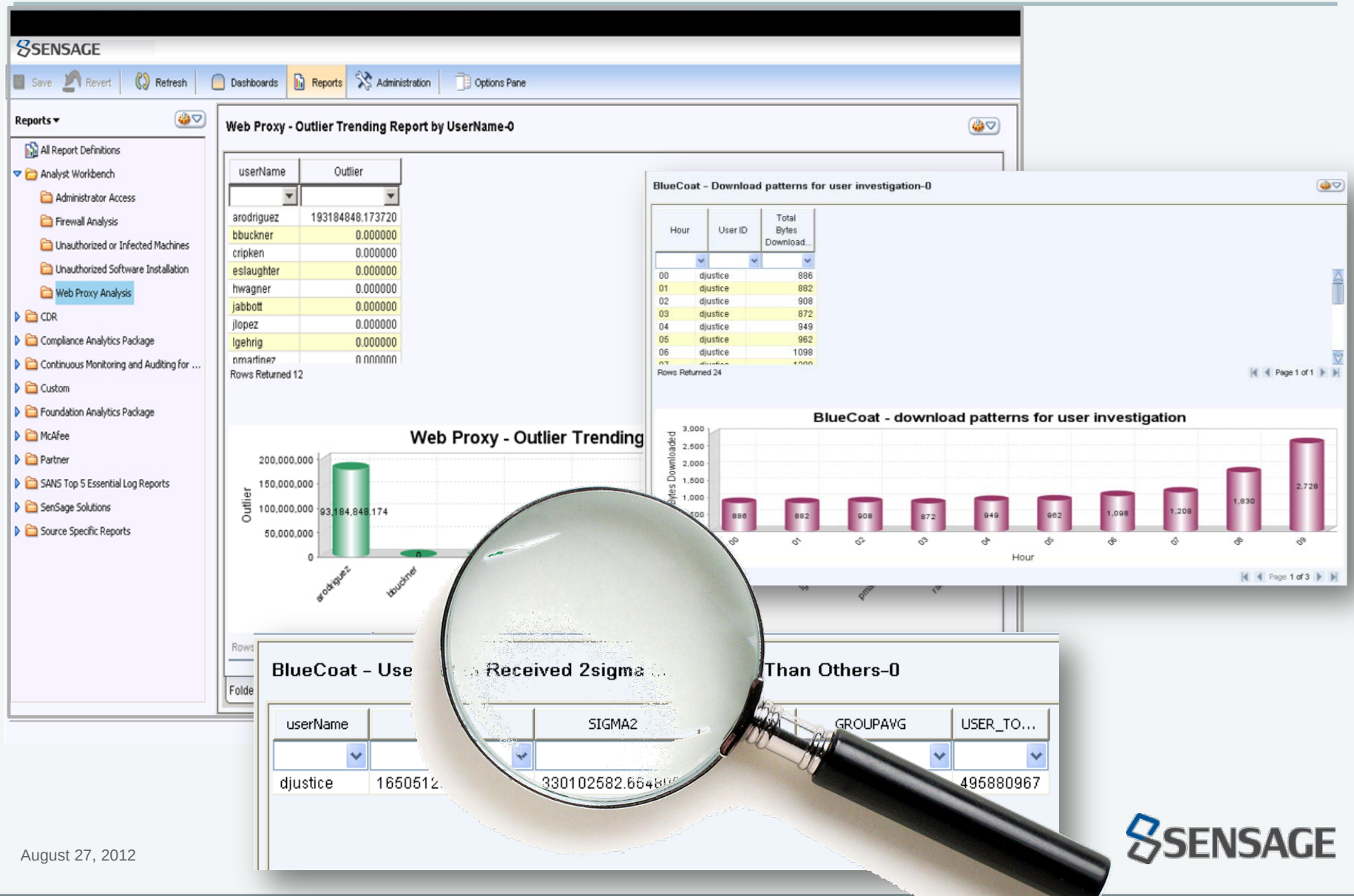
- Ability to analyze and report on years worth of data
- High-speed filtering and searching
- Wizard driven report creation
- Automated drill-down for forensic investigation
- 100s of out-of-the-box reports

