



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

INFORMATION

A SIMPLE COMPARISON...

FRAUD

SECURITY

PROBLEM:

- 1) RECURRING
- 2) EVOLUTIONARY
- 3) COSTLY

SOLUTION:

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

STATUS:

- 1) EXPECTED
- 2) CONTROLLED

PROBLEM:

- 1) RECURRING
- 2) EVOLUTIONARY
- 3) COSTLY

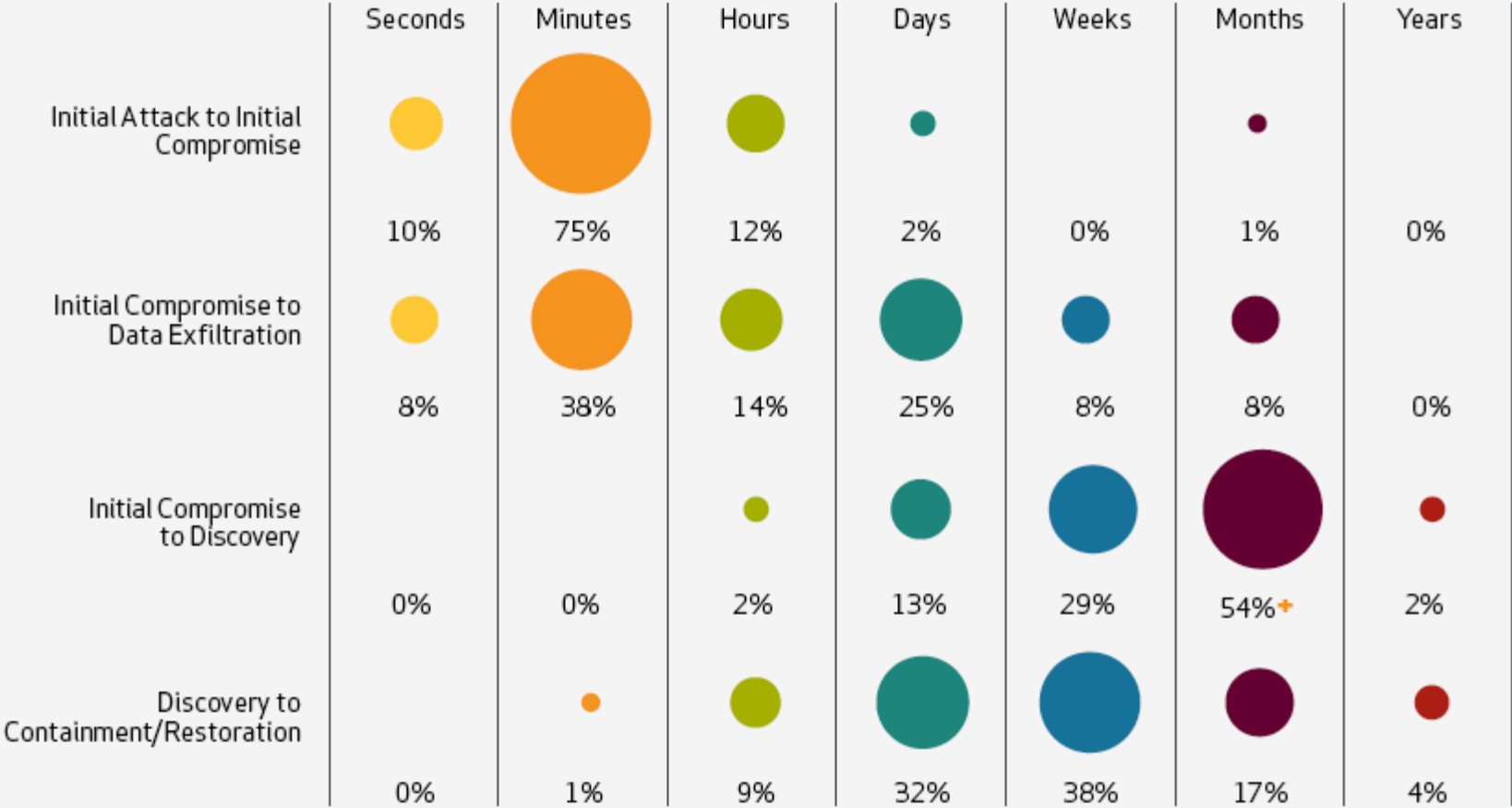
SOLUTION:

