Must Collect IOCs… Now What?!  
SANS THIRS, New Orleans Louisiana, April 2016

William M Phillips IV
Forward-Looking Statements

Statement under the Private Securities Litigation Reform Act of 1995:

This presentation may contain forward-looking statements that involve risks, uncertainties, and assumptions. If any such uncertainties materialize or if any of the assumptions proves incorrect, the results of salesforce.com, Inc. could differ materially from the results expressed or implied by the forward-looking statements we make. All statements other than statements of historical fact could be deemed forward-looking, including any projections of product or service availability, subscriber growth, earnings, revenues, or other financial items and any statements regarding strategies or plans of management for future operations, statements of belief, any statements concerning new, planned, or upgraded services or technology developments and customer contracts or use of our services.

The risks and uncertainties referred to above include – but are not limited to – risks associated with developing and delivering new functionality for our service, new products and services, our new business model, our past operating losses, possible fluctuations in our operating results and rate of growth, interruptions or delays in our Web hosting, breach of our security measures, the outcome of any litigation, risks associated with completed and any possible mergers and acquisitions, the immature market in which we operate, our relatively limited operating history, our ability to expand, retain, and motivate our employees and manage our growth, new releases of our service and successful customer deployment, our limited history reselling non-salesforce.com products, and utilization and selling to larger enterprise customers. Further information on potential factors that could affect the financial results of salesforce.com, Inc. is included in our annual report on Form 10-K for the most recent fiscal year and in our quarterly report on Form 10-Q for the most recent fiscal quarter. These documents and others containing important disclosures are available on the SEC Filings section of the Investor Information section of our Web site.

Any unreleased services or features referenced in this or other presentations, press releases or public statements are not currently available and may not be delivered on time or at all. Customers who purchase our services should make the purchase decisions based upon features that are currently available. Salesforce.com, Inc. assumes no obligation and does not intend to update these forward-looking statements.
What Did We Do

• Automated IOC searching
• Historical lookback
• Multiple environments
• Actually works
$whoami

- Securitah Researcher
  - Automation
  - Incident Response
  - Huntin’
  - Threaty threats
  - etc
Roadmap

• Problem
• Goals
• Overlord
  • Configuration
  • Modularity
  • Extractor
  • Searcher
  • Alerter
• DEMO
Problem
Problem(s)

- Indicator Fire Hose
- Complexities of Volume
- Consistency Across Sources
- Source types
- Competing Priorities
Goals
Goals

• Remove the human
• Support multiple search environments
• Integrate with our case management system
Overlord
Overlord

IOC Repository

Log Repo A

Log Repo B

Log Repo C

Log Repo D
Configuration
Configuration file

- Encrypted at rest
- Quickly change advanced settings
- Object Oriented Hierarchy
Modularity
Built in Security

• Disparate home environments
• Each receiver unique cert capable
• Transmission validation
Extractor
Extractor

- Retrieves Indicators
- Formats
- Sends to searcher
- Controls historical searches
Searcher
Searcher

• Customized for each snowflake
• Distributes load
• Addition of new environments
Alerter

- Generates alerts
- Independent
- Platform agonistic
Caveats’/Future dev

- Searcher Speed Limited
- Not real time
- Extractor abstraction
- Moar modules
Takeaways

• Modular
  • Extractor
  • Searcher
  • Alerter

• Scalable
  • Configuration file

• It works
  • Automated IOC searching
  • Platform agnostic

*It’s not perfect*
thank you