Compliance Reporting



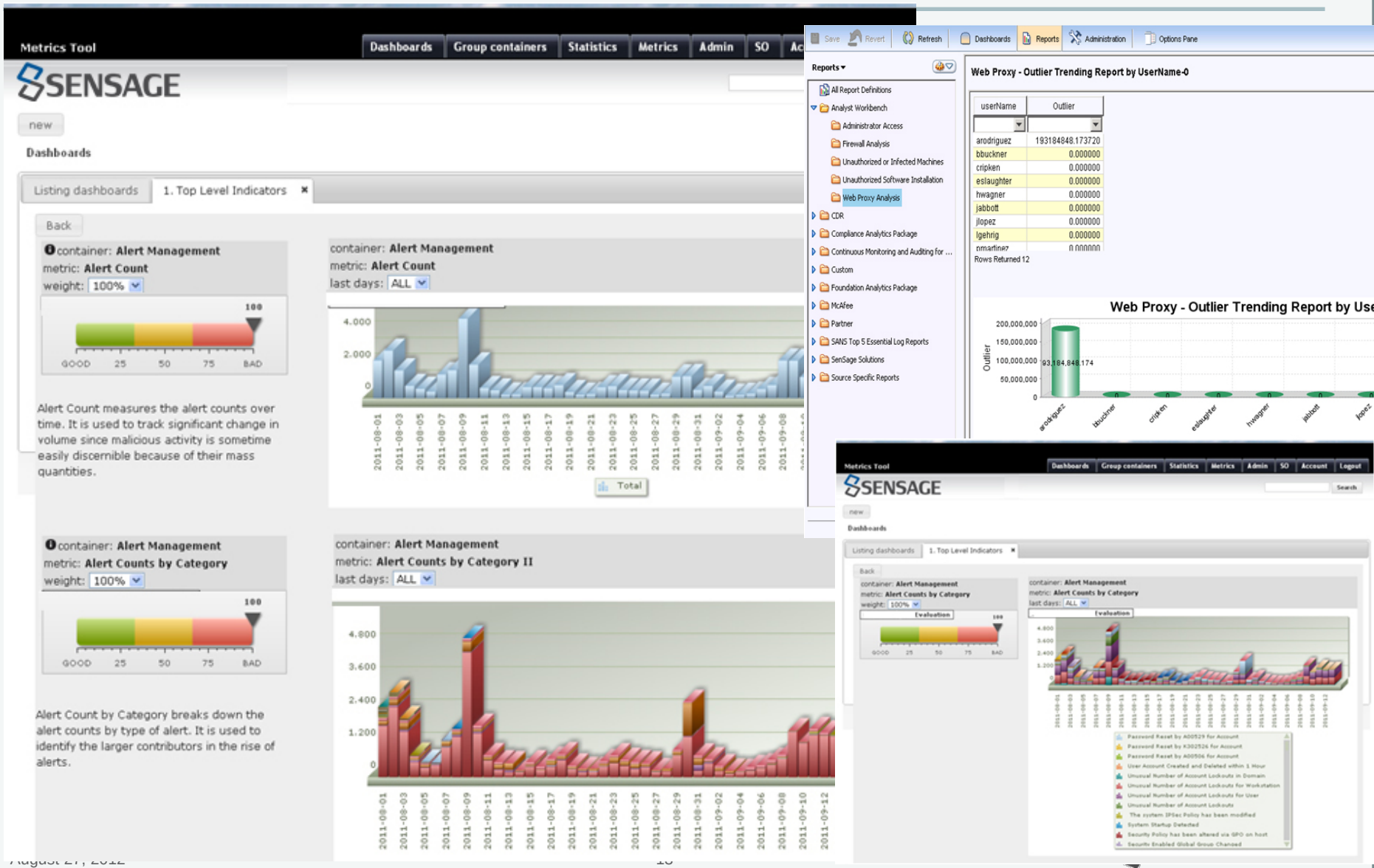
- High-level graphical aggregation reporting
- Easy to show and analyze trend data
- Variety of graph types
- Business analyst friendly interface
- One-click drill down from high-level to report details

