Leveraging RSA NetWitness in Small Information Security Teams

Lars Giusti, Senior Manager - Information Security (Seattle, WA)

https://www.linkedin.com/in/lgiusti

#RSACharge

RSA Charge 2016

"You must pinky-swear to never reveal our company secrets. That's the cornerstone of our new information security program."

The Organization at a Glance

- Approximately 1400 users
- 2683 assets (devices to manage)
- 5 main sites & 3 micro sites across the globe
- 1 data center
- Publically traded company
- Technology sector
- Mix of On-Premise & Cloud Infrastructure
- Events Per Day/Events Per Second (EPD/EPS) see next slide

Core Data Generated Per Day

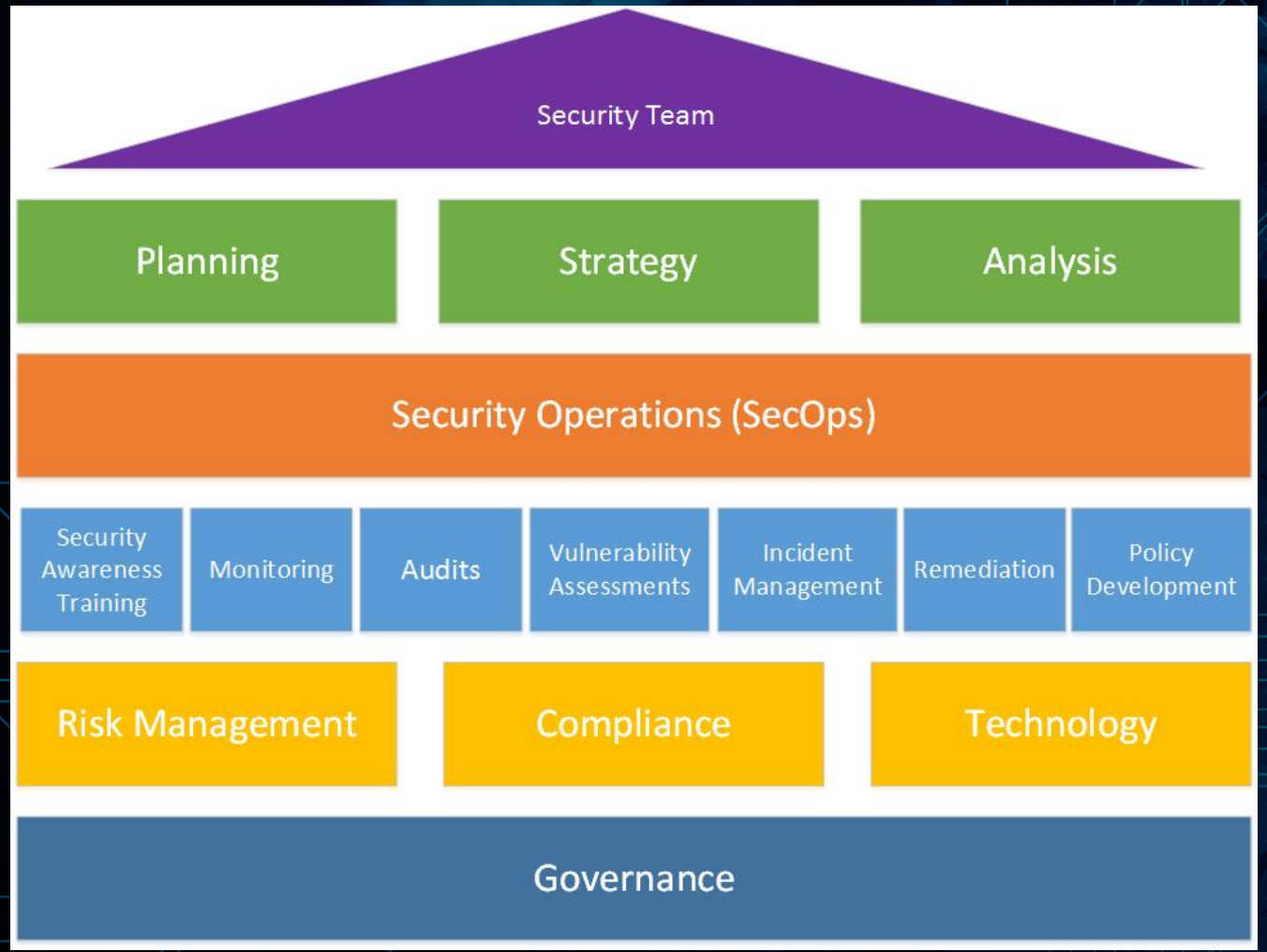
FIREWALL/ROUTER-		
SITE:	PACKETS:	FLOWS:
1	8,272,000	186,583,000
2	1,322,000	5,353,000
3	1,068,000	30,910,000
4	89,000	2,546,000
5	97,200	2,330,357
Total=	10,848,200	227,722,357

