RAPID7

Security Data & Analytics

From Prevention to Detection & Response

Pim van der Poel
Rapid7

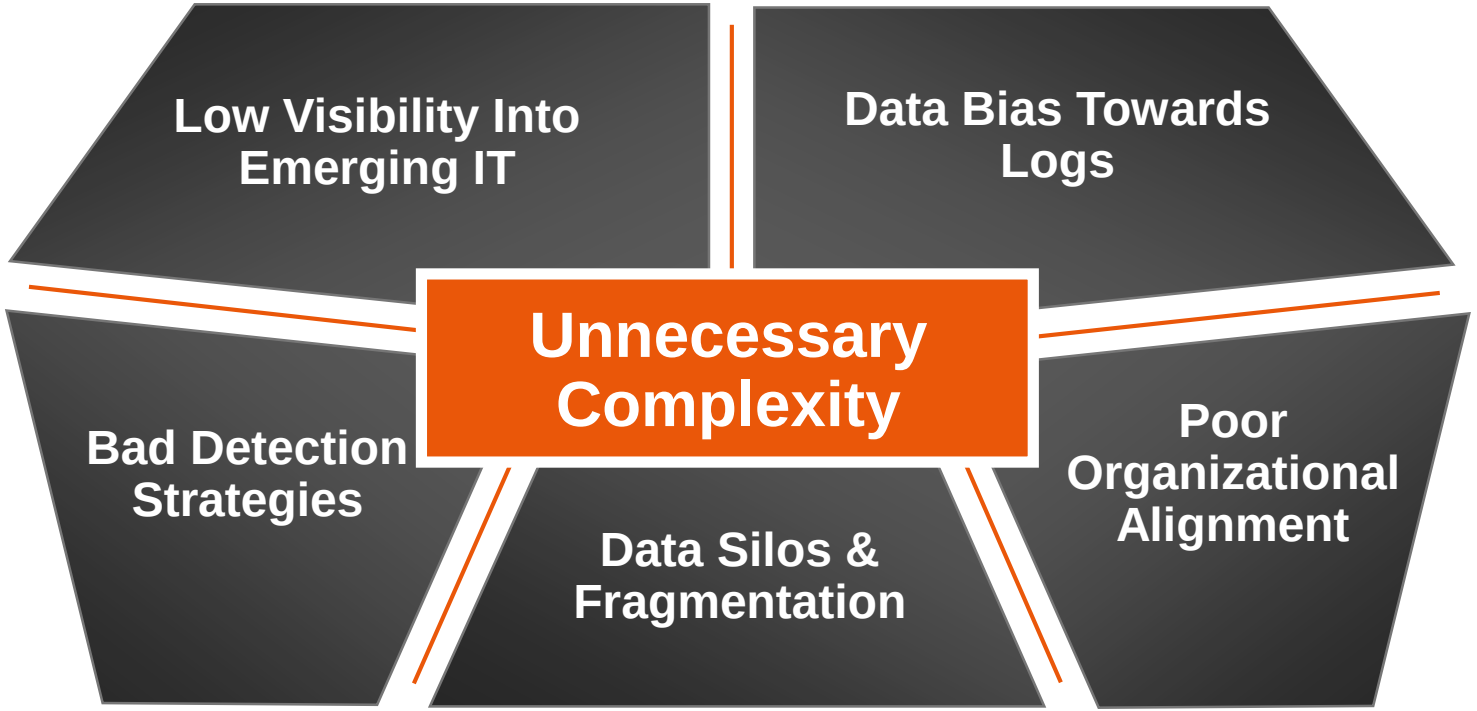
June 2016

Delivering Security Data & Analytics

that revolutionize the practice of cyber security

5,200+	37%	99	800+
Customers	Fortune 1000	Countries	Employees

The Shadow Challenge – Detection & Investigation



Fixing the Visibility Problem – Emerging IT

Expanding attack surface

79% of companies allow the use of approved cloud services…

67% of companies don't have visibility into those services.

2015 Incident Detection & Response Survey

IDR Survey Results

Figure 5: Tell us about your incident response spending.

Answered: 270 (99%) Skipped: 1 (1%)