Big Security Data: Advanced Statistical Analytics



SENSAGE

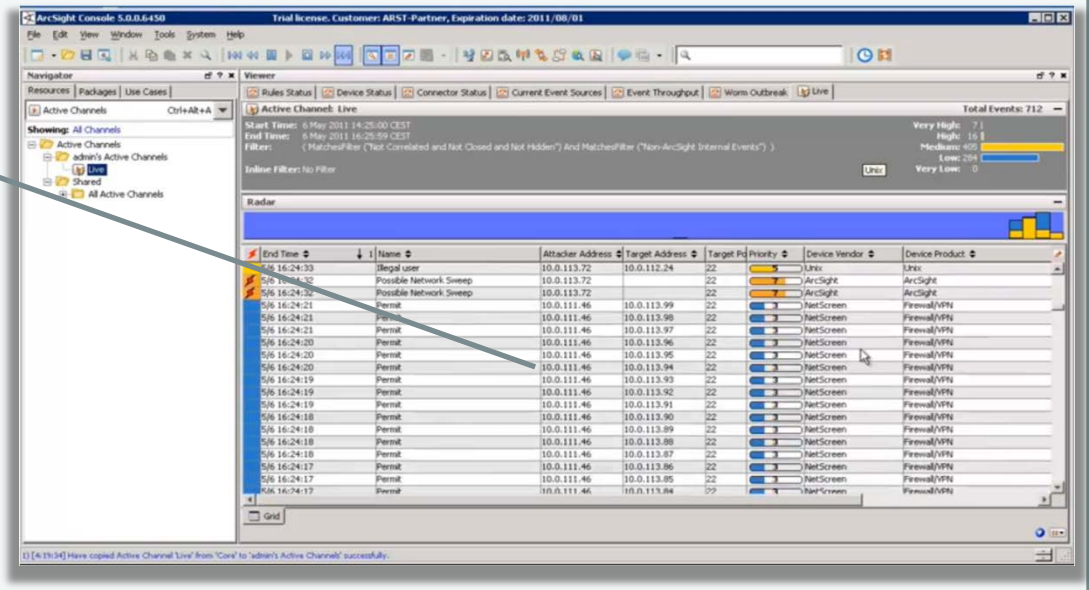
Correlating Support Ticketing with Network Activities



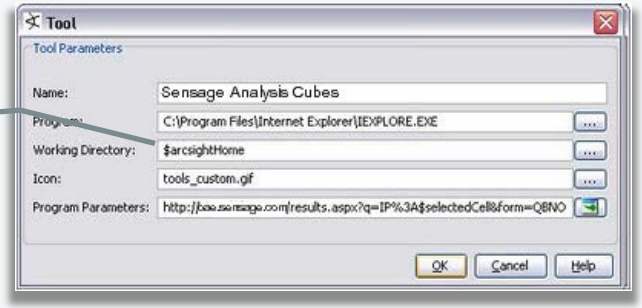
SIEM Extension for ArcSight

- Bi-directional interoperability lets ArcSight users drill into historical data “underneath” real-time alerts

- An ArcSight real-time correlation rule detects malicious activity
- The Alert shows up in the ArcSight Active Channel View, where analyst right-clicks on Attacker-Address/Target Address column and selects Sensage Forensic Drill-down Wizard from Tools menu



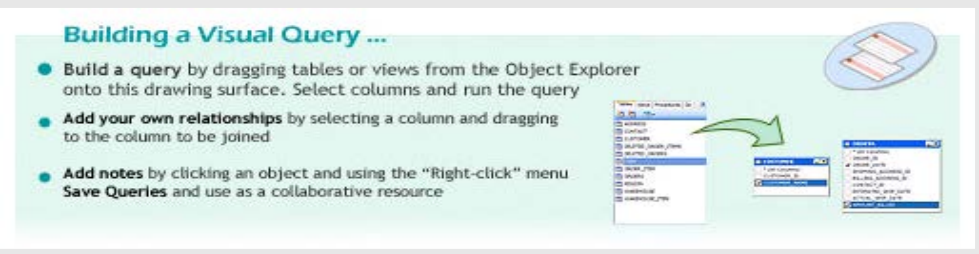
- The ArcSight Tool is used to deep link into Sensage

