RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SPO2-W03

Providing First-Rate Security Services With Analytics-Driven Security

Stephen Fisher

VP Network Planning & Security
Integra

#RSAC

About Integra

- Integra is one of the largest regional facilities-based providers of carrier-grade networking, communications and technology solutions in the western United States. Through our business units, Electric Lightwave and Integra Business, we provide critical connectivity, Unified Communications, managed and cloud services, and security services to domestic and international customers, including large enterprises, government customers, wholesale customers and regional business customers.

Challenges We Faced

- Wide Range of Security Requirements
  - Internal audits (Financial, PCI)
  - Contractual security program requirements with customers
  - Internal information and asset protection
  - Security products (Cloud Firewall/DDoS)

- Cultural and Organizational Challenges
  - Security not a priority for everyone
  - Outsourced security operations
  - Limited resources
  - Data not available for security operations
    - Information hoarders and data silos

An Ambitious Goal

Create a comprehensive balanced information security program with management, operational and technical security controls.

- ✓ Secure Integra’s information/assets
- ✓ Enable security products to be secure

Mission:

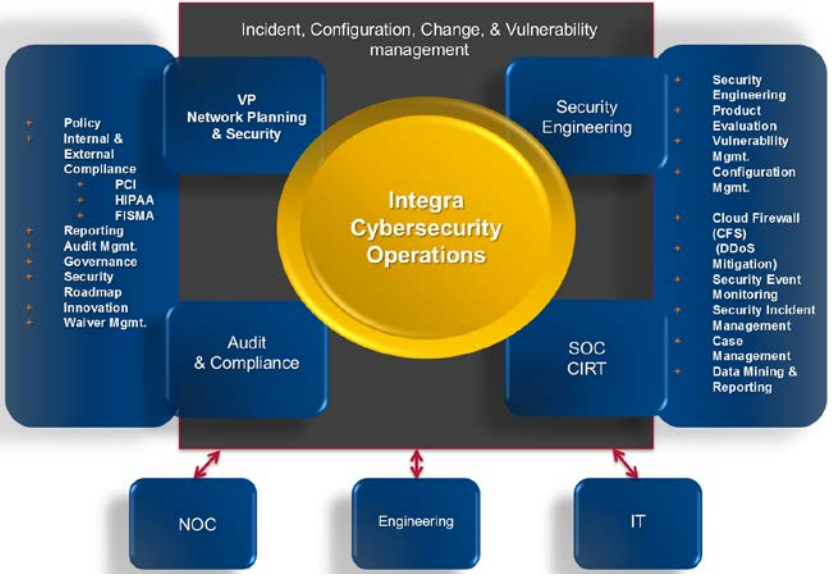
- ✓ Create security program valuing transparency, accountability and oversight
- ✓ Ensure the success of the company’s mission
- ✓ Support the missions of our customers

Our Plan to Cross the Chasm

- Build a SOC in eight months
- Buy the right tools and implement the ones we have!
- Break down the silos
- Don’t just identify problems – solve them
- Don’t repeat past mistakes

Build a SOC in 8 Months

- **Why we insourced a SOC**
  - Needed to change the culture
  - Needed control to get things done
  - Needed a evangelist for security
- **Building the SOC**
  - Find a location
  - Procure & setup SIEM infrastructure
  - Redirect all logs to SIEM
  - Re-allocate resources
  - Hire additional staff
  - Train staff
  - Define SOC incident response policies and procedures
  - Transition from outsourced SOC



