.conf2015

# Splunk Cloud as a SIEM for Cybersecurity Collaboration

Timothy Lee

CISO, City of Los Angeles

splunk>

# Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

# City of Los Angeles


- 4 million people, 465 sq mi, 15-Council District
- 2nd largest city in the US
- 1.8 million employed
- 42.2 million annual visitors
- 42 departments with 35,000 FTE
- Port of LA,  Airport, Water and Power – 3 proprietary departments all managing their own networks
- Information Technology Agency (ITA) manages the rest

# Our Challenge

- IT Security Team is understaffed
- Dispersed log capturing capabilities
- Minimal use of collaboration tools
- Lack of Incident Management platform
- No integrated threat intelligence program
- Limited situational awareness and operational metrics for City as a whole
- Imbalance in response capability
- Growing cyber threats including DDoS & Malware

# Mayor's Executive Directive on Cybersecurity

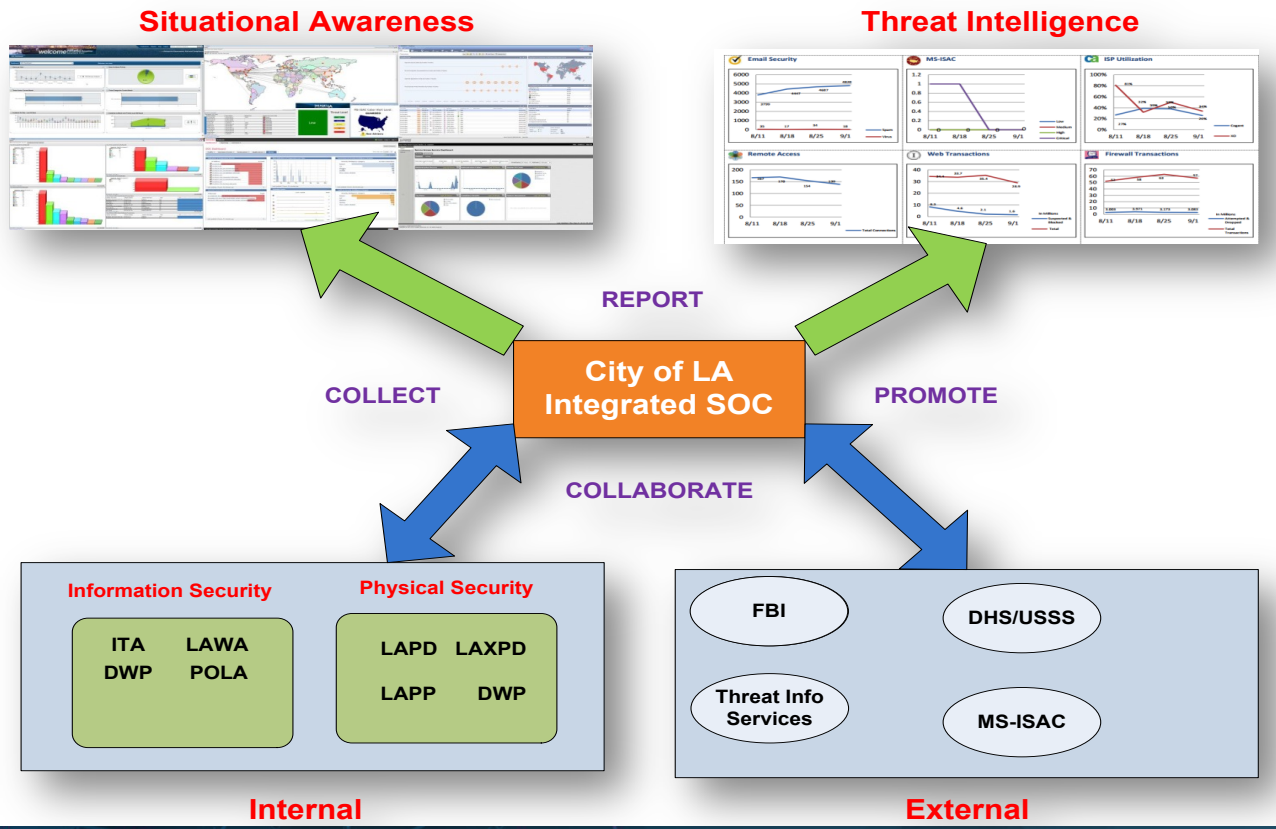
- Facilitate the identification and investigation of cyber threats and intrusions against City assets
- Ensure incidents are quickly, properly, and thoroughly investigated by the appropriate law enforcement agency
- Facilitate dissemination of cybersecurity alerts and information
- Provide uniform governance structure accountable to City leadership
- Coordinate incident response and remediation across the City
- Serve as an advisory body to City departments
- Sponsor independent security assessments to reduce security risks
- Ensure awareness of best practices