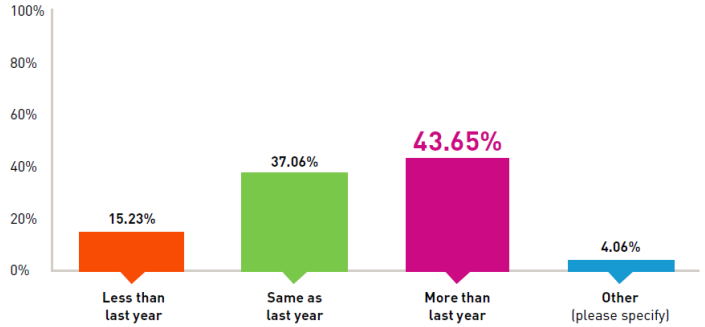
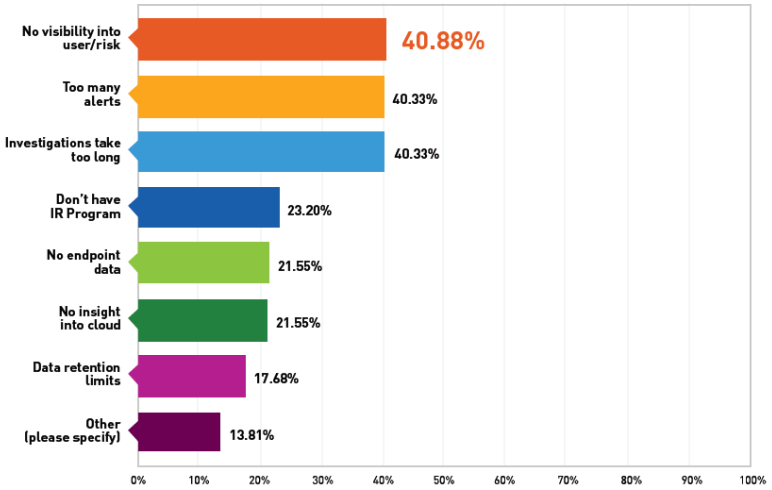


Figure 7: What are major sources of pain with your Incident Response Program?

Answered: 181 (67%) Skipped: 90 (33%)



Top Survey Themes

Security teams are strained

Strained sec team; incomplete ecosystem coverage

Compromised Credentials

90% of respondents worry about creds, only 40% can detect

SIEMs = too many alerts

62% orgs receiving more alerts than they can investigate

Eliminating the Blind Spots Created by Data Bias

Frequently Collected Data	Occasional Collected Data	Rarely Connected but Essential Data
Data Center Logs	Vulnerability Data	Endpoint Logs
	Asset Inventory	Processes & Services
		Asset Configuration
		Intruder Traps
		Application Behavior

Leading Indicator of Bad Detection Strategies

Too many alerts to investigate

62% of companies are receiving more alerts than they can investigate.

90% of companies say compromised credentials are a concern…

60% of companies cannot detect credentials based attacks.

2015 Incident Detection & Response Survey

How Detection Works Today….

- Collect data center logs
- Spend massive amounts of money to create static rules based on machine anomalies
- Get high quality alerts for a short period
- IT evolves through natural change cycle
- Everything becomes an anomaly
- **Reach alert overload and fatigue**

How Attacks Work – The Attack Chain

Infiltration and Persistence

- Phish users
- Use leaked credentials
- Connect to network
- Anonymize access
- Deploy backdoors

Reconnaissance

- Get user list
- Scout targets
- Find vulnerabilities

Lateral Movement

- Access machines with credentials
- Collect more passwords
- Increase privileges

Mission Target

- Access critical data
- Upload data to external location

Maintain Presence

- Deploy backdoors
- Continued check-ins for future use

Simpler, Better Detection

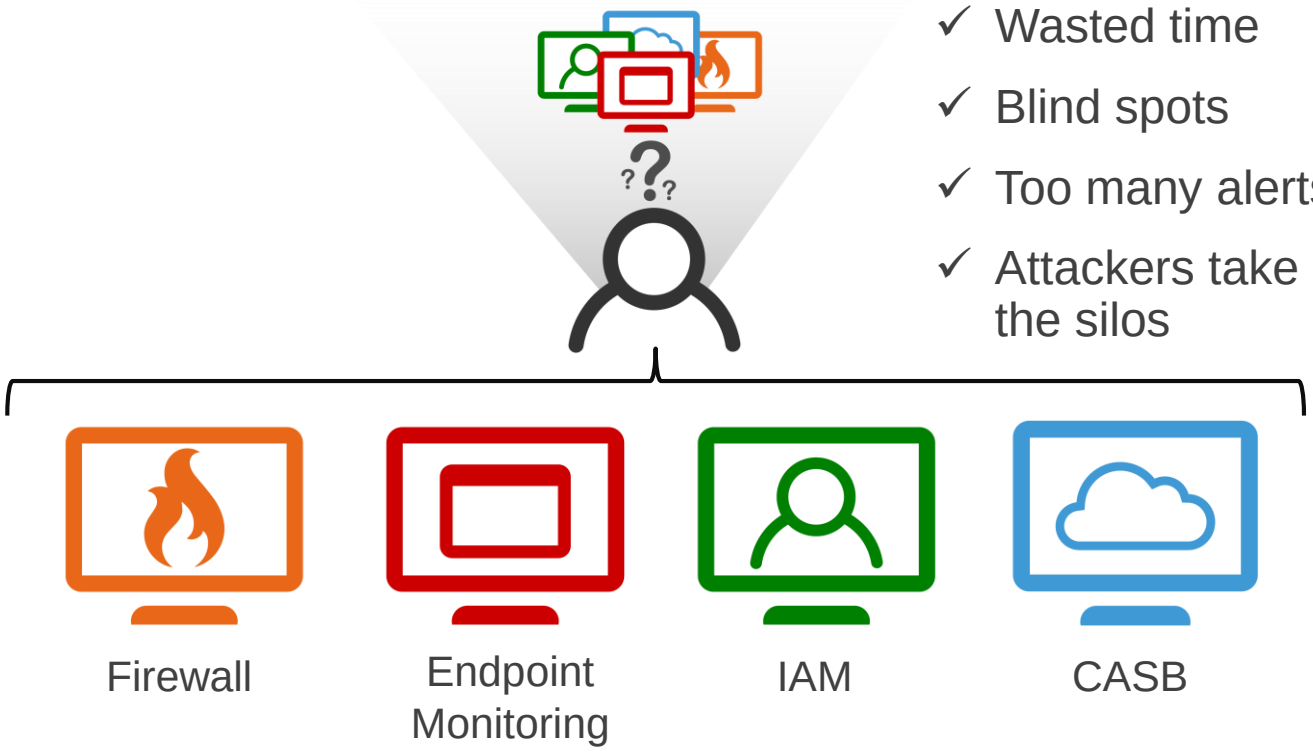
Use advanced analytics to detect attacks at every point on the attack chain