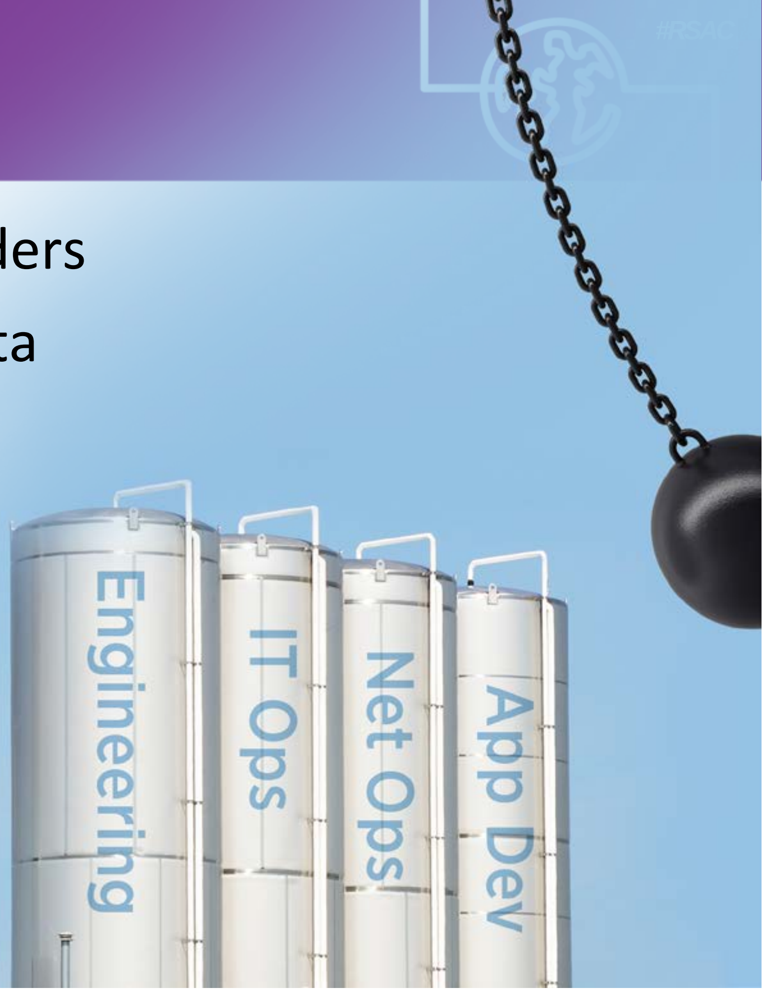
Flexible and Comprehensive Tools

- Meet both the Data Owner and Security requirements:
  - Support our security and non-security needs
  - Provide visibility across the organization
  - Deliver immediate value
  - Meet our longer term goals to be proactive and predictive

- Solve many organizational challenges:
  - Give the organization a reason to care (break the silos)
  - Increase visibility across the organization
  - Fast time to value and low TCO justifies the investment

Break Down the Silos

- Support the needs of individual stakeholders
- Show them a better place to put their data
- Solve their use cases
- Sell the value of sharing!

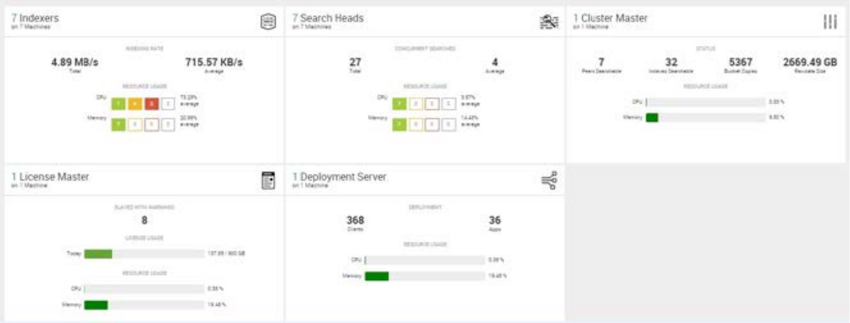


Engagement & Big Data Architecture

Engage Professional Services:

- Interview key stake holders (data owners)
- Identify and prioritize the data sources
- Document findings in a priority matrix
- Deliver an overall architecture

