



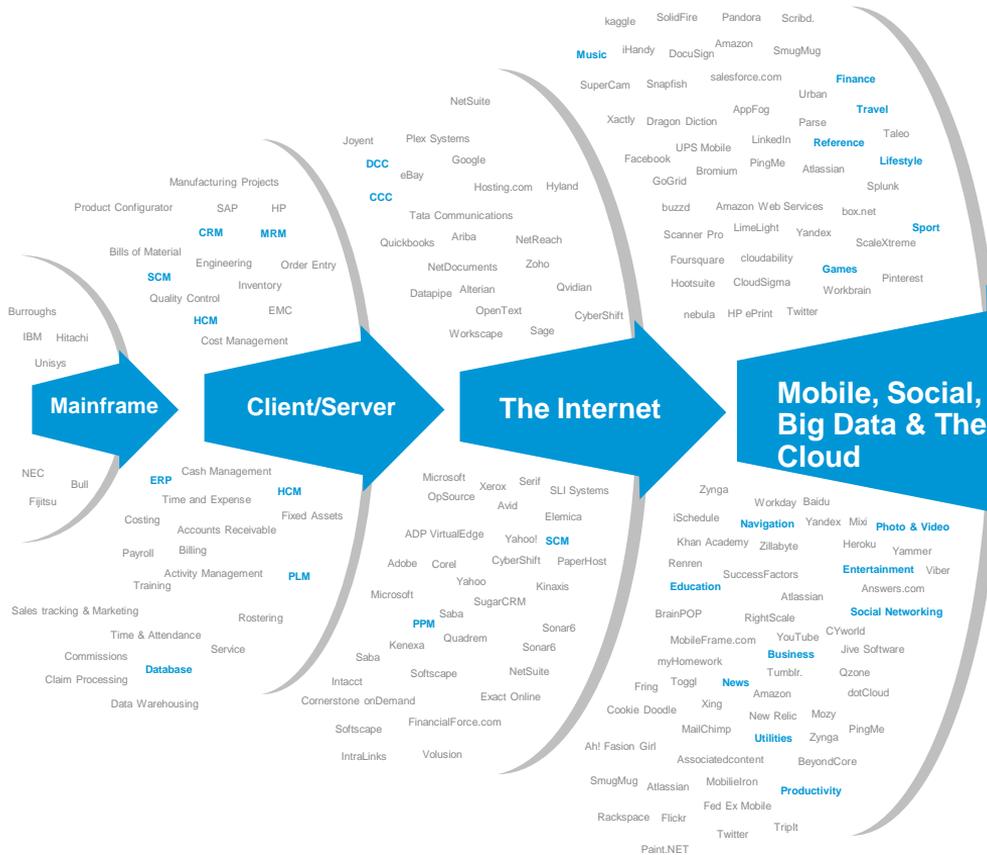
Managing Data Explosion

Samuel Olin
June 5, 2013

Agenda

- Introduction
- “Tectonic Shifts” in Enterprise Computing
- The Coming Data Explosion
- Security in the age of Free Data
- 2013 “CISO 100” Tour
- Challenges and Solutions for MDE
- Questions and Answers

