RAPID7

Future-Ready Detection & Response

SOC, SIEM, or MDR?

ASMGi & Rapid7

03/07/2019

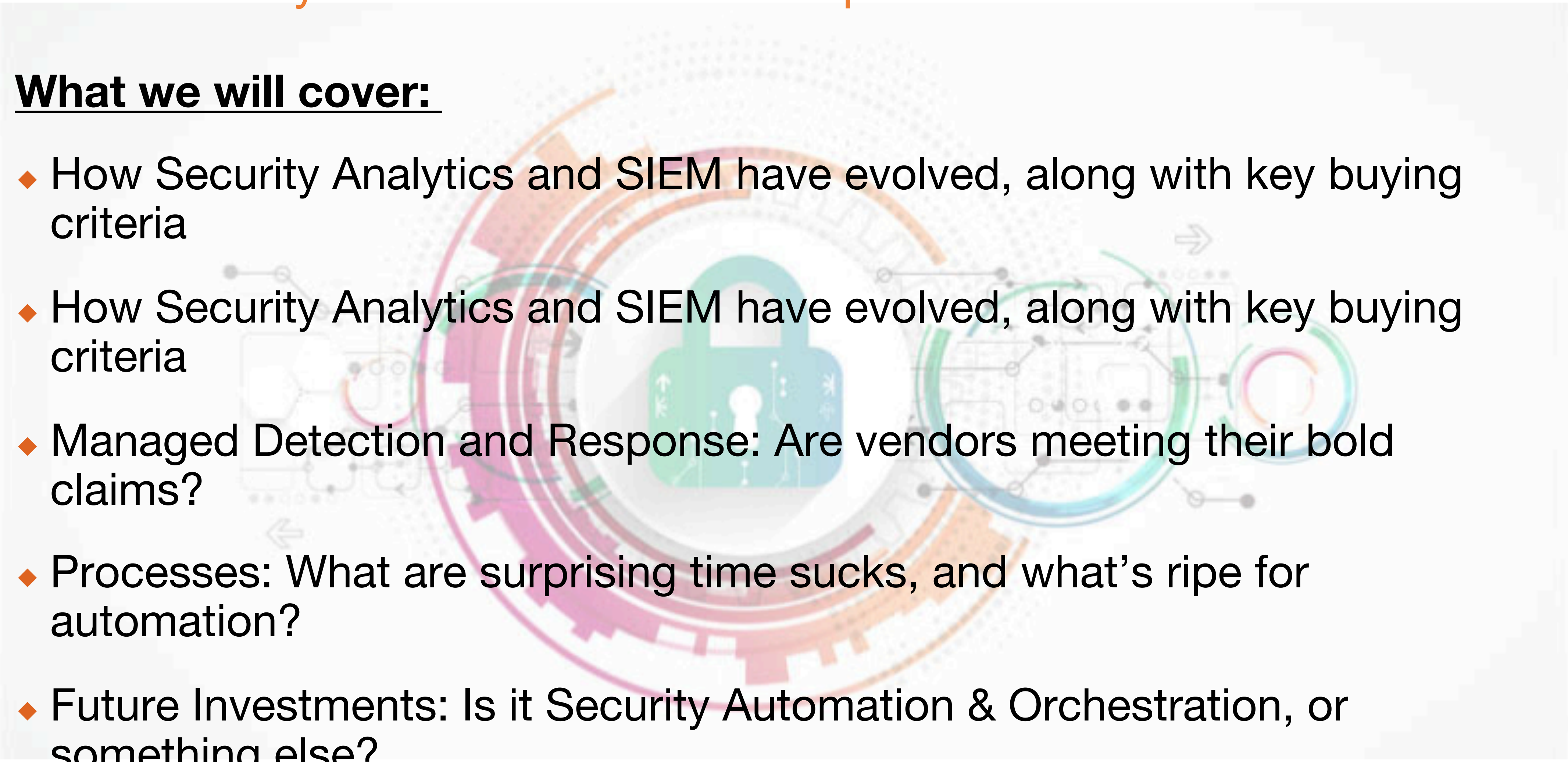
ASMGi

Future-Ready Threat Detection & Response

Presented by ASMGi and Rapid7

March 7, 2019

Today’s Webinar
Future-Ready Threat Detection & Response



What we will cover:

- How Security Analytics and SIEM have evolved, along with key buying criteria
- How Security Analytics and SIEM have evolved, along with key buying criteria
- Managed Detection and Response: Are vendors meeting their bold claims?
- Processes: What are surprising time sucks, and what’s ripe for automation?
- Future Investments: Is it Security Automation & Orchestration, or something else?