- 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

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

```
10110010010110011000110100
111111011100011001110110011
110101101111011111000011000
111011100011101110110110010
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 Exchange Commission

Division of Corporation Finance
Securities and Exchange Commission

CF Disclosure Guidance: Topic No. 2

Cybersecurity

Concept of Operations (CONOPS)



Office of Management and Enterprise Services

REGULATION & INFORMATION POLICY

About OIRA

Information Policy

Federal Collection of

Information Policy

Standards Policy

Information Quality Government-wide Initiative

OMB-Specific Information Quality Web page

Information Policy Documents

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 supremacy might seek to exploit our computer vulnerabilities here at home.

Article

Comments (270)



By BARACK OBAMA
Last month I signed an executive order on intelligence and cybersecurity, carrying into effect several state fall ill.

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



2012 DBIR: EXECUTIVE SUMMARY

2011 will almost certainly go down as a year of civil and cultural uprising. Citizens revolted, challenged, and even overthrew their governments in a domino effect that has since been coined the "Arab Spring," though it stretched beyond a single season. Those disgruntled by what they perceived as the wealth-mongering "1%," occupied Wall Street along with other cities and venues across the globe. There is no shortage of other examples.

This unrest that so typified 2011 was not, however, constrained to the physical world. The online world was rife with the clashing of ideals, taking the form of activism, protests, retaliation, and pranks. While these activities encompassed more than data breaches (e.g., DDoS attacks), the theft of corporate and personal information was certainly a core tactic. This re-imagined and re-invigorated specter of "hacktivism" rose to haunt organizations around the world. Many, troubled by the shadowy nature of its origins and proclivity to embarrass victims, found this trend more frightening than other threats, whether real or imagined. Doubly concerning for many organizations and executives was that target selection by these groups didn't follow the logical lines of who has money and/or valuable information. Enemies are even scarier when you can't predict their behavior.

This re-imagined and re-invigorated specter of "hacktivism" rose to haunt organizations around the world.

It wasn't all protest and lulz, however. Mainline cybercriminals continued to automate and streamline their method du jour of high-volume, low-risk attacks against weaker targets. Much less frequent, but arguably more damaging, were continued attacks targeting trade secrets, classified information, and other intellectual property. We certainly encountered many faces, varied tactics, and diverse motives in the past year, and in many ways, the 2012 Data Breach Investigations Report (DBIR) is a recounting of the many facets of corporate data theft.

855 incidents, 174 million compromised records.

This year our DBIR includes more incidents, derived from more contributors, and represents a broader and more diverse geographical scope. The number of compromised records across these incidents skyrocketed back up to 174 million after reaching an all-time low (or high, depending on your point of view) in last year's report of four million. In fact, 2011 boasts the second-highest data loss total since we started keeping track in 2004.