A new style of IT emerging



Every 60 seconds



98,000+ tweets



695,000 status updates



11 million instant messages



698,445 Google searches



168 million+ emails sent



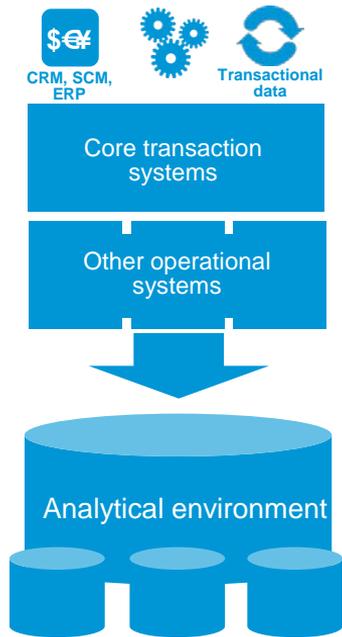
1,820TB of data created



217 new mobile web users



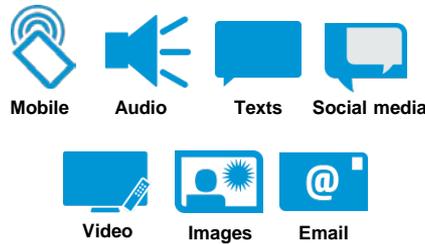
Data Explosion is at hand.



Predefined reporting, dashboards, and analytics to:

- Measure/monitor the business
- Analyze and improve operations

“Human-friendly information”



Requiring filters for *meaning* (context, relevance, urgency) to:

- **Protect the business** (such as new compliance requirements)
- **Grow the business** (such as customer engagement models)



This is the future.



By 2014, Gartner estimates that about 20% of enterprises will own no assets

By 2020, 2 trillion devices will connect to the internet...and to each other.



Security trends are on a collision course.

Growing cyber threat

56% of organizations have been the target of a cyber attack

Extended supply chain

44% of all data breach involved third-party mistakes

Financial loss

\$8.9M is the average cost associated with data breach

Reputation damage

30% market cap reduction due to recent events

Cost of protection

11% of total IT budget spent on security

Reactive vs. proactive

60% of enterprises spend more time and money on reactive measures vs. proactive risk mgmt.

Key issues:

- Security is a **Board of Directors/Cabinet level concern.**
- Security leadership is under immense pressure.
- There is a need for greater visibility of business risks and to make sound security investment choices.



The challenge is complex

Primary challenges

1

Nature and motivation of attacks
(national interest to new markets)

A new type of adversary



Research



Infiltration



Discovery



Capture



Exfiltration

2

Cloud and Traditional IT
(delivery and consumption changes)

Delivery

Traditional



Network Storage Servers

Private cloud



Managed cloud



Public cloud



3

Regulatory pressures
(increasing cost and complexity)