CREDENTIALS-			
AREA	EVENTS PER DAY	EVENTS PER SECOND	SIZE
Active Directory	31890636	369	6.8 (GB)

EMAIL-			
AREA	EVENTS PER DAY	EVENTS PER SECOND	SIZE
Mail	12372721	143	53733 (KB)

SYSTEM/SECURITY-			
AREA	EVENTS PER DAY	EVENTS PER SECOND	SIZE
Security	4882155	57	42417 (KB)

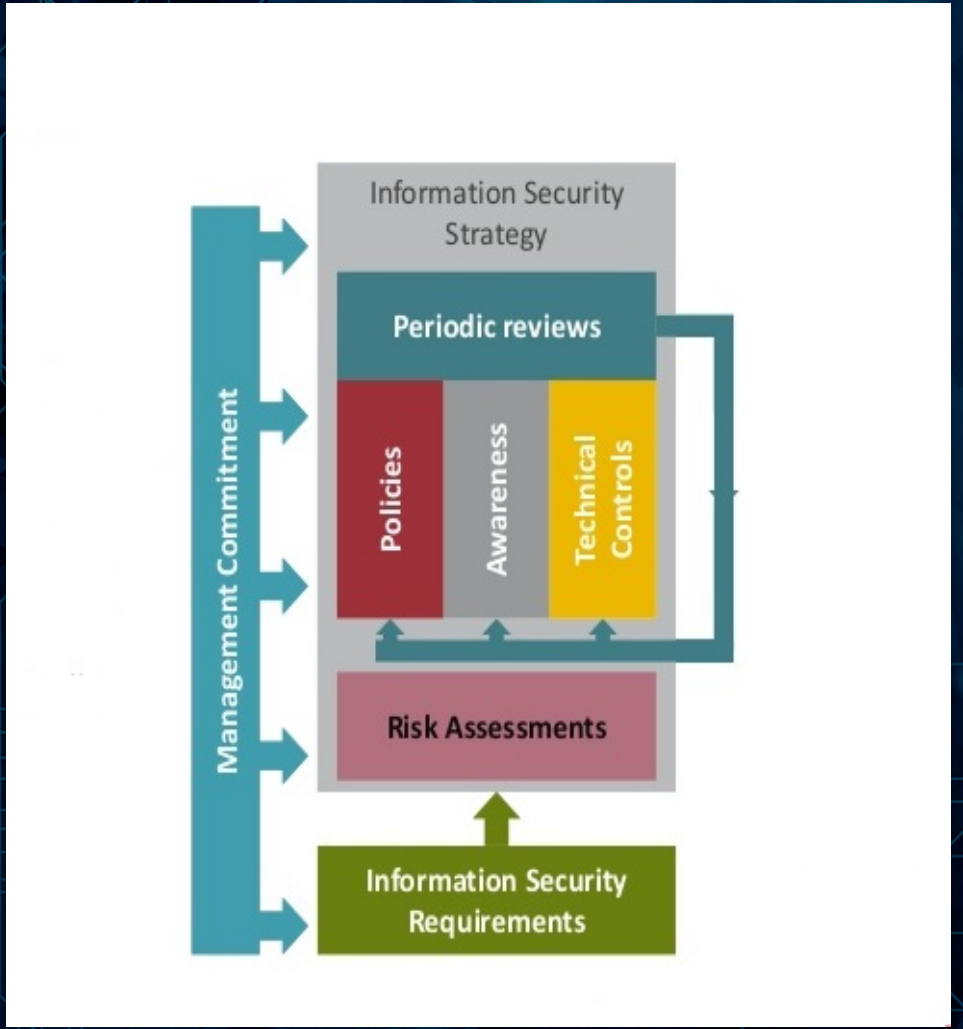
Building Blocks: The Information Security Program



- The Harmonious Cycle!
- Create a 2-3 year roadmap
- Strategy flows down
- Your Building Blocks Ensure Governance
  - Risk Management
  - Compliance
  - Technology Representation
- Lessons Learned Flow Back Up
- The Cycle Does Not Stop!