97% of breaches were avoidable...

79% of victims were targets of opportunity (-4%)

96% of attacks were not highly difficult (+4%)

94% of all data compromised involved servers (+18%)

85% of breaches took weeks or more to discover (+6%)

92% of incidents were discovered by a third party (+6%)

97% of breaches were avoidable through simple or intermediate controls (+1%)

96% of victims subject to PCI DSS had not achieved compliance (+7%)

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

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



00100010110010010110011000110100
11100001100011101110001110111010
00100100111101100010001011001001
01100110001101001111110111000110
01110110011110101101111011111000
01100011101110001110111011011001
01101000110111100010010011110110
00100010110010010110011000110100
10011010100011

Sensage



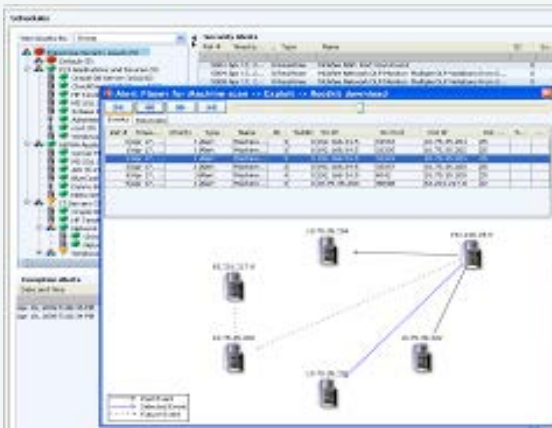
Sensage Unique Capabilities

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

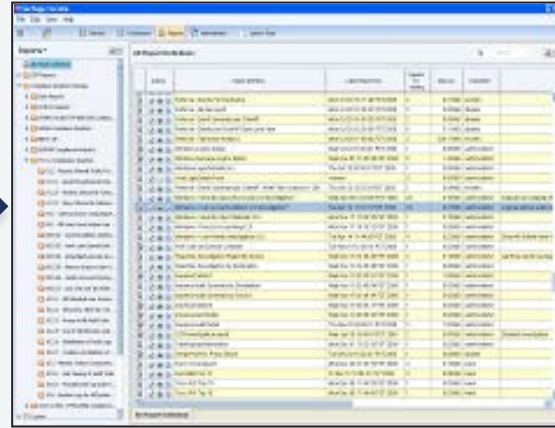
Sensage Solution – Analytics for Greater Security Intelligence

Real-time Monitoring



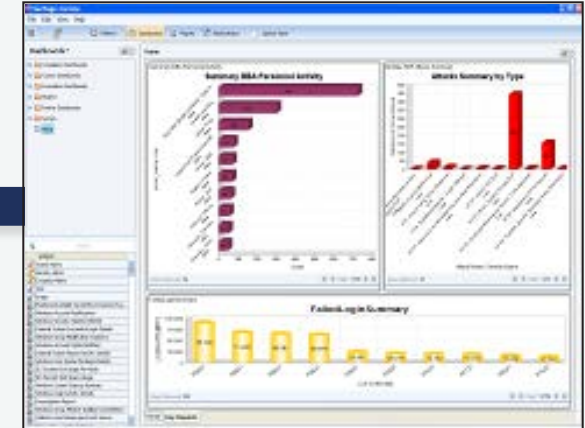
- Powerful real-time correlation
- Scenario-based analysis
- Integrated with historical correlation
- Easy to create and deploy template-based rules
- Dozens of common out-of-the-box rules

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

Save Revert Refresh Dashboards Reports Administration Options Pane

Reports

- All Report Definitions
- Analyst Workbench
 - Administrator Access
 - Firewall Analysis
 - Unauthorized or Infected Machines
 - Unauthorized Software Installation
 - Web Proxy Analysis
- CDR
- Compliance Analytics Package
- Continuous Monitoring and Auditing for ...
- Custom
- Foundation Analytics Package
- McAfee
- Partner