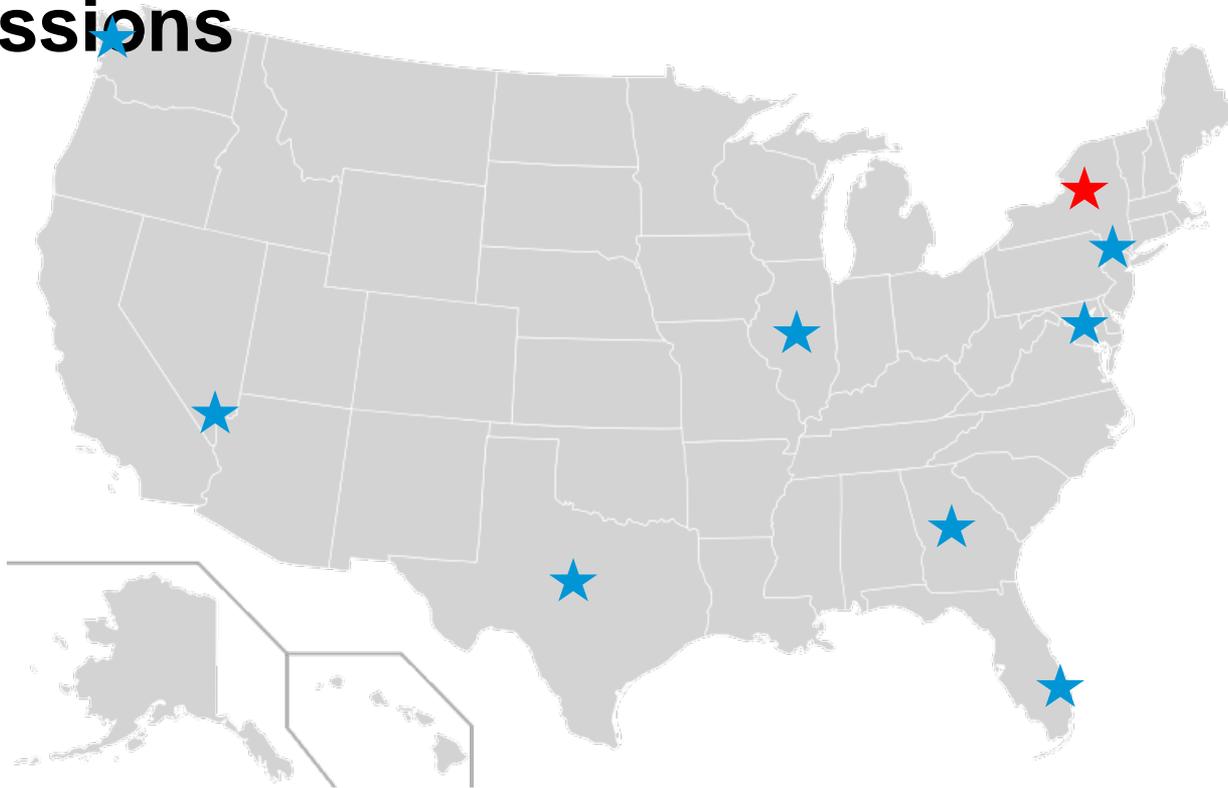
Enhanced regulatory environment

NERC • Sarbanes-Oxley •
Basel III • PCI Security Standards Council

Deal with all three while **DATA** itself is **EXPLODING** in velocity, variety, and volume.



2013 Northern American CISO MDE Discussions



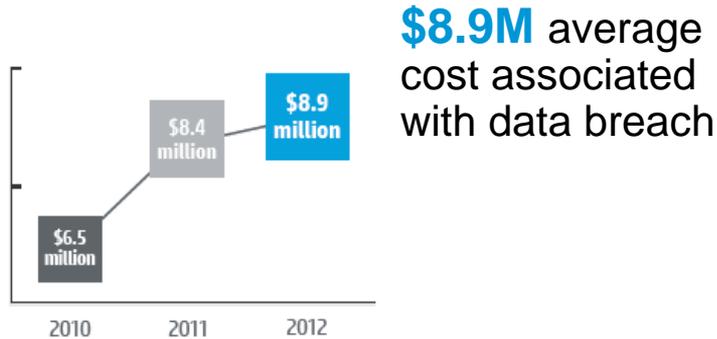
Hot Management Topics

- Does this mean we will be breached?
- Where should I start?
- Am I spending my money wisely?



With “Data Explosion” breaches are a certainty.

How much do you think a breach will cost?

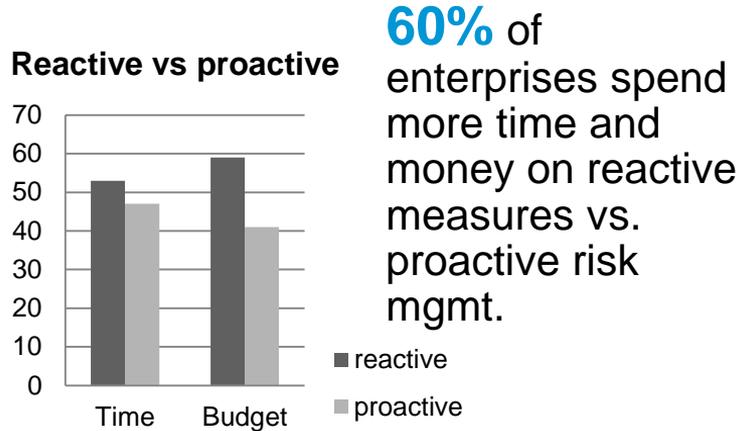


Associated costs rising year on year

- Breaches are a certainty. Expect them.
- Some of the fastest growing breaches are occurring via suppliers and business partners (no direct control)
- Critical functions such as incident response and recovery, investigation and forensics, eDiscovery/eDisclosure, PR/brand management are increasing areas of focus and investment

Spending decisions

Where are you spending your money?