All Virtualized – RHEV with RHEL



7 Indexers
on 7 Machines
4.89 MB/s
Total
715.57 KB/s
Average
CPU
Memory

7 Search Heads
on 7 Machines
27
Total
4
Average
CPU
Memory

1 Cluster Master
on 1 Machine
STATUS
7
32
5367
2669.49 GB
CPU
Memory

1 License Master
on 1 Machine
8
Today
CPU
Memory

1 Deployment Server
on 1 Machine
368
36
CPU
Memory

1 Search Head Cluster (3 Search Heads) +

2 User Specific Search Heads + 1 Deployment Server

1 Enterprise Security Search Head

7 Indexers

10 Heavy Forwarders

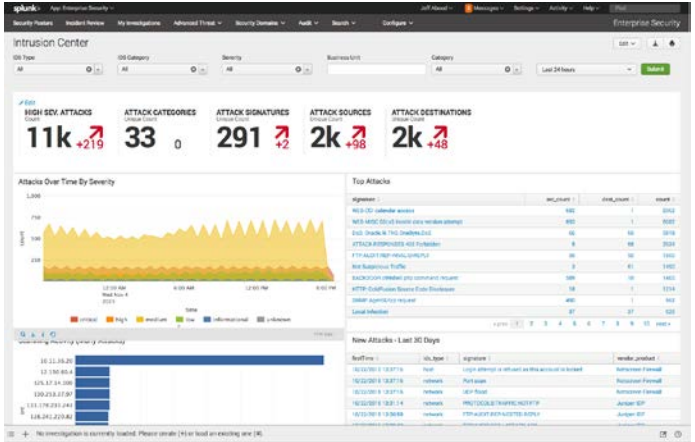
1 SNMP Forwarder

1 NetApp VM Ware Forwarder

Use Case #1

Security Challenge:

- Detection and response to possible brute force attacks
  - Check for brute force patterns from logon events
    - Active Directory
    - Win: Security logs
    - Cisco Secure ACS logs
    - Unix authentication logs



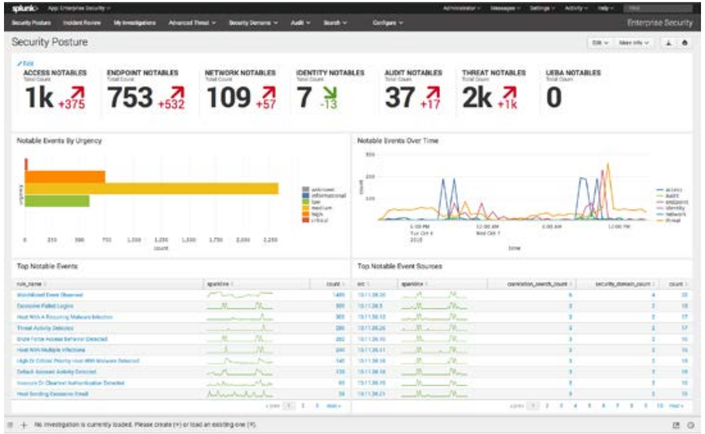
How the data Helped:

- Facilitated rapid detection and deep investigation
  - Enabled SecOps to detect the attempts
  - Provided substantial forensic data
    - Determined source of the attack
    - Identified compromised systems

Use Case #2

Security Challenge:

- Detection and response to web application security
  - – Aggregate and correlate logs from web application systems
    - WAF
    - SQL servers
    - web servers



How the data Helped:

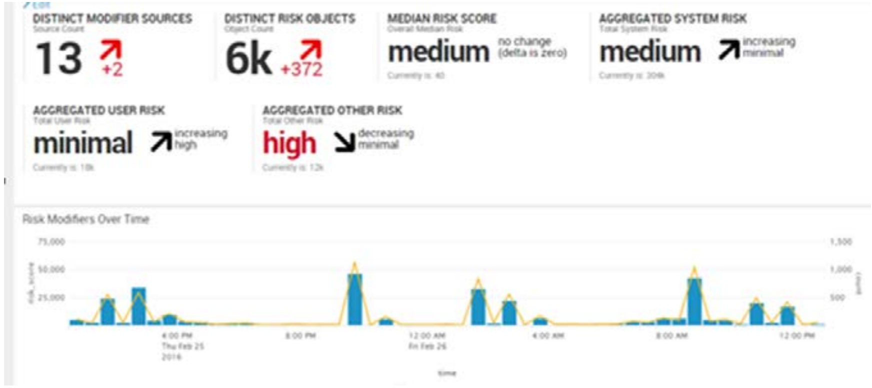
- Enabled detection of potential web application attacks
  - – SQL injection
  - – Cross site scripting
  - – Buffer overflow attempts