# Our Solution

Integrated Security Operations Center

*Leveraging Splunk Cloud and Splunk Enterprise Security*

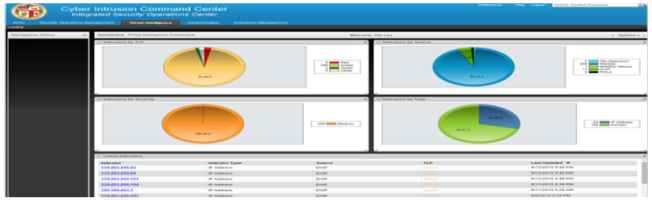
# Integrated Security Operations Center



# Integrated Security Operations Center

## Situational Awareness

## Threat Intelligence Portal



CICC ISOC Security Operations Management

**Threat Intel Feeds**

- MS-ISAC
- Vendor Feeds
- FBI Cyberhood Watch

splunk>

Forwarder

splunk>

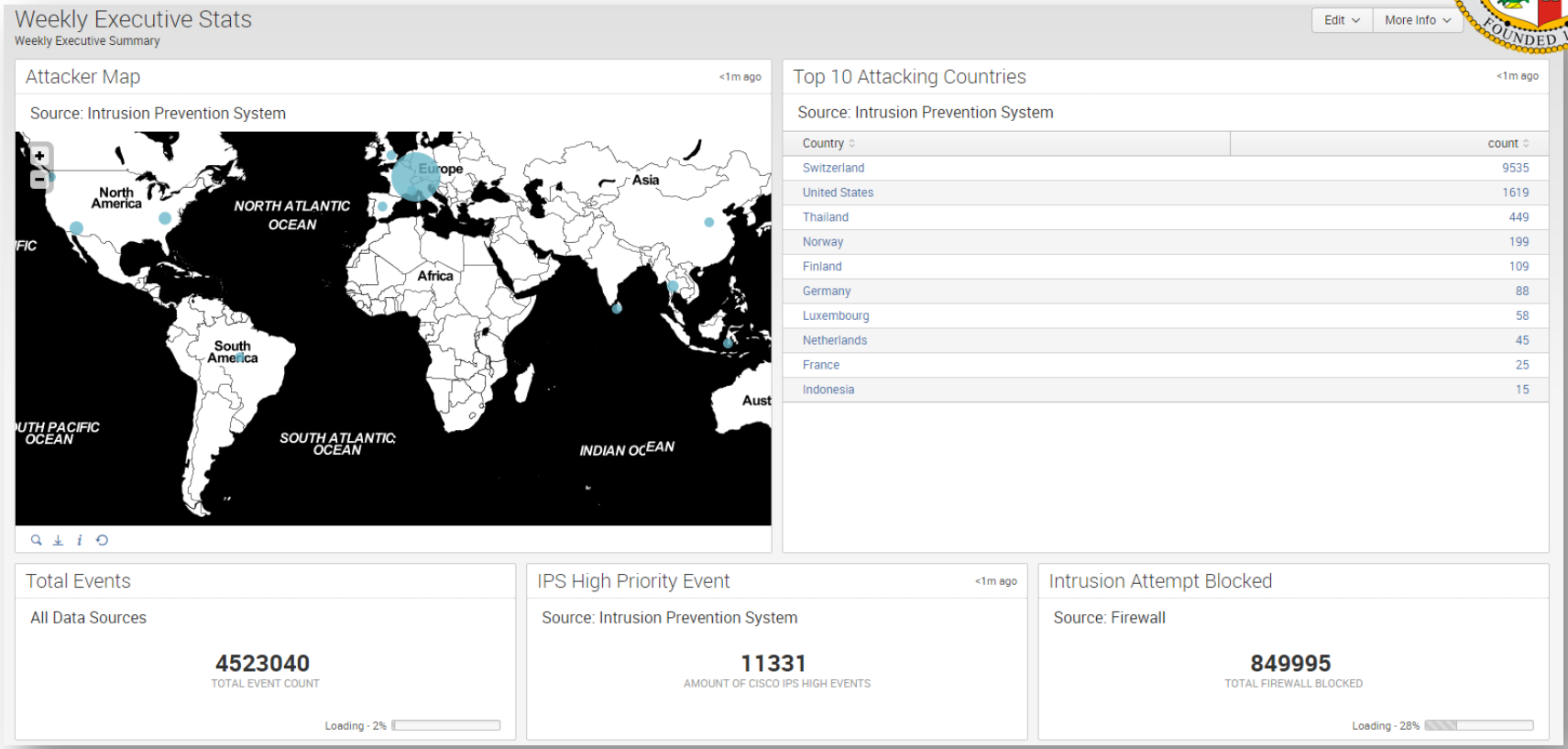
**Log Sources**

- Firewall
- IDS/IPS
- Proxy
- Endpoint Protection
- Active Directory
- Network Access Control
- Routers/Switches

# How Did We Sell It Internally?


- Prepare to answer why you need SIEM and why cloud-based
  - Security Audit Report (Recommendation and Action Plan)
  - Compliance Gap Assessment Report
  - Security metrics (numbers of intrusion attempts, incidents, outages caused by incidents, top attackers, threat activity and trends etc.)
  - Present it from the business risk perspective
- Engage others outside of IT to also help sell it
- Provide potential risks of not implementing SIEM
- Share real-world examples of cyber incidents and costs that your audience can relate to
- Provide source of funding for implementation and operations
- Align results to organizational goals

# Example: Executive Dashboards



# Use Case Example: Top Attackers


Explore Splunk Enterprise

Executive Stats

Just the numbers.