Organizations need optimized security

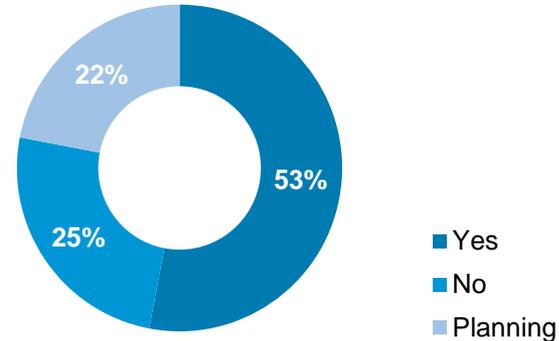
- Appropriate balance is organization specific
- Proactive measures likely to reduce number of reactive responses
- Generally not enough intelligence regarding an organization to make robust trade-off investment decisions (“blind patching” and “protect everything” approach common)
- Need to prioritize proactive investments based on risk/exploitability

Information management/governance strategy

- IT infrastructure security will be difficult if not impossible
- Information governance and management strategy is critical
- Must prioritize data/information based and balance with risk
- Investment strategies must align to information risk

Where is your organization?

Information risk strategy ?



Security executives need to have a seat at the table

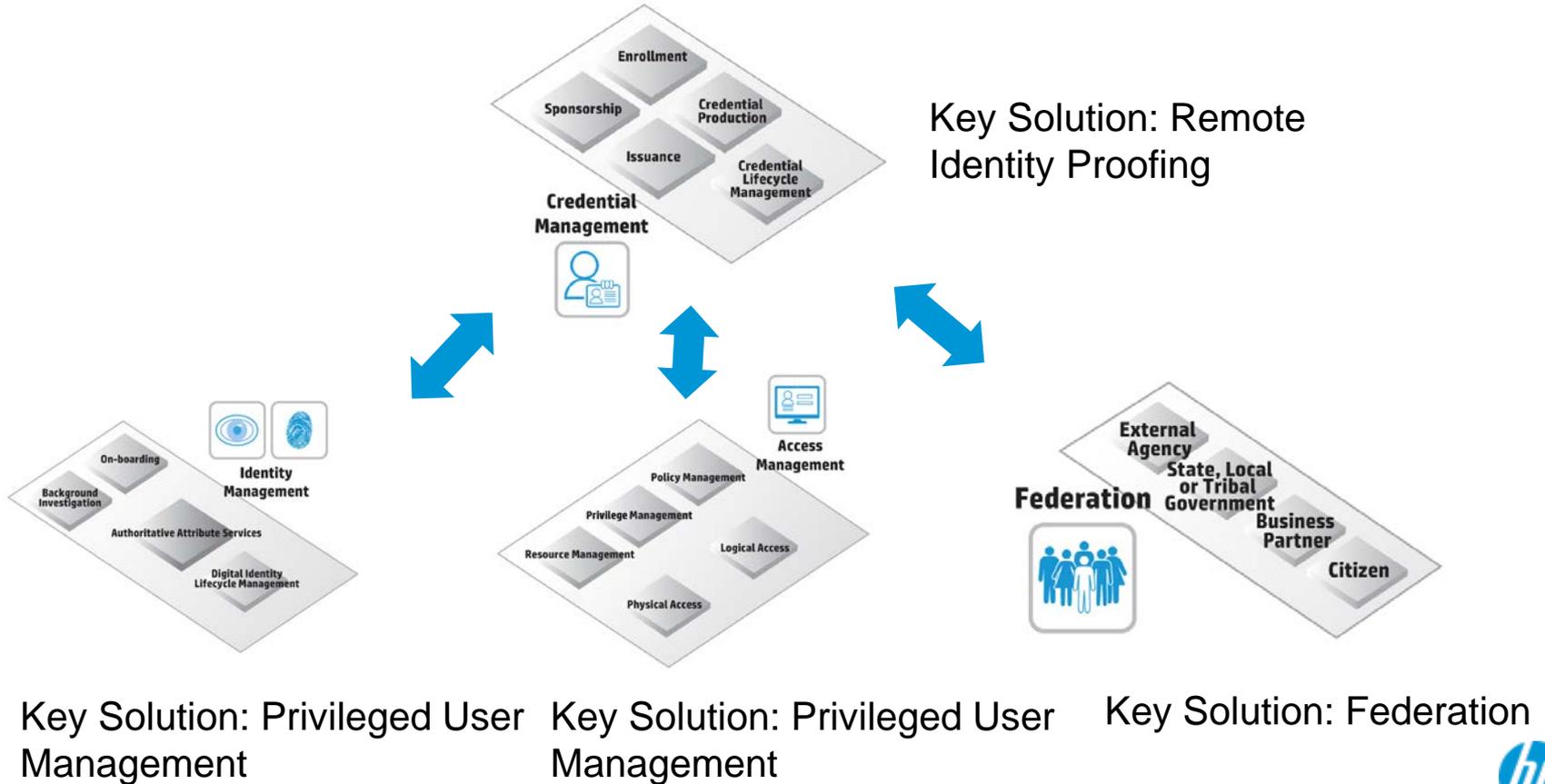


Top Solutions for MDE

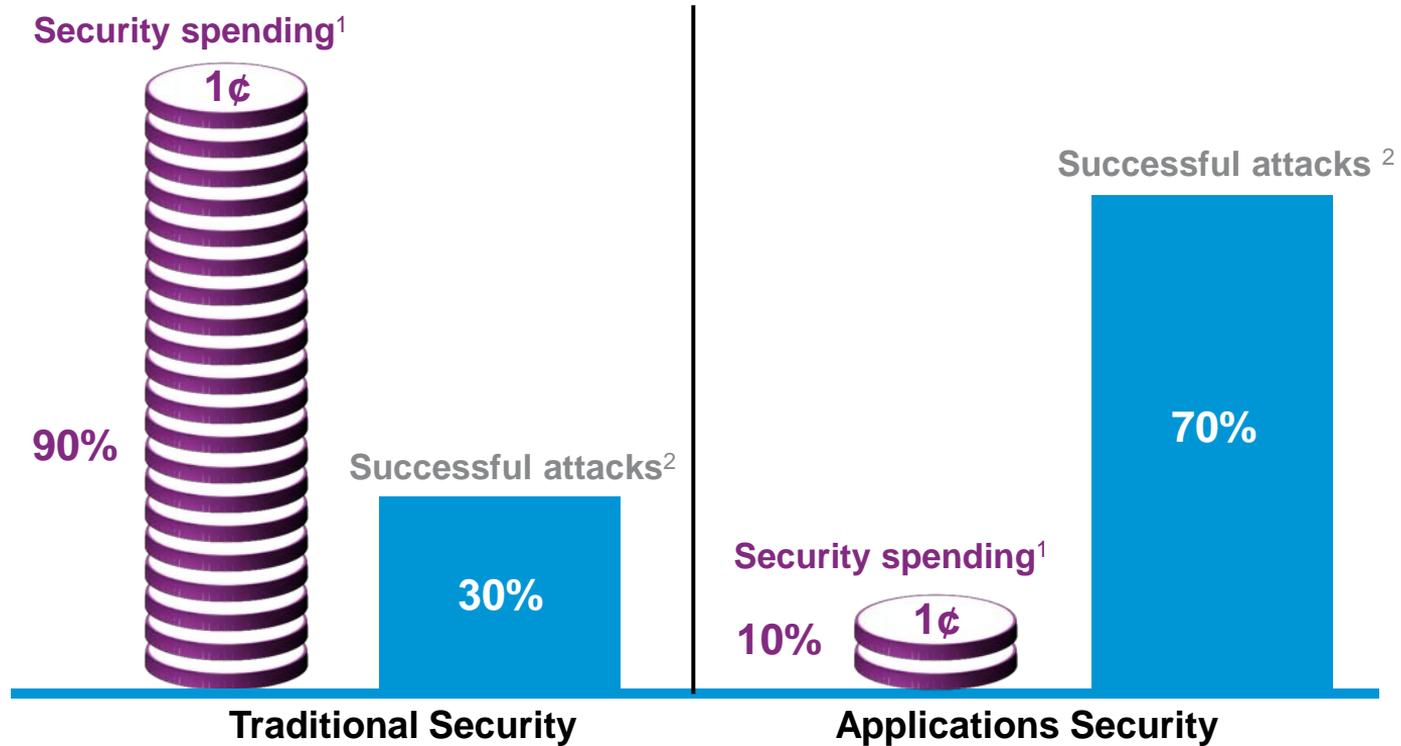
- Identity & Credential Management
- Application Security
- Data and Content Protection
- Security Intelligence



