SEARS HOLDINGS

Managing and Analyzing Data for Near Real-Time Security Analytics

Brad Lindow

The Security Architect

Sears Online Business Unit (OBU)

October 2, 2013

Brad.Lindow@searshc.com

About Me

- Former attorney
- Worked with some of the largest computing environments in the world
  - Orbitz
  - Travelport
  - Department of Commerce
  - Consulting organization
- What I do now – The Security Architect for Sears Online
  - Identify and build security and fraud solutions that defend against cyber criminals and their clever ways of attacking systems

Agenda

- Executive Summary
- Sears Online Business Unit (OBU) Security Challenges
- A Vision for Developing a Next Gen Threat Intelligence Platform
- A Phased Approach & Lessons Learned

The Challenge

How do you take over 10 million possible security events per day and make sense of the data in less than 4 months?

The solution must protect the brand and be transparent to the end users

Why is This Important?

- Over 5,000 attacks go undetected per day in the United States, according to a Bloomberg report
- Only 40% of surveyed companies said they had the tools and funding to understand breaches, according to a Ponemon report
- Average cost per record for a data breach is about $200, according to a Ponemon report
- Total losses from cybercrime in the U.S. may reach over $100 billion dollars a year, according to a McAfee report

Sears Background

- In existence for over 100 years
- Operates over 2,500 stores
- Operates over 100 Web sites
- Fast-paced environment

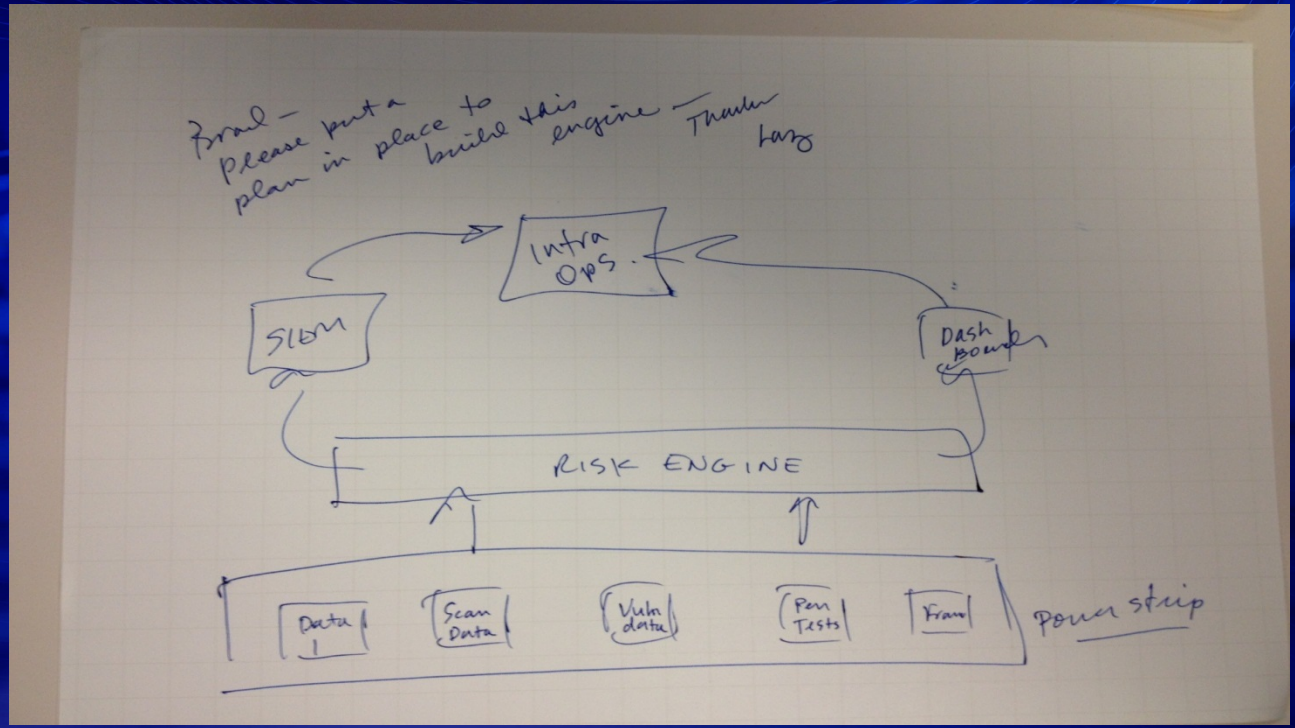
The Sears environment is complex

Executive Summary – Sears Online

- Sears Online has a massive amount of data
- We needed to reduce access to data from minutes to seconds
- We evaluated and compared solutions to support our vision – to build a next generation InfoSec platform internally called the “Threat < Alert Platform”
- Splunk was chosen as the foundation for the platform for a number of reasons
- We achieved great results – surpassing our expectations

Cyber criminals are evolving – we must as well

Original Architecture



From idea to functioning system within four months

Requirements for Building “Threat < Alert”

- Process a massive amount of data
- Be able to process different types of data
- Use for searching, reporting and alerting
- Searching and alerting have to be completed within seconds

We want to get rich data quickly and more efficiently!