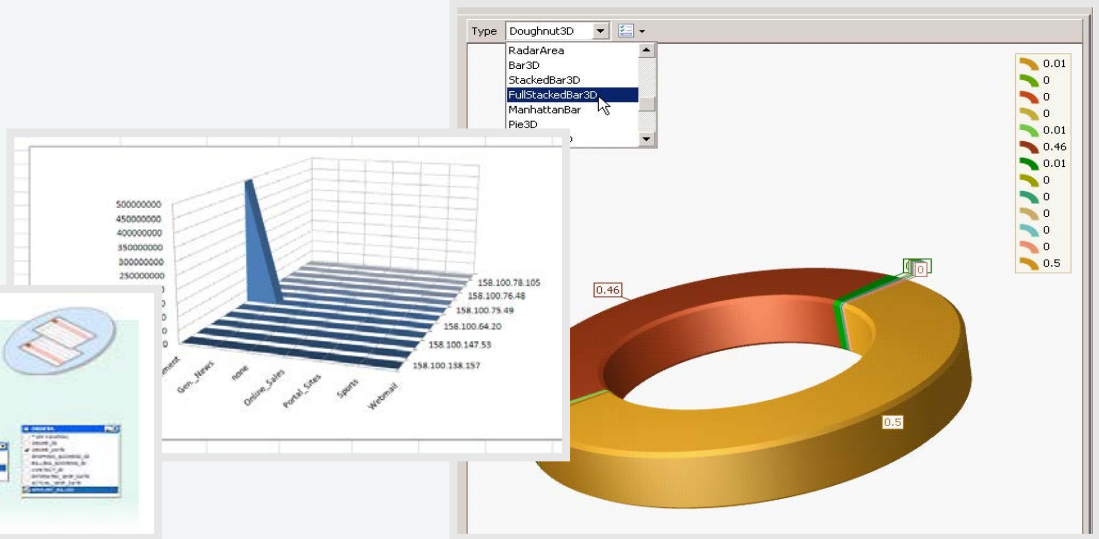


SENSAGE

More Advanced Use Cases Being Explored with Our Federal Government Customers…

- Baseline, trend and flag anomalies on anything
  - This requires all of the log data to be available to SQL
  - This requires a Business Intelligence layer that analysts can aim at their areas of interest
- OLAP cubes for security data analysis
  - Example:
    - Pivot on suspected origin, threat/attack type and targeted mission for a certain period of time
    - Change time period
    - Compare time periods





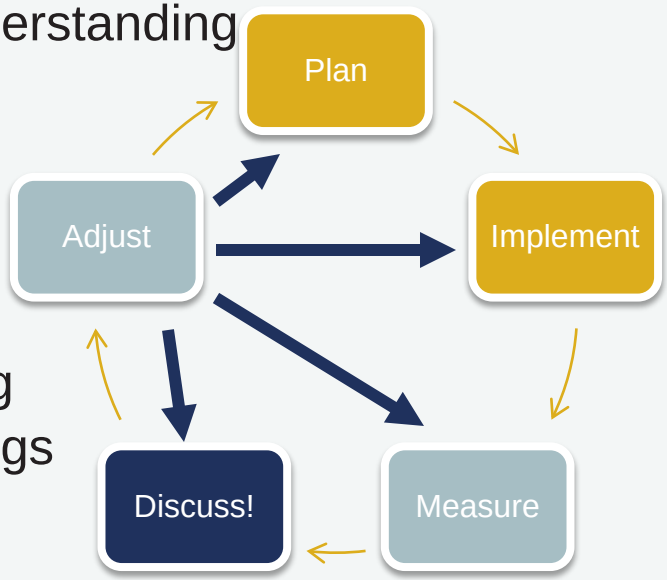
A New Perspective on Security Management

- Analyze historical data
  - Understand what “secure” looks like
  - Establish baselines and acceptable thresholds
  - Create policies that drive appropriate behaviors
  - Develop *informed* alerts when variances occur
  - Reduce reactive security investigations
  - Continuously improve security management based on logical metrics/ measurements