Identity & Credential Management



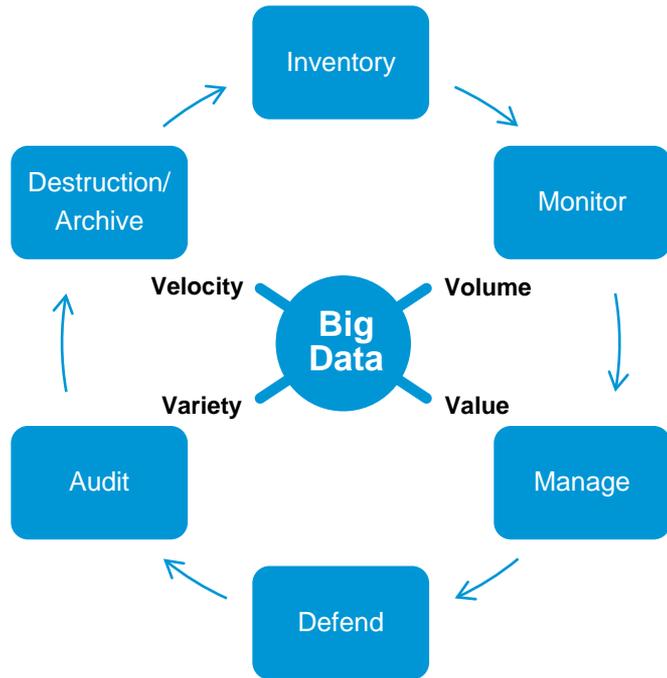
Applications Security: Protecting the primary DHI



Sources: 1) Gartner IT Security Budgets and Staffing Projections for 2012: Constant Demand and Constant Spending, Mar, 2012
2) Microsoft Security Intelligence Report (SIR), v12, - Dec 2011