- SANS Top 5 Essential Log Reports
- SenSage Solutions
- Source Specific Reports

Web Proxy - Outlier Trending Report by UserName-0

userName	Outlier
arodriguez	193184848.173720
bbuckner	0.000000
cripken	0.000000
eslaughter	0.000000
hwagner	0.000000
jabbott	0.000000
jlopez	0.000000
lgehrig	0.000000
rmartinez	0.000000

Rows Returned 12

BlueCoat - Download patterns for user investigation-0

Hour	User ID	Total Bytes Download...
00	djustice	886
01	djustice	882
02	djustice	908
03	djustice	872
04	djustice	949
05	djustice	962
06	djustice	1,098
07	djustice	1,208
08	djustice	1,830
09	djustice	2,728

Rows Returned 24

Web Proxy - Outlier Trending

BlueCoat - download patterns for user investigation

BlueCoat - Use ... Received 2sigma ... Than Others-0

userName	SIGMA2	GROUPAVG	USER_TO...
djustice	1650512...	330102582.6648...	495880967

Rows: Folde

August 27, 2012

SENSAGE

Correlating Support Ticketing with Network Activities

Metrics Tool | Dashboards | Group containers | Statistics | Metrics | Admin | SO | Account | Logout

SENSAGE

new

Dashboards

Listing dashboards | 1. Top Level Indicators

Back

container: **Alert Management**
metric: **Alert Count**
weight: 100%

Alert Count measures the alert counts over time. It is used to track significant change in volume since malicious activity is sometime easily discernible because of their mass quantities.

container: **Alert Management**
metric: **Alert Count**
last days: ALL

Total

container: **Alert Management**
metric: **Alert Counts by Category**
weight: 100%

Alert Count by Category breaks down the alert counts by type of alert. It is used to identify the larger contributors in the rise of alerts.

container: **Alert Management**
metric: **Alert Counts by Category II**
last days: ALL

Reports

- All Report Definitions