Requirements – cont.

- Reliable and relevant alerting
- Easy to use
- Flexible to support future investments
- Support from the vendor was important

Approach & Methodology

- Documented all business requirements
- Compared various solutions
- Splunk was chosen as the foundation for the "Threat < Alert" platform

Splunk Exceeded All of Our Expectations

SEARS HOLDINGS

Threat < Alert Platform: Data

- How about the data?
  - Traditional Security Events
  - Vulnerabilities
  - System State
  - Community
  - Geography
  - Fraud
  - Cyber Intelligence Monitoring
  - Behavioral Analytics

Multi-Phased Approach

Phase 1	Phase 2	Phase 3

• Deployed Splunk in a small environment
• Learned more about Splunk
• Imported a subset of data feeds
• Learned more about our data
	• Defined and classified alerts
	• Created SOPs for alerts
	• Integrated with our Operations dashboard
	• Trained operations personnel on tool and SOPs
		• Added more data sources
		• Added advanced alerts utilizing:
		  • Correlation
		  • Trending
		  • Health Checks
		  • Added third-party data

2 Weeks/4 FTEs	6 Weeks/4 FTEs	8 Weeks/4 FTEs

Phase I - Deployed Splunk in a Small Environment

- Partnered with Performance team
- Set up a Search head for security team

Splunk is flexible!

SEARS HOLDINGS

Phase I – Learned More About Splunk

- The team started off trying the tool without instructions
- The team then used online resources
- Splunk was very helpful when we had questions

Over 80% of what we needed was there – out of the box!

Phase I – Imported a Subset of InfoSec Data Feeds

- Perform an inventory of available data
- OSSEC
- Added data from a sampling of network devices

Consider your data strategy

Phase I – Learned More About our Data

- Immediately saw interesting things
- Needed to normalize data
- Started to see other data being added

Be prepared to see data in different ways

Phase 2 – Added More Data

- Added WAF, Behavior Analytics & more
- Looked at other data being indexed

Phase 2 – Defined and Classified Alerts

- Performed Threat Modeling
- Created alert classification framework
  - Types:
    >1000 - 1999: Application-related alerts
    >4000 - 4999: Database-related alerts
    >6000 - 6999: Pattern & Trend alerts
    >9000 - 9999: User Generated Content alerts
  - Criticality:
    >Critical
    >Major
    >Minor
    >Informational
- Developed queries for the alerts

Phase 2 – Example Alert

- “Sniffer Detected”

  Interface entered in promiscuous(sniffing) mode. | `security_device_sos_IP_whitelist(src_ip)` | `TEMPORARY_sos__IP_whitelist(src_ip)`| `whitelist(src_ip)`

Start with more straightforward alerts

Phase 2 – Created SOPs for Alerts

- Created instructions for all alerts
  - Needed to be clear for SOC & others

Phase 2 – Integrated With Our Operations Dashboards

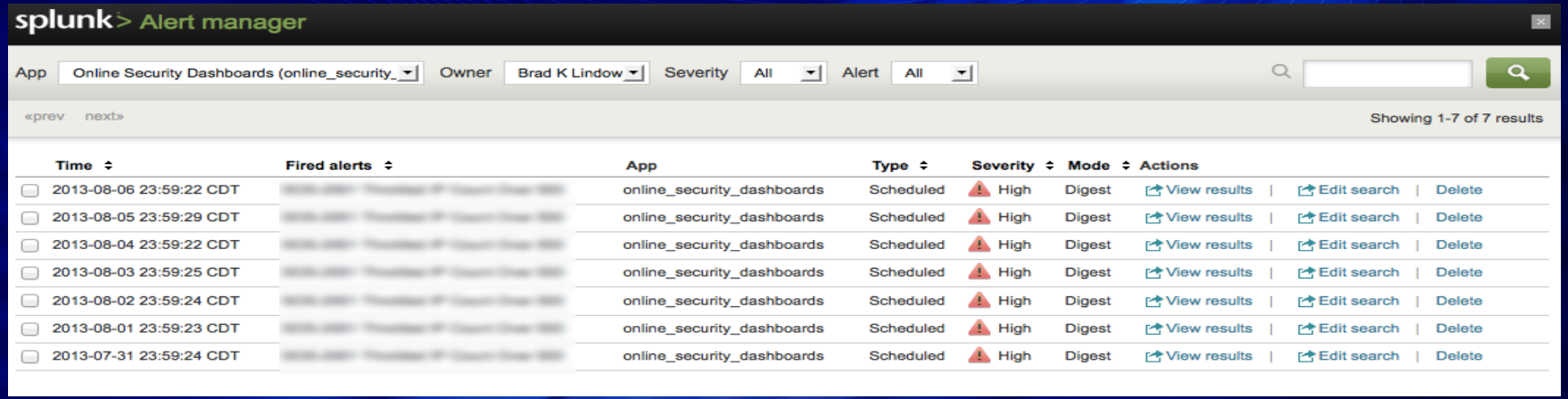
- Operations Center uses one dashboard for alarms
- Seamless integration was critical for us