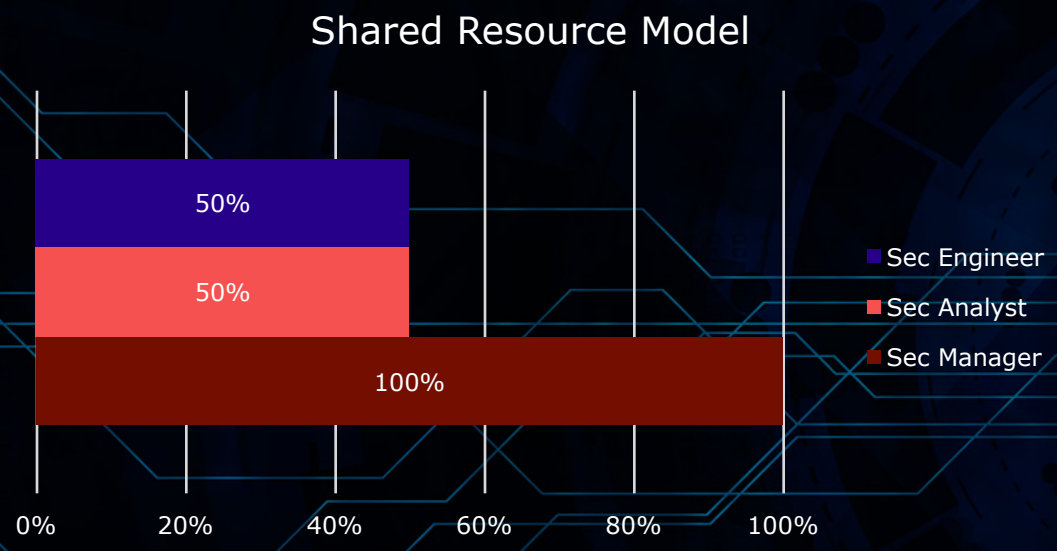
Ten Steps to Security Team Success

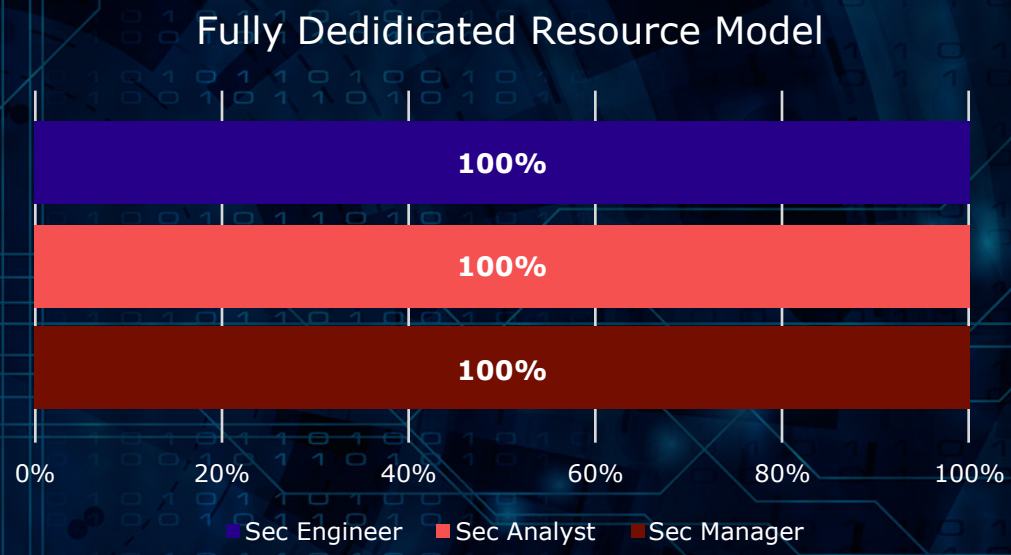
1. Identify critical *Information Assets* to the business
2. Conduct *Periodic Reviews*
3. Study the technical *Threat Landscape*
4. Define *Information Security Strategy*
5. Obtain *Management Support*
6. Develop a 3-year *Roadmap* (project plans)
7. Engage *Partners*
8. *Execute* on strategy
9. *Measure Deliverables* against project plan
10. *Repeat* Steps!