SENSAGE

Consistent Measurement, Continuous Improvement

- Plan and Implement
  - Plan changes in scope of people/process/functionality in enforcement/management/response based on findings
- Measure
  - Drop old metrics that are no longer interesting (reduce clutter)
  - Refine current metrics based on deeper understanding
  - Add new metrics based on new:
    - Concerns
    - Priorities
    - Appetite for depth
- Test and Discuss
  - Execute ongoing Metrics Penetration Testing
  - Evolve topics and outcomes based on findings
  - Evolve discussion participants based on:
    - Changes to scope
    - Changes to depth of discussion



SENSAGE

Sensage:
Proud to Serve the Federal Government

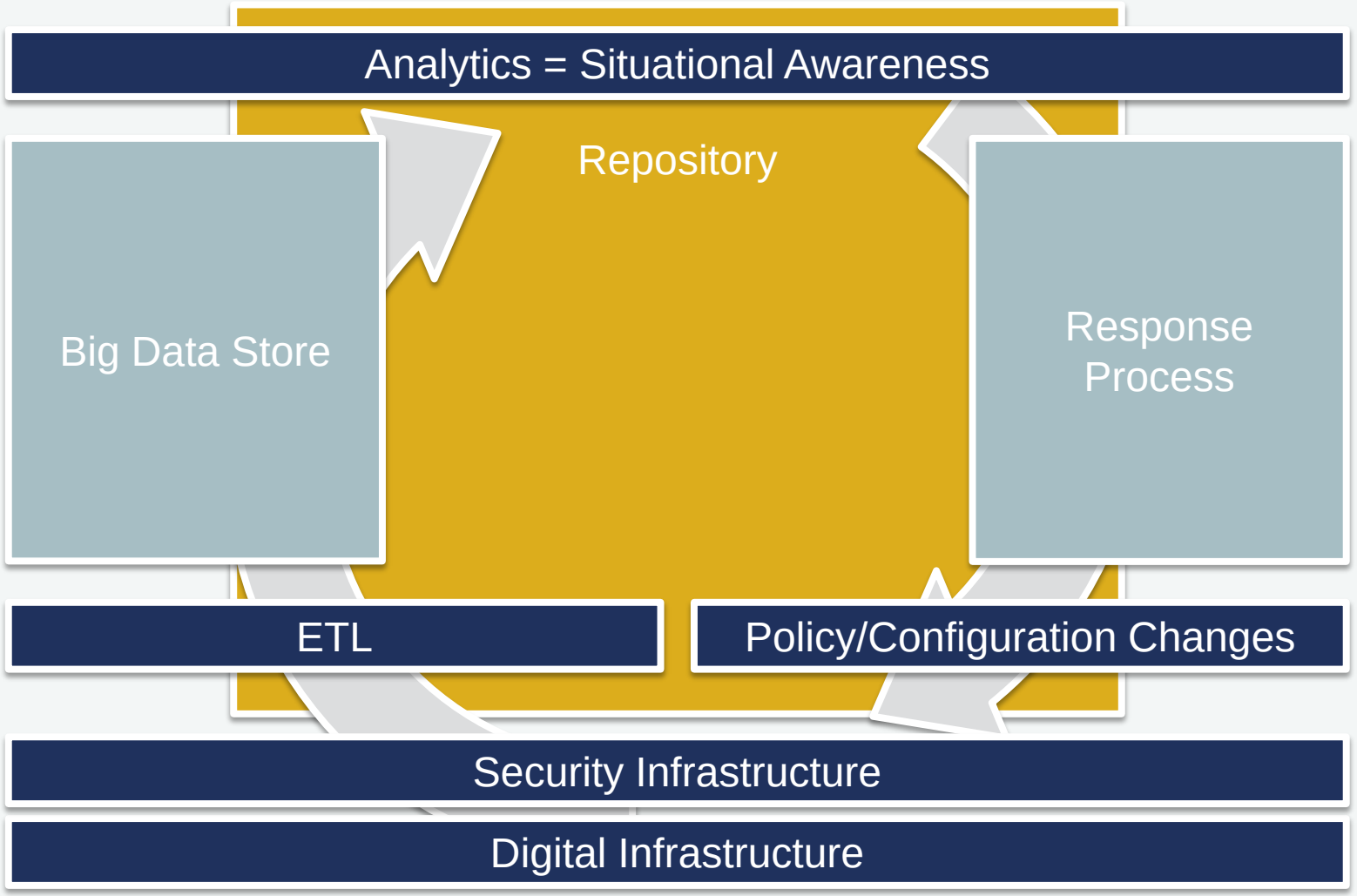
Learn More

- Visit www.sensage.com
  - Get a copy of the “Top Ten Tips for a Metrics-Minded Organization”
  - Register for the upcoming “The Buried Truth” webcast outlining top challenges with security process management
  - Find out why you don’t have to rip-and-replace your real-time monitoring solution

Questions?