Collect the right data across the environment

Use machine learning to evolve with the environment

Use kill chain based behavioral detection

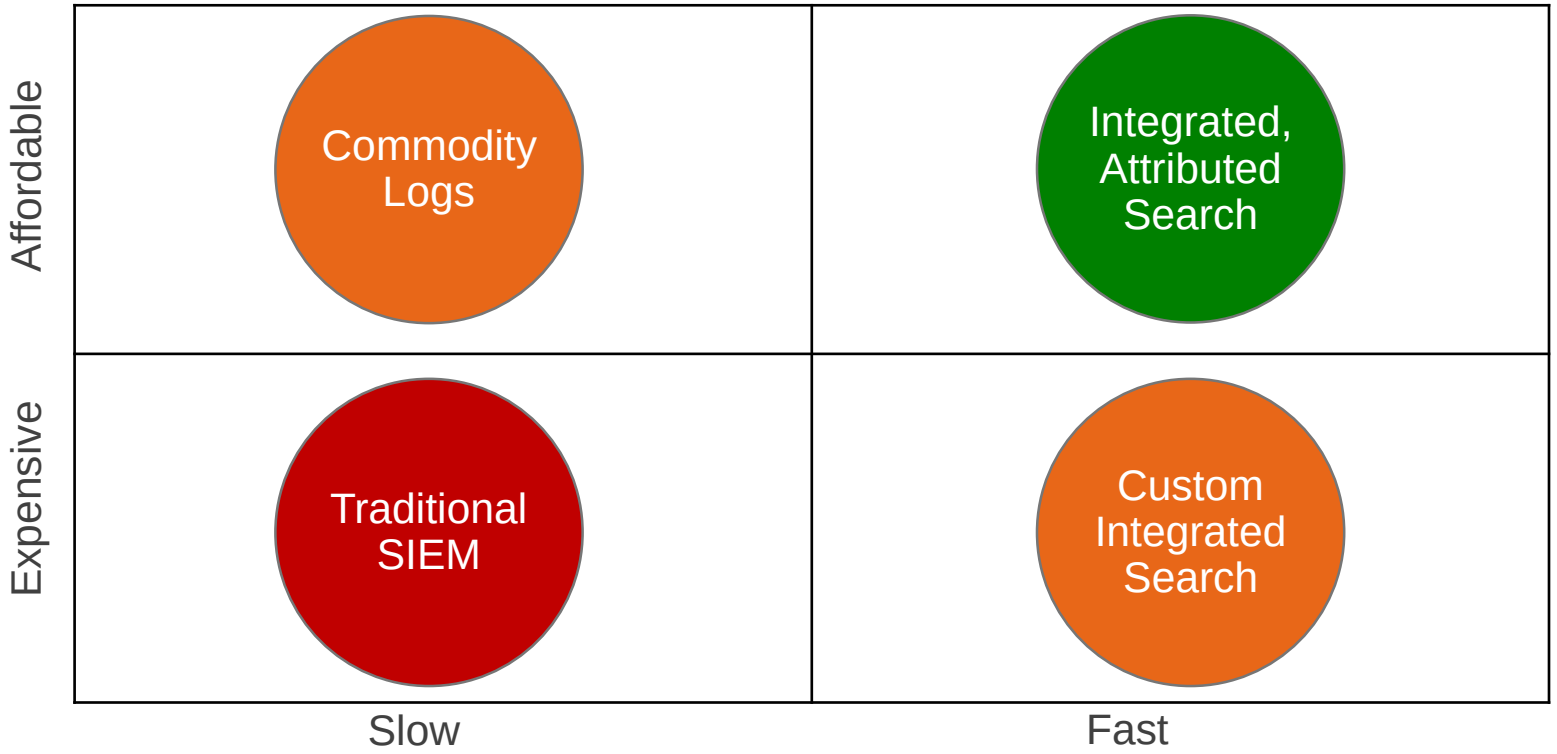
Data Silos & Fragmented Point Solutions Expose Us