Information Security Team Resource Models

- Shared vs Dedicated
- Security team members may be split across multiple projects
- Security Analytics platform roles (operators, admins, analysts)
- Security Analytics is the backbone to your security operations (SecOps)





#RSACharge

RSA Charge 2016

Improving Security Operations with RSA NetWitness Security Analytics

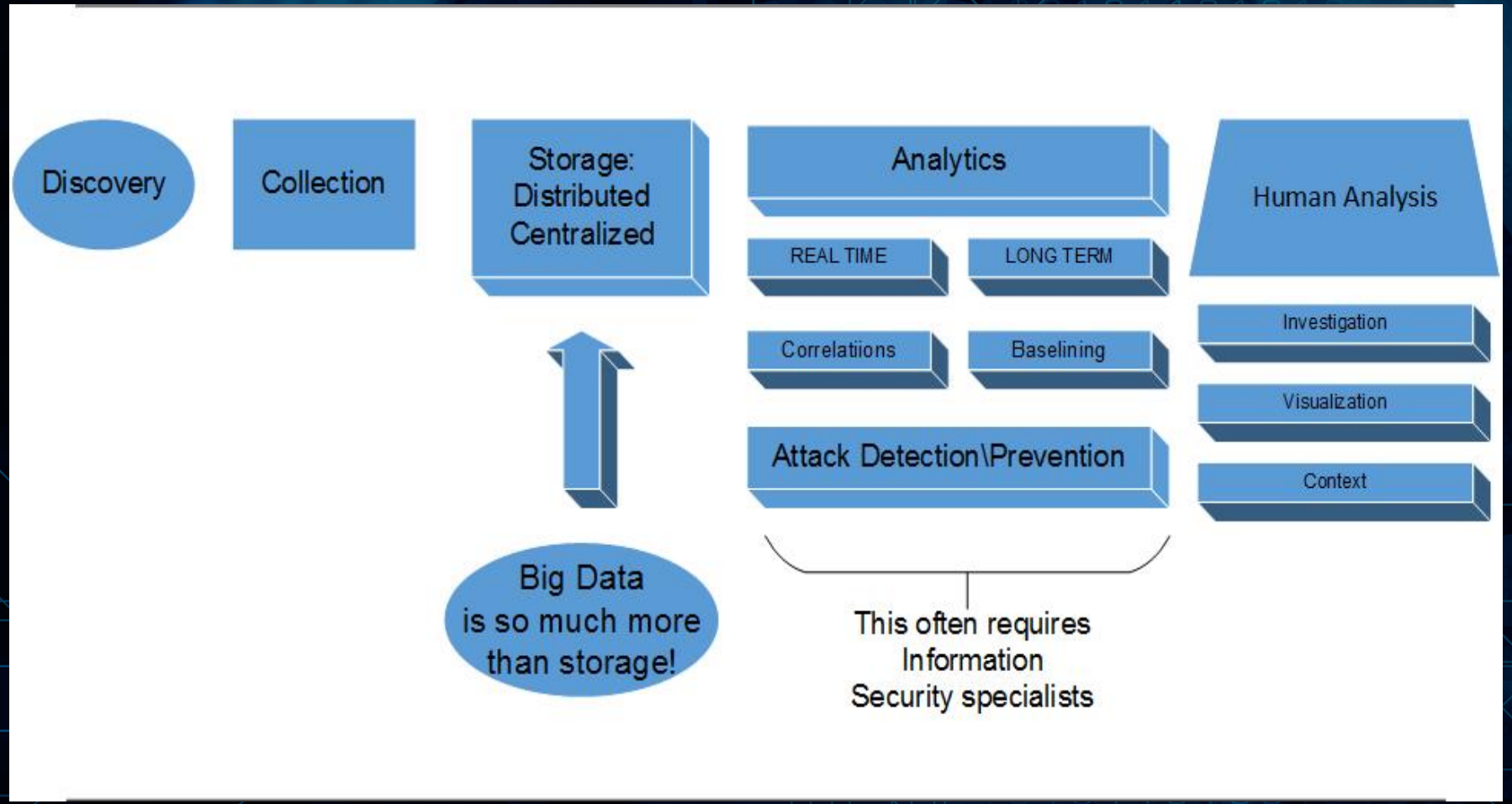
YESTERDAY (2013):

- Thin slices of visibility
- Disparate data sources
- Lack of context
- Decisions took a long time
- Struggling with switching between tools
- Very reactionary