- Analyst Workbench
 - Administrator Access
 - Firewall Analysis
 - Unauthorized or Infected Machines
 - Unauthorized Software Installation
 - Web Proxy Analysis
- CDR
- Compliance Analytics Package
- Continuous Monitoring and Auditing for ...
- Custom
- Foundation Analytics Package
- McAfee
- Partner
- SANS Top 5 Essential Log Reports
- SenSage Solutions
- Source Specific Reports

Web Proxy - Outlier Trending Report by UserName-0

userName	Outlier
arodriguez	193184848.173720
bbuckner	0.000000
cripken	0.000000
eslaughter	0.000000
hwagner	0.000000
jabbott	0.000000
jlopez	0.000000
lgehrig	0.000000
mmartinez	0.000000

Rows Returned 12

Web Proxy - Outlier Trending Report by User

Metrics Tool | Dashboards | Group containers | Statistics | Metrics | Admin | SO | Account | Logout

SENSAGE

new

Dashboards

Listing dashboards | 1. Top Level Indicators

Back

container: **Alert Management**
metric: **Alert Counts by Category**
weight: 100%

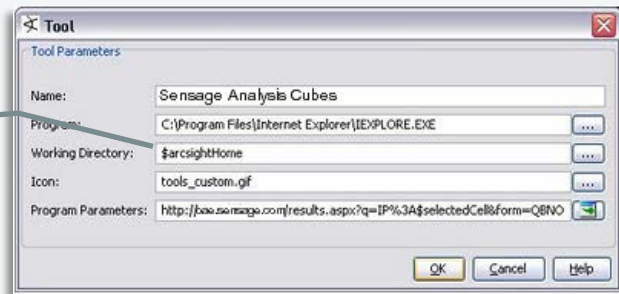
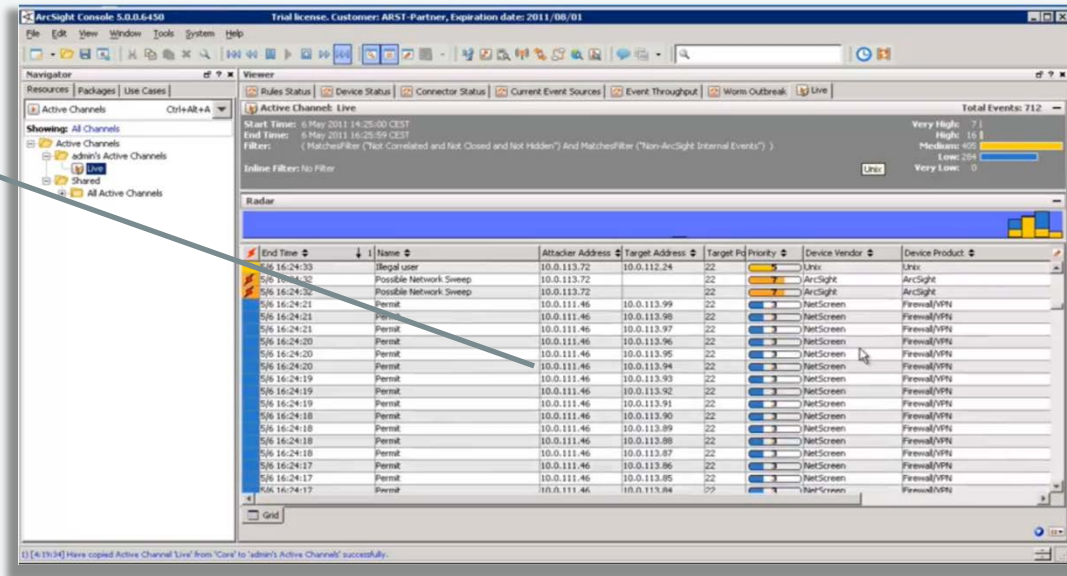
container: **Alert Management**
metric: **Alert Counts by Category**
last days: ALL

Evaluation

- Password Reset by AD0529 for Account
- Password Reset by 302216 for Account
- Password Reset by AD0506 for Account
- User Account Created and Deleted within 1 Hour
- Unusual Number of Account Logouts in Domain
- Unusual Number of Account Logouts for Workstation
- Unusual Number of Account Logouts for User
- Unusual Number of Account Lockouts
- The system IPsec Policy has been modified
- System Startup Deferred
- Security Policy has been altered via GPO on host
- Security Enabled Global Group Changed

SIEM Extension for ArcSight

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

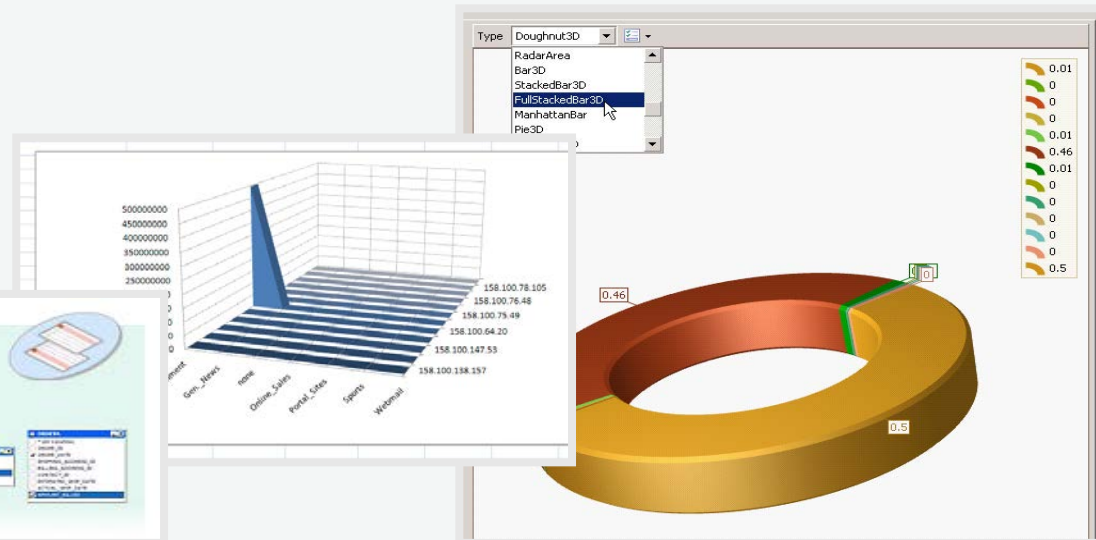


- An ArcSight real-time correlation rule detects malicious activity