Phase 2 – Dashboard Integration

Count	Severity	Ticket	First Occurence	Last Occurence	Summary
1	Critical	Pete	[Aug 12] 2:45 pm	[Aug 12] 2:45 pm	Security Event SOS-1004 Akamai WAF: XSS Detection IP:
1	Critical	checking	[Aug 12] 4:25 pm	[Aug 12] 4:25 pm	Security Event SOS-1007 Akamai WAF: SQL Injection IP:
1	Major		[Aug 12] 12:15 pm	[Aug 12] 12:15 pm	Security Event SOS-1030 Silvertail: Password resets (User) Site:
1	Major		[Aug 12] 12:25 pm	[Aug 12] 12:25 pm	Security Event SOS-1016 Silvertail: Excessive order status (IP) IP:
1	Major		[Aug 12] 12:25 pm	[Aug 12] 12:25 pm	Security Event SOS-1030 Silvertail: Password resets (User) Site:
1	Major		[Aug 12] 12:25 pm	[Aug 12] 12:25 pm	Security Event SOS-1030 Silvertail: Password resets (User) Site:
1	Major		[Aug 12] 12:35 pm	[Aug 12] 12:35 pm	Security Event SOS-1016 Silvertail: Excessive order status (IP) IP:

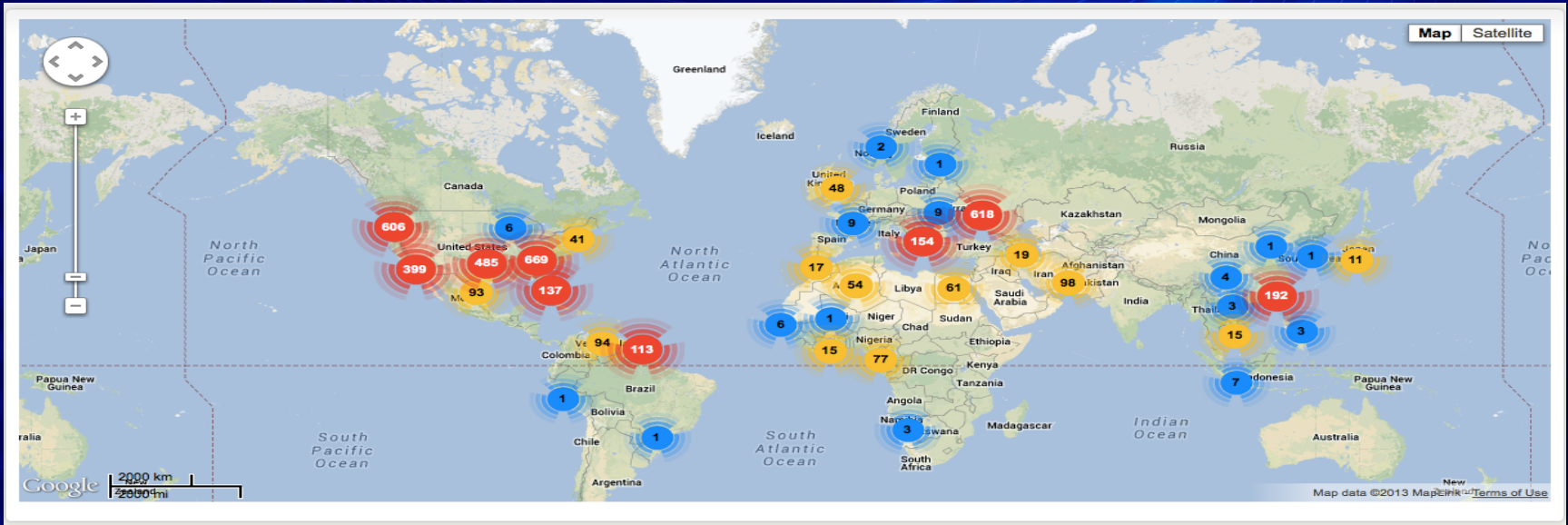
Visibility is key

Phase 2 – Splunk Alert Manager



You can manage alerts within Splunk

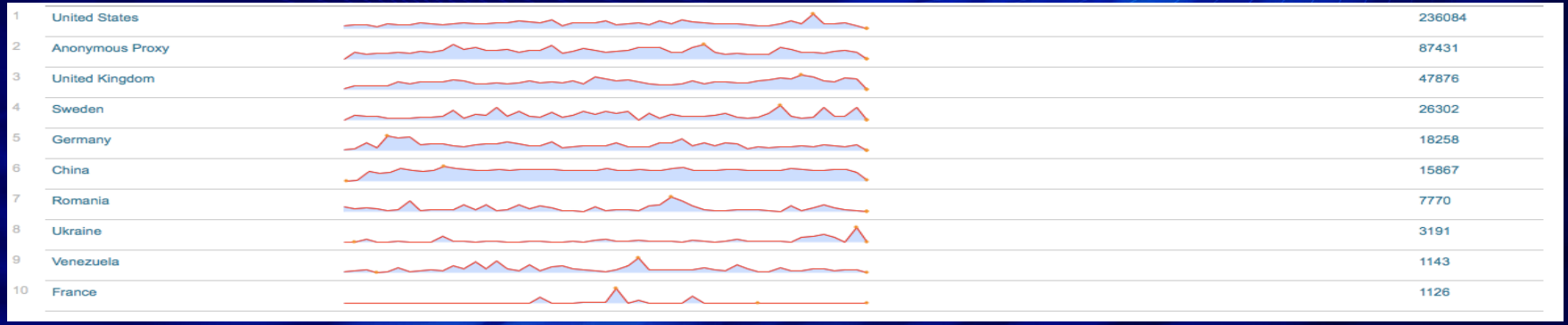
Phase 2 – Geospatial Visualization



Splunk makes data visualization easy

SEARS HOLDINGS

Phase 2 – Patterns & Trends



1	United States	236084
2	Anonymous Proxy	87431
3	United Kingdom	47876
4	Sweden	26302
5	Germany	18258
6	China	15867
7	Romania	7770
8	Ukraine	3191
9	Venezuela	1143
10	France	1126

Read Stephen Few's Approach on Data Visualization

Phase 2 – Trained Operations Personnel on Splunk

- 16 total team members working 24x7x365
- Trained the team every 2 weeks for 2 months
- The team caught on quickly – ramp up time was incredible

Phase 3 – Added More Data Sources

- Fraud Data
- Reputation Lists
- Health & Performance
- Vulnerability
- Used other indexed data

Did I mention that Splunk is flexible?

Phase 3 – Added Advanced Alerts