Integra

Use Case #3

Security Challenge:

- Detection of suspicious behavior from log sources
  - Correlation of organization-wide machine data
  - Analysis of security and non-security data



DISTINCT MODIFIER SOURCES
Source Count
13 +2

DISTINCT RISK OBJECTS
Object Count
6k +372

MEDIAN RISK SCORE
Overall Median Risk
medium no change (delta is zero)
Currently is: 40

AGGREGATED SYSTEM RISK
Total System Risk
medium increasing minimal
Currently is: 204k

AGGREGATED USER RISK
Total User Risk
minimal increasing high
Currently is: 18k

AGGREGATED OTHER RISK
Total Other Risk
high decreasing minimal
Currently is: 12k

Risk Modifiers Over Time

How the data Helped:

- Discovered compromised JetDirect cards
  - Able to index, correlate and analyze data from all device types
  - Rapidly discovered common patterns and trends

Integra

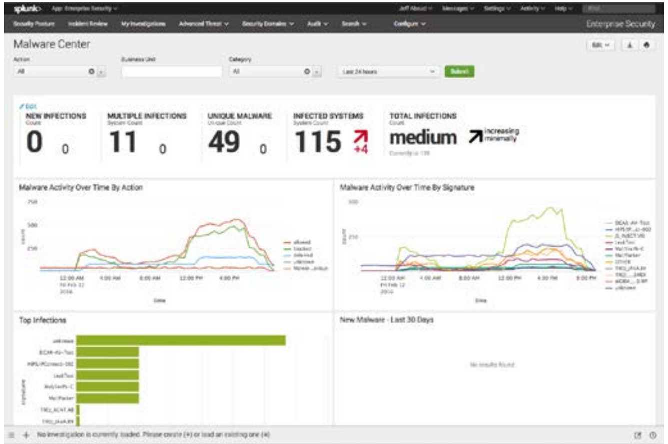
Use Case #4

Security Challenge:

- Detection and response to malware
  - Anti-malware alone is insufficient

How the data Helped:

- Able to ingest and correlate all log data – from perimeter to endpoints
  - Enabled rapid malware detection
  - Facilitated rapid threat mitigation



No investigation is currently loaded. Please create (+) or load an existing one (#)

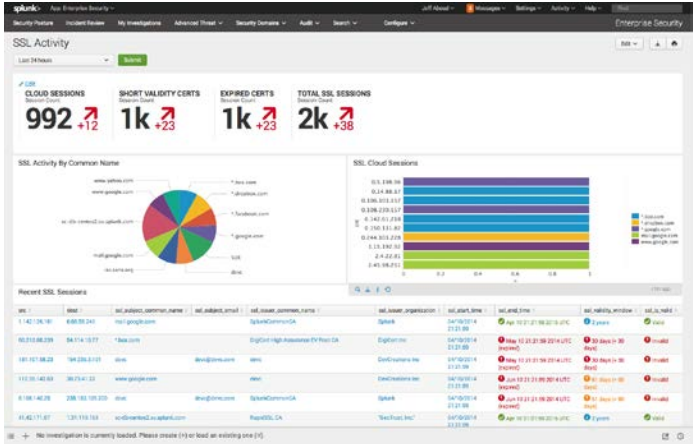
Use Case #5

Security Challenge:

- Detection and response to anomalous ports and services
  - Unpatched systems introduce ingress points

How the Data Helped:

- Delivered visibility across the IT deployment
  - Able to observe services starting out of the ordinary
    - Overutilization of ports
    - SSH and SSL sessions generating high volumes of traffic
    - Other unusual internal/external traffic patterns



SSL Activity

CLOUD SESSIONS 992 +12

SHORT VALIDITY CERTS 1k +23

EXPIRED CERTS 1k +23

TOTAL SSL SESSIONS 2k +38

RSAConference2016

Key Takeaways

- Engage and enable the business
- Create a balanced information security program
- Employ a solid foundation of security controls first
- Don’t be overwhelmed – take one step at a time
- Create security program valuing transparency, accountability & oversight
- Remove the limits of outsourced security operations