- The Alert shows up in the ArcSight Active Channel View, where analyst right-clicks on Attacker-Address/Target Address column and selects Sensage Forensic Drill-down Wizard from Tools menu

- The ArcSight Tool is used to deep link into Sensage

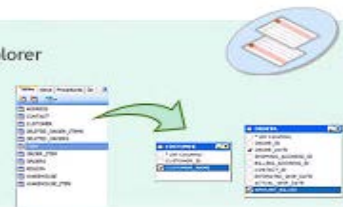
More Advanced Use Cases Being Explored with Our Federal Government Customers...

- 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



Building a Visual Query ...

- Build a query by dragging tables or views from the Object Explorer onto this drawing surface. Select columns and run the query
- Add your own relationships by selecting a column and dragging to the column to be joined
- Add notes by clicking an object and using the "Right-click" menu Save Queries and use as a collaborative resource



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



Consistent Measurement, Continuous Improvement

- Plan and Implement

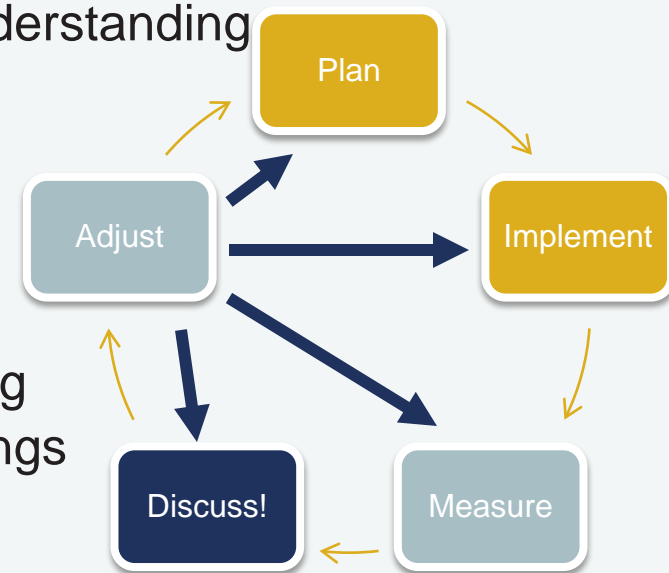
- Plan changes in scope of people/process/functionality in enforcement/management/response based on findings

- 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: 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

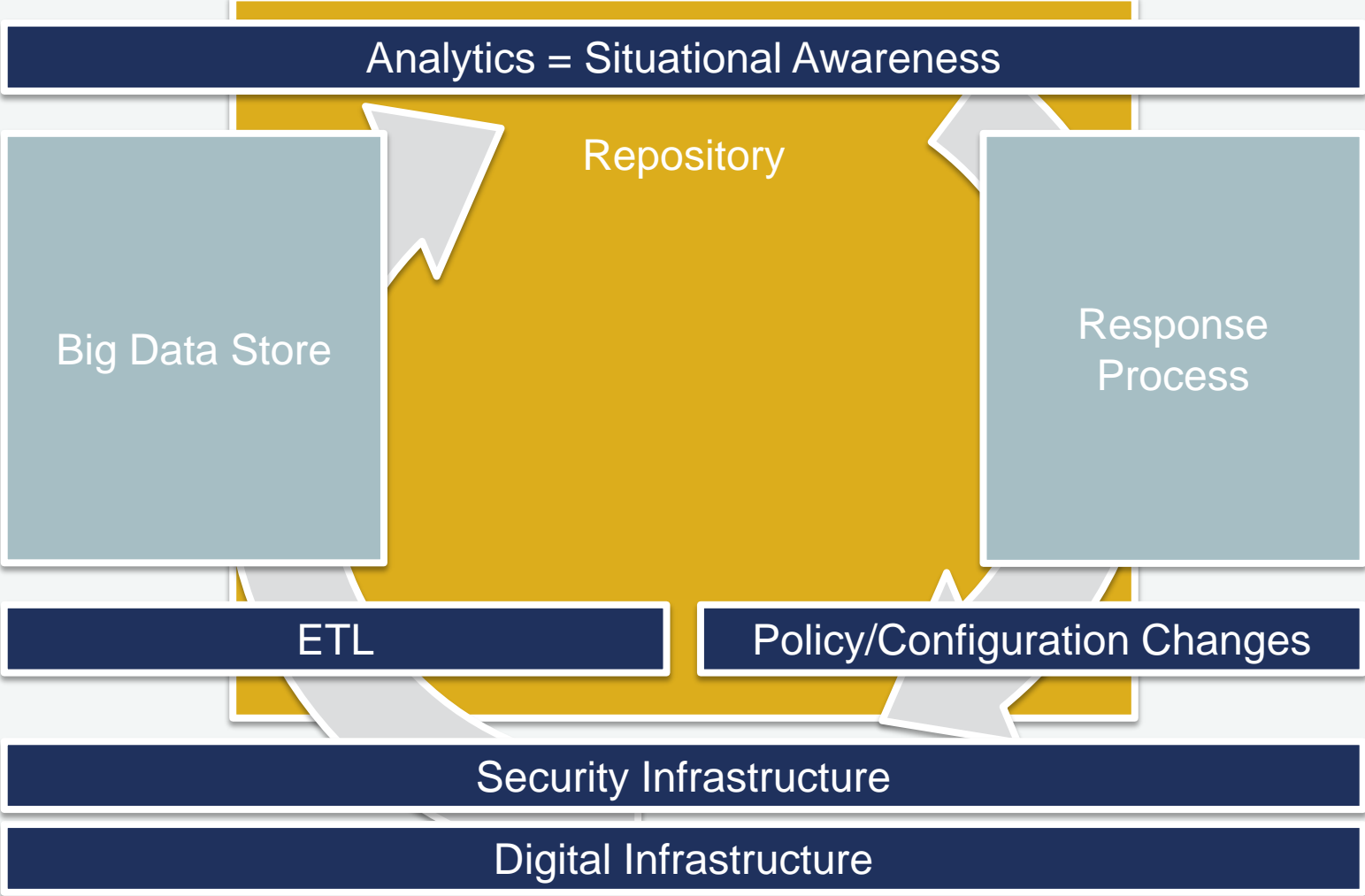




Questions?

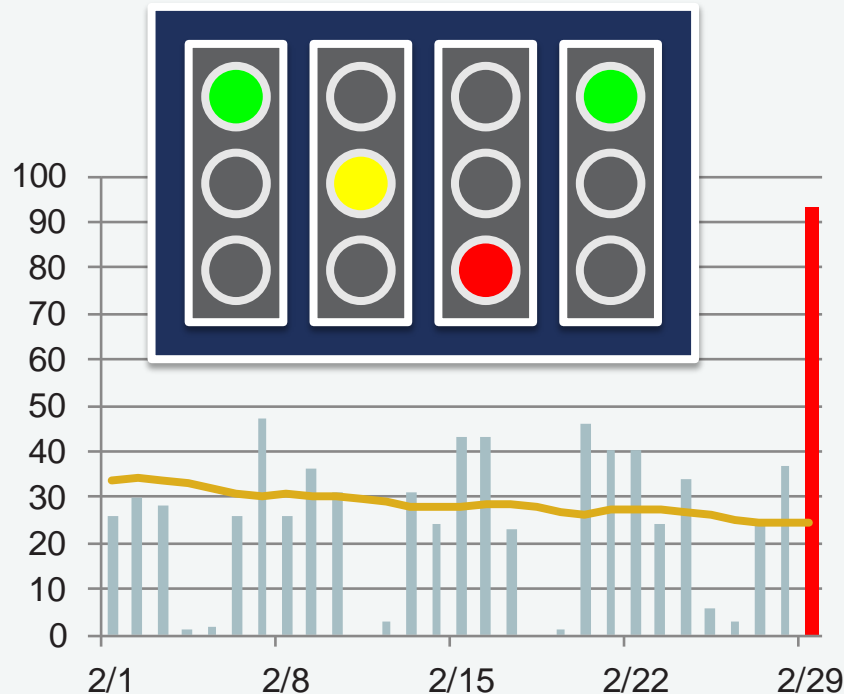
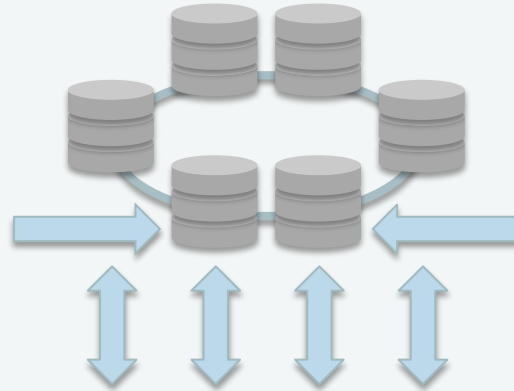
Joe Gottlieb
President and CEO
joe.gottlieb@sensage.com

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

Government Deployment Example

Network Monitoring

User Monitoring

Application Monitoring

Data Monitoring

Compliance Reporting

Real-Time Event Analysis

Operational Reporting

Situation Awareness

- > Complex aggregation and statistical analysis
- > Role-based access controls
- > Automated alerting functions
- > Historical querying