- New Alerts to support:
  - Trending & Statistical Analysis
  - Health Checks
  - Correlation
  - Third-Party Data

The Challenge Was Met!

- How do you take over 10 million possible security events per day and make sense of the data in less than 4 months?
- With proper planning – this is very achievable!

The solution must protect the brand and be transparent to the end users

Use Case – Investigation

- What: Your WAF indicates possible malicious behavior from a particular IP and you need to investigate
- Before:
  - Who: SOS, Sys Eng, Net Eng, Middleware, Performance, Ops
  - How: Personnel need to check 10 different data sources and correlate events
  - When: ~90 minutes
- After:
  - Who: SOS, Ops
  - How: Check Splunk for all activity for that IP, associated users, etc.
  - When: ~10 minutes

Next Steps

1. Further development of intelligent correlation-based alerting
2. Machine learning
3. Predictive analytics
4. Integrate mitigation actions with Splunk
5. Investigating the Splunk app for Enterprise Security to augment what we've built
6. Further Integrating transaction-based Fraud data

Lessons Learned

- Plan out indexes for different data from beginning
- Tuning needs to be continual
- Organize white and black lists up front
- Volume of data/alerts may be huge
- Daily meetings were effective
- Collaborate with multiple stakeholders – data is valuable
- Utilize Splunk expertise in coaching your team

Quick Recap

- Start small
- Normalize data
- Prioritize threats
- Systematically created alerts & SOPs
- Tune continuously
- Use any sort of data relevant to you

Getting great results quickly can be be pretty easy

Questions?

SEARS HOLDINGS

Thank You!

Brad Lindow
The Security Architect
Sears Online Business Unit (OBU)

Brad.Lindow@searshc.com