IPS Attacker Country (1w) 1m ago

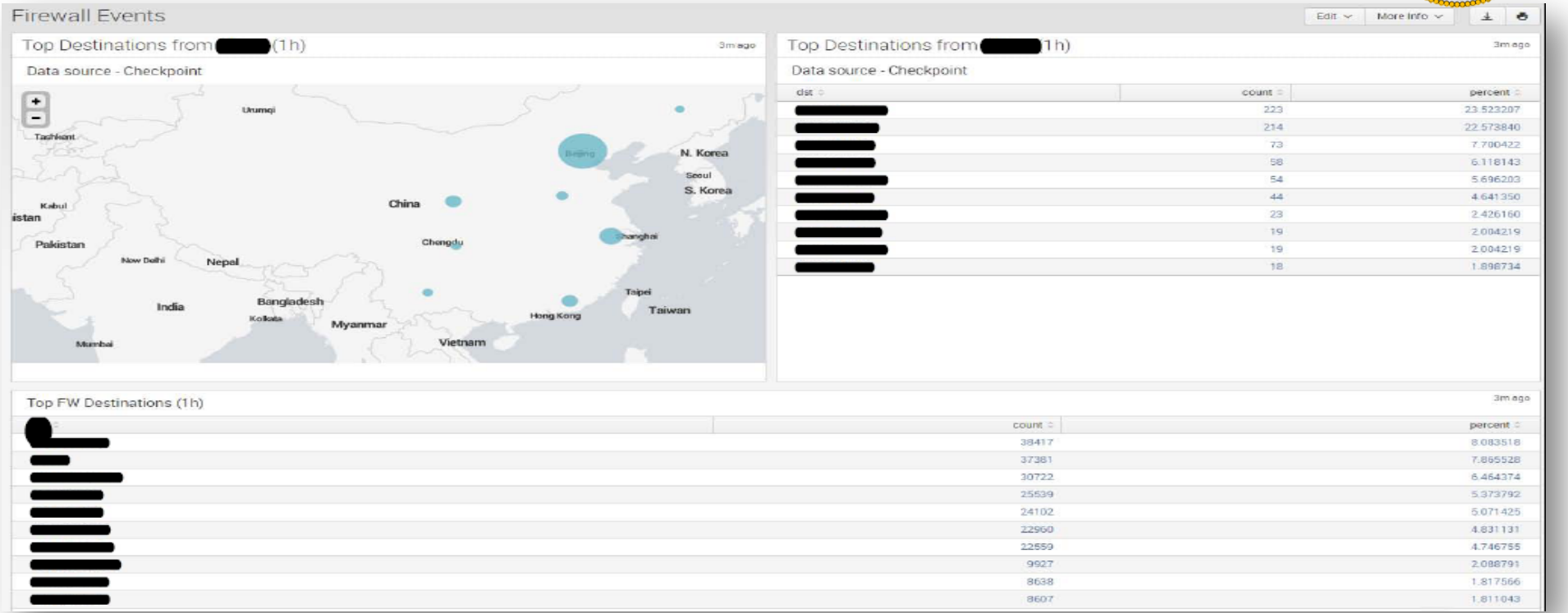
Data source Cisco IPS


List of Top Attacking Countries (1w) 1m ago

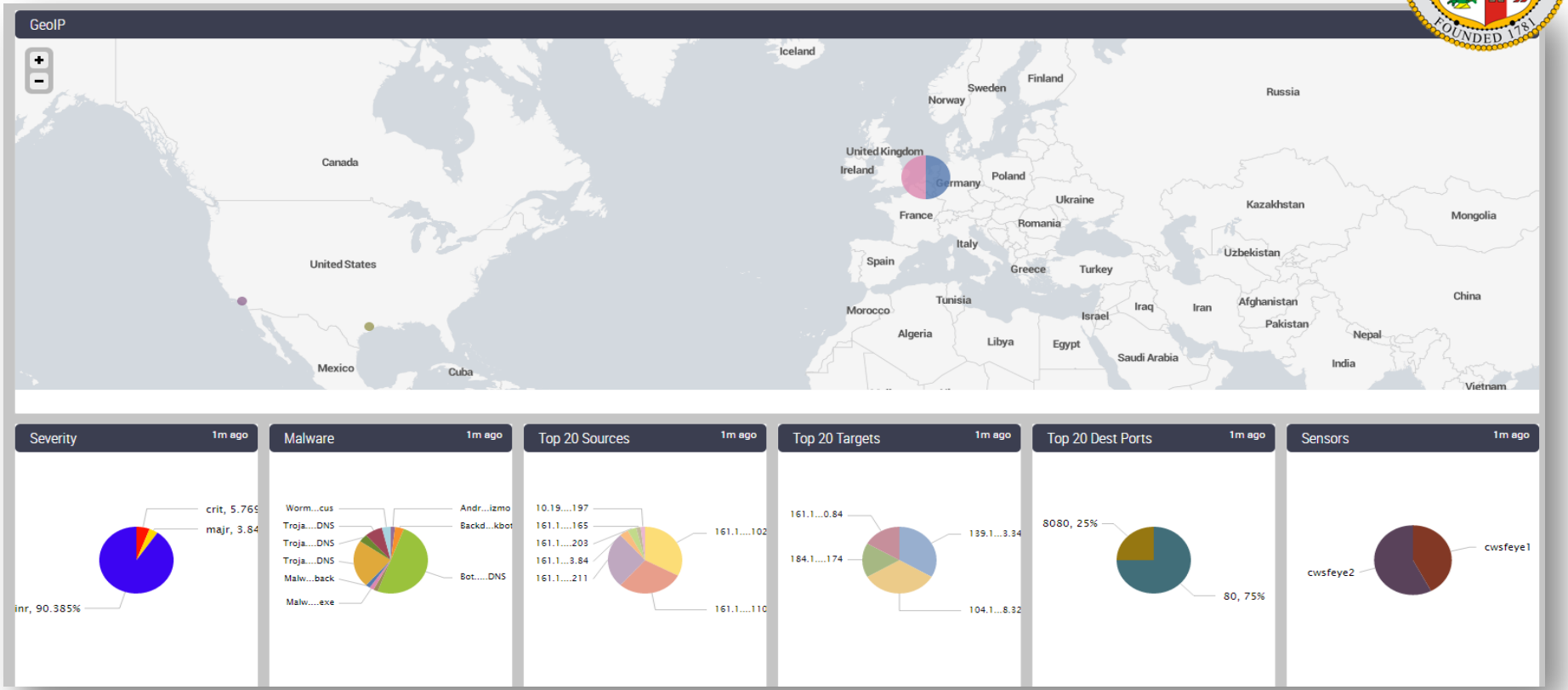
Data source Cisco IPS

| Country | count |
|---|---|
| Thailand | 449 |
| Norway | 199 |
| Finland | 109 |
| Germany | 88 |
| Luxembourg | 58 |
| Netherlands | 45 |
| France | 25 |
| Indonesia | 18 |
| Ukraine | 15 |
| China | 12 |