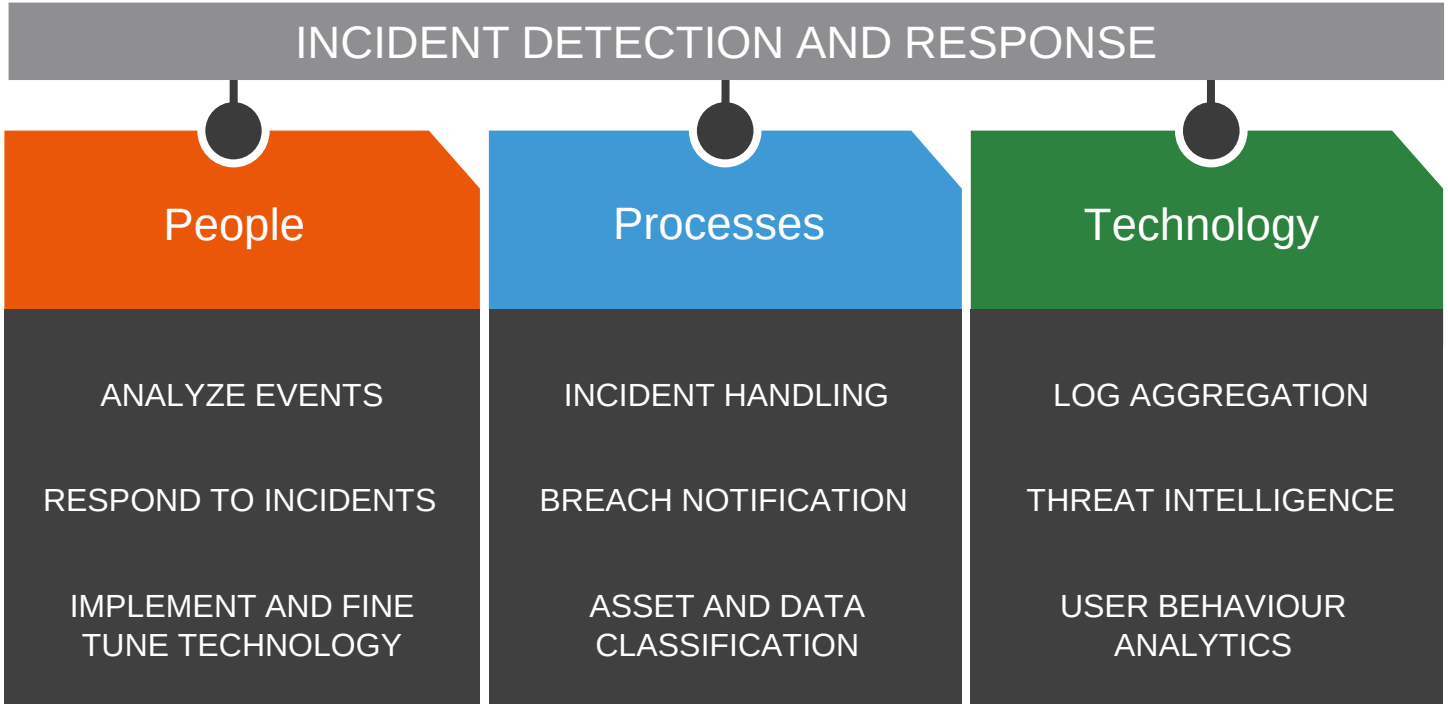
- ✓ Wasted time
- ✓ Blind spots
- ✓ Too many alerts
- ✓ Attackers take advantage of the silos

Level set / Getting the basics right first

Solving Data Fragmentation – The Productivity Killer



Fixing the Organization – People, Process & Tech



Future Challenges

- Technology overkill
- Data collection madness
- Availability of Know How

Technology Overkill

- Needs Consolidated approach
- Focus on what's needed for decisions, not technology
- Next Generation X products, Whats next?
- Rethinking needed in Security Industry

Data Collection Madness

- Differentiate between Data Collection and Data needed
- Prioritization solutions
- Costs vs benefits

Availability of Know How

- Attract students in Security Teams
- Motivational programs
- Work Appreciation in Security
- Outsourcing?

Thank You