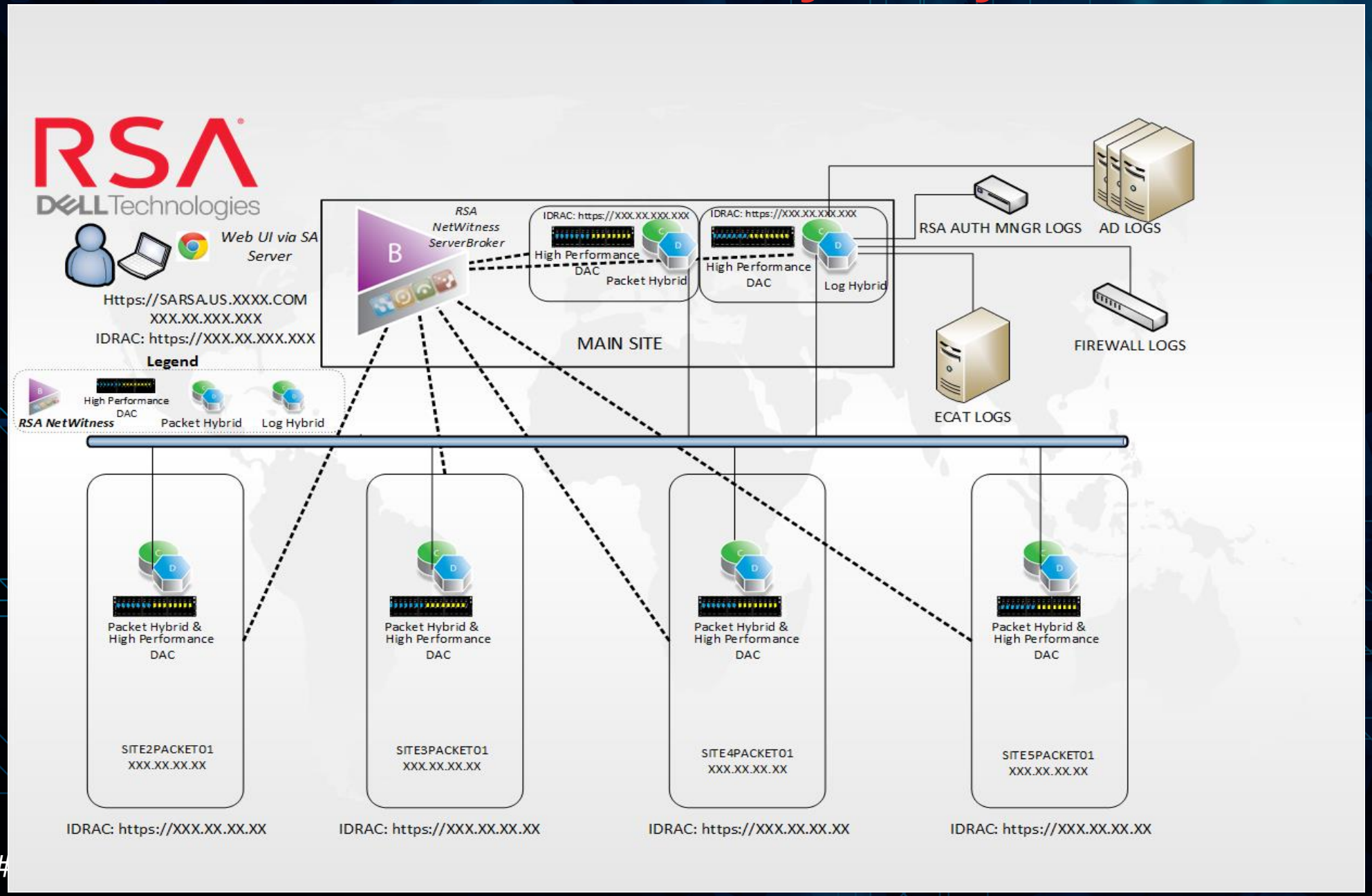
TODAY (2016):

- Vastly improved visibility
- Improved workflow with integration
- Deeper security context
- Better & quicker decision making
- Powerful correlation of data
- Improved data visualization

Big Data Flow From A Security Perspective



Our RSA NetWitness Security Analytics Network Diagram



Putting RSA Security Analytics to Work!

- Indicators of Compromise (IoCs)
  - Finding malware infected hosts
  - Assessing high risk file types
  - Malware beaconing & ransomeware detection
- Data Leakage
  - Analyzing outbound data transfers
- Black listed IP Addresses & Black listed URL activity
- Compliance Failures
  - User behaviors (not adhering to company policies)
- Tor Anonymizing Activities
- Nation State Activity
  - Suspicious activities
  - Network anomalies

Questions & Answers

Leveraging RSA NetWitness in Small Information Security Teams

RSA Charge 2016

Please Complete Session Evaluation

#RSACharge

RSA Charge 2016

#RSACharge