# Use Case Example: Top Destination By Specific Attacker



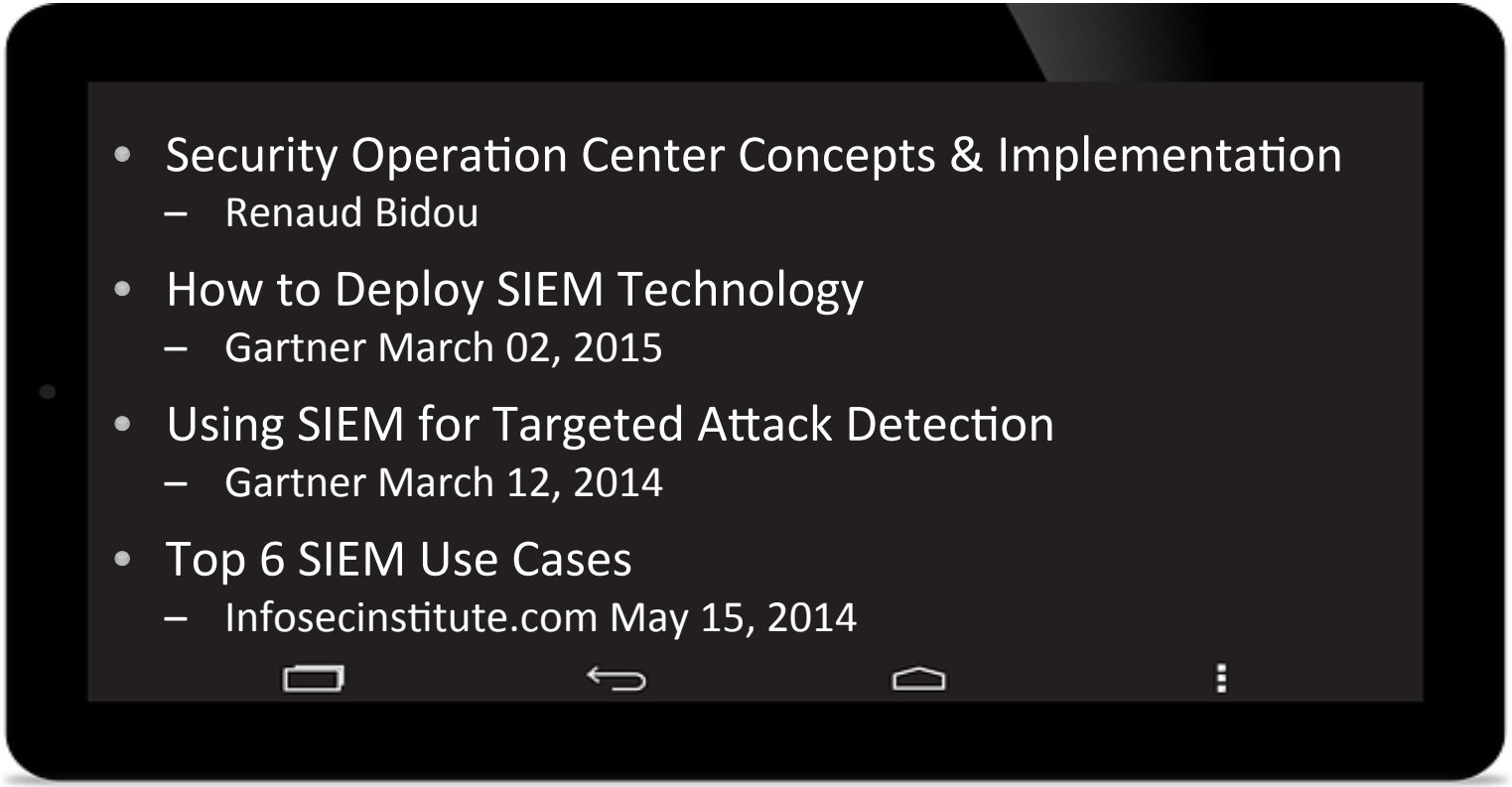
# Use Case Example: Malware Monitoring



# Lessons Learned

- Conduct SOC readiness assessment before anything else
- Prepare to answer why you need CSOC
- Look for grant opportunities
- Pick the right tools and technology
- Be mindful of operating costs
- Pick the right contractor
- Pick the right team. Invest in people.
- Cybersecurity collaboration and information sharing are essential

# Resources


• Security Operation Center Concepts & Implementation
– Renaud Bidou
• How to Deploy SIEM Technology
– Gartner March 02, 2015
• Using SIEM for Targeted Attack Detection
– Gartner March 12, 2014
• Top 6 SIEM Use Cases
– Infosecinstitute.com May 15, 2014


# Q&A

splunk>


# THANK YOU

splunk>