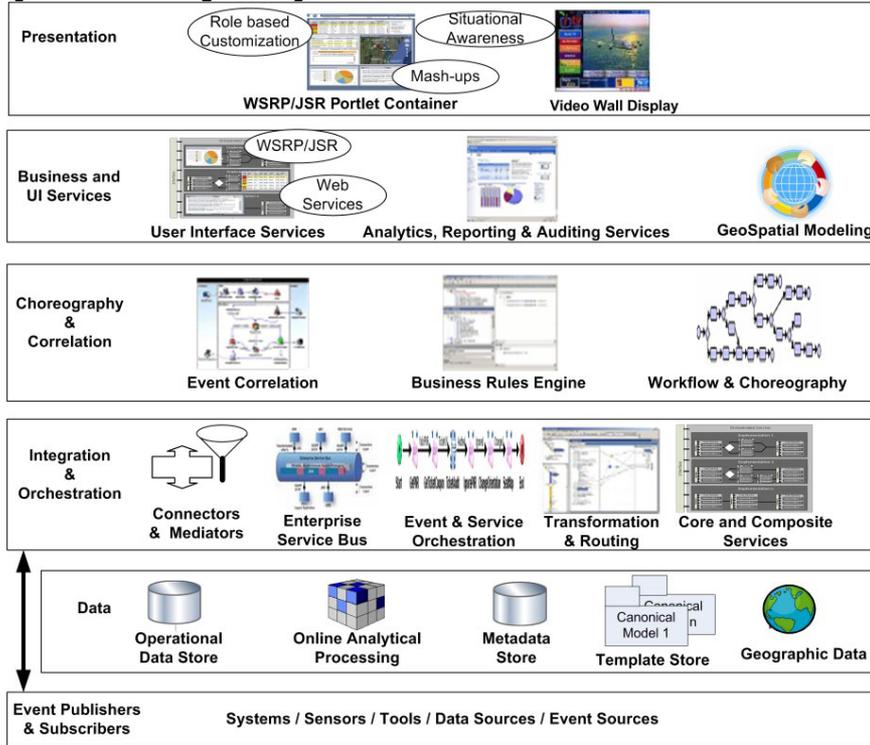


Protecting what Matters: DLP and Beyond



- Data like any other asset has it's own lifecycle
- Many IT enterprises can't account for all of it's data
- Many IT enterprises lack the tools to discover all of their data (especially cross platform unstructured)
- A lot of focus on DLP as a technology but DLP works best as a full-lifecycle data governance approach

Security Big Data: Intelligence & Decision Support (Example)



Cyber Command Center Demonstrator

Complex Incidents

Impact Level	Incident Type	ID Number	Incident State	Process or Status	Assigned To	Last Update	Updated By
High	DNS Poisoning	DNSP-246	05 May 09	Pending	Waltcher, John	06 May 09	Waltcher, John
Significant	Denial of Service	DOS-459	04 May 09	In Progress	Seec, Jane	07 May 09	Seec, Jane
Significant	Data Exfiltration	DE-78	04 May 09	Informational	Roscoe, Bob	06 May 09	Roscoe, Bob
Minor	Denial of Service	DOS-459	03 May 09	Pending	Waltcher, John	04 May 09	Waltcher, John
Significant	Data Exfiltration	DE-78	02 May 09	In Progress	Waltcher, John	02 May 09	Waltcher, John

Contributing Events

Event	Category	Location	Time Stamp
Potential DNS cache Poisoning attempt	Security	Annapolis, MD	1312:34 27 Jan 09
Potential SPAM attack	Security	Norfolk, VA	1213:39 24 Jan 09
Firewall Server Accepted HTTP request	Security	Washington, DC	1312:34 21 Jan 09

Event Info

Attention: Potential DNS cache poisoning attempt

If you have determined that this event should be dissociated from this Complex Incident, enter the reason, why and contents.

Internal Incidents Being Monitored

Incident Type	Percentage
Denial of Service	34%
DNS Cache	22%
Phishing Attack	19%
Data Exfiltration	13%
Excessive IDS	10%
Other	3%

News

Online Trust: A Thing of the Past? InformationWeek.com: 6 hour ago
 Malware attacks are turning the Web upside down, and complicating the efforts of security vendors and users to cope with the threat. [Read More](#)

Computer experts say the person, or group, controlling a new Internet worm could control viruses on an unprecedented scale. [Read More](#)

Crime Experts Warn of Internet Malware: sms.com: 10 hrs
 Computer experts say the person, or group, controlling a new Internet worm could control viruses on an unprecedented scale. [Read More](#)

New Fast, Blue Botnet Using Browser Specific exploits to Attack Victims PC's come down: IT news age
 AVG's Chief Research Officer, talks about a new discovery that a security guy at the BG made the weekend. [Read More](#)





Thank you