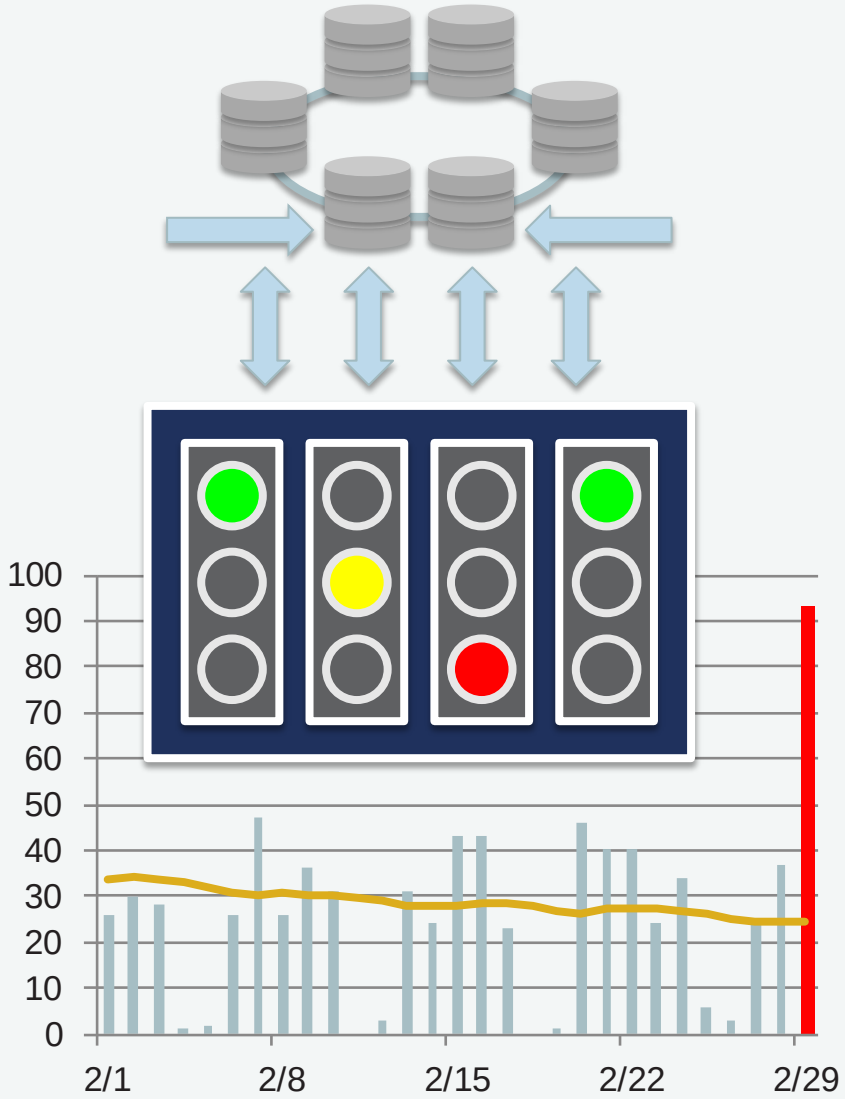
Joe Gottlieb
President and CEO
joe.gottlieb@sensage.com

What Sensage is doing with Open Security Intelligence…



Our Value Proposition

- Our customers have questions
- They want answers
- Compliance is not enough
- Monitoring is not enough
- They want to improve
- They're willing to crunch data and pay attention to what it says



- Sensage delivers security intelligence that is:

BI

OPEN

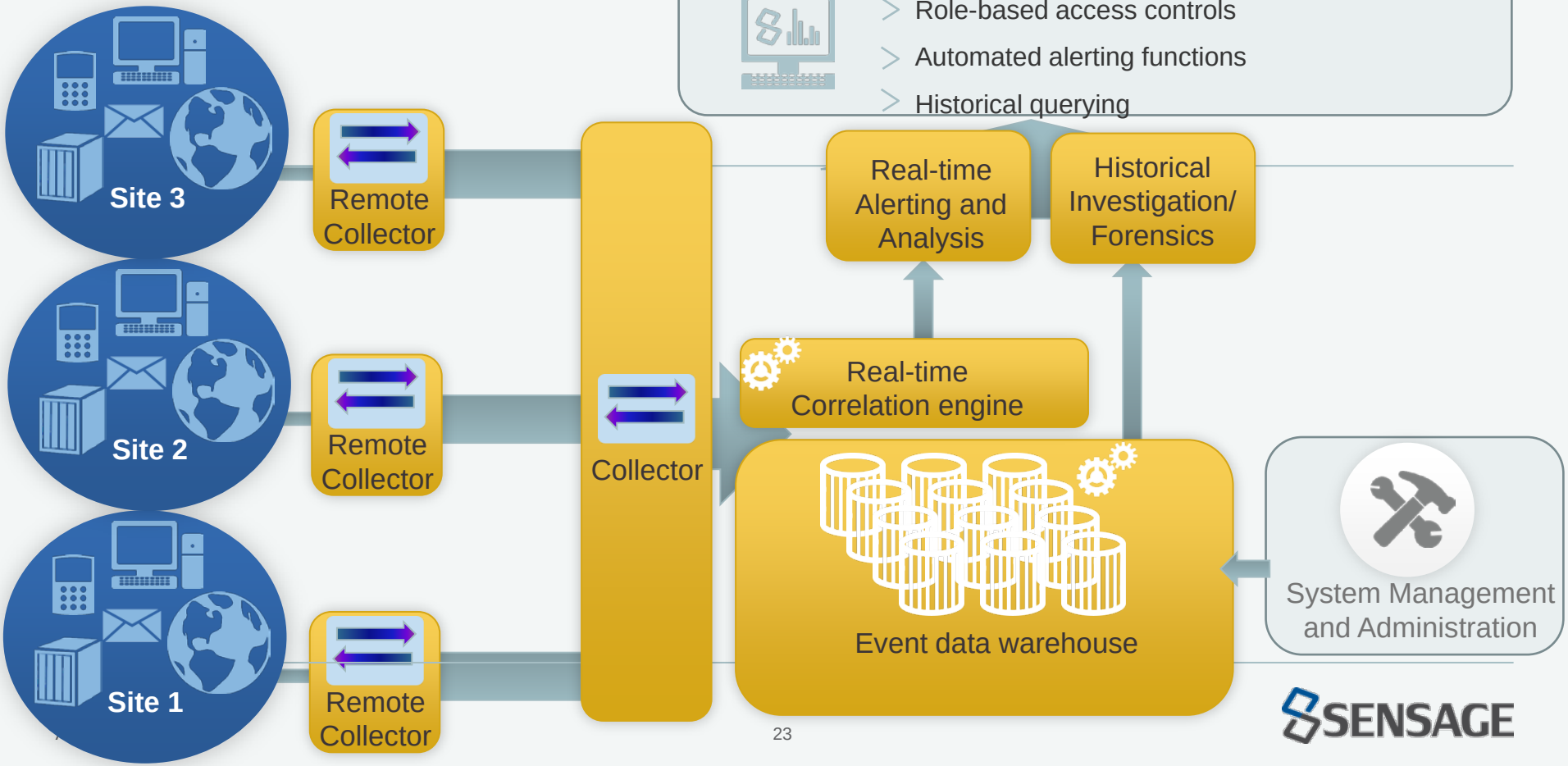
SIMPLE

SMART

SENSAGE

Government Deployment Example

Network Monitoring | User Monitoring | Application Monitoring | Data Monitoring | Compliance Reporting | Real-Time Event Analysis | Operational Reporting | Situation Awareness



SENSAGE