ASMGi is …

Global Technology Services and Consulting company focused on **Total Solutions** that provide immediate positive impact to your business

Total Solutions = People + Process + Technology

We deliver IT, Software and Cyber Security solutions from our headquarters in Cleveland, OH by helping our customers Plan, Manage and Execute:

- *Strong programs as a foundation to meet compliance requirements as well as foster best practices across the enterprise*
- *Best-in-Class platforms and tools to drive value thru adoption and shorter time to value*
- *A security eco-system model to ensure tools work together*
- *Achieve Results:*
  - ONEteam "XaaS" capabilities to ensure you maximize adoption – *Benefits without the Burden*!
  - "Fill the gap" approach to leverage your existing resources and complement/ supplement where needed
  - Action = Results -> Orchestrated Action = Great Results!

Managing Incident Detect and Respond solutions

1. Formal program that drives technical and process requirements and practice with table top exercises
2. Leverage a modern technology platform and services
3. Execute Incident Response per program

Future-Ready Threat Detection & Response

I am excited about today’s webinar!

- Keeping up with the threat landscape is increasingly difficult – most enterprises need help with visibility, anomaly detection, and structure response to
- Most wouldn’t argue the challenges, so how do you actually **change the game**?
- Our goal is to help you succeed – how can we best position you to confidently detect and respond to actual or suspected compromises

Agenda

1. Modern threat landscape and trends
2. What is SOC, SIEM, Security Analytics, MDR?
3. Buying decision criteria: What to prioritize?
4. Today’s state: What’s working? Where to next?
5. Audience Q&A

Speakers

Steve Roesing

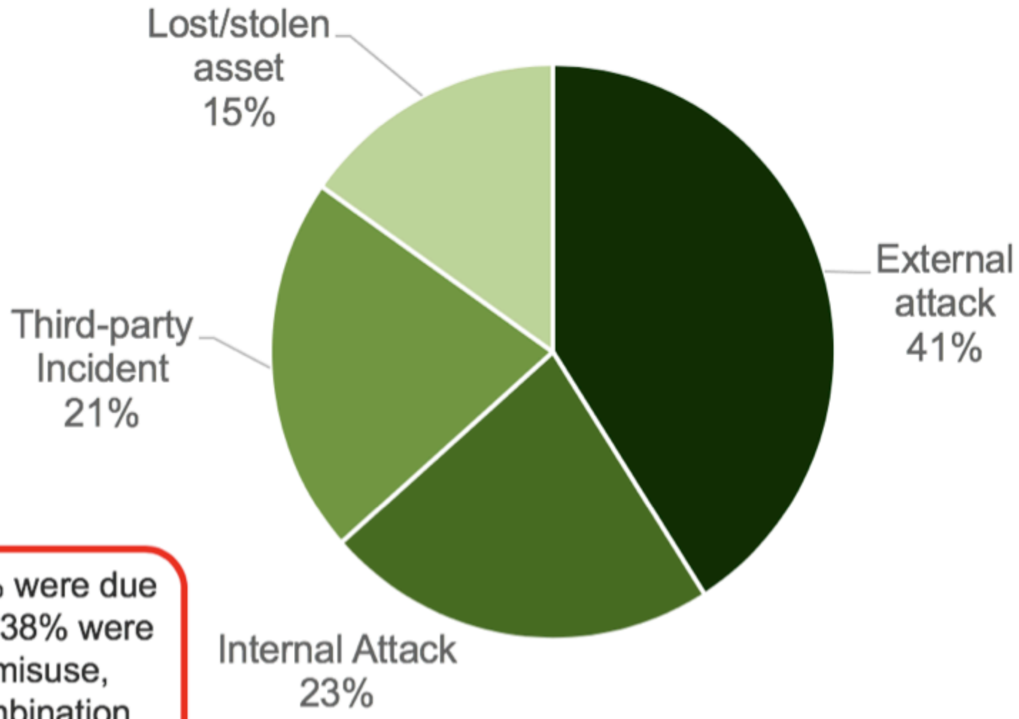
President and CEO, ASMGi

Jake Godgart

Product Marketing Manager,
Threat Detection & Response

56% of Respondent Firms Breached in 2018

Causes of confirmed breaches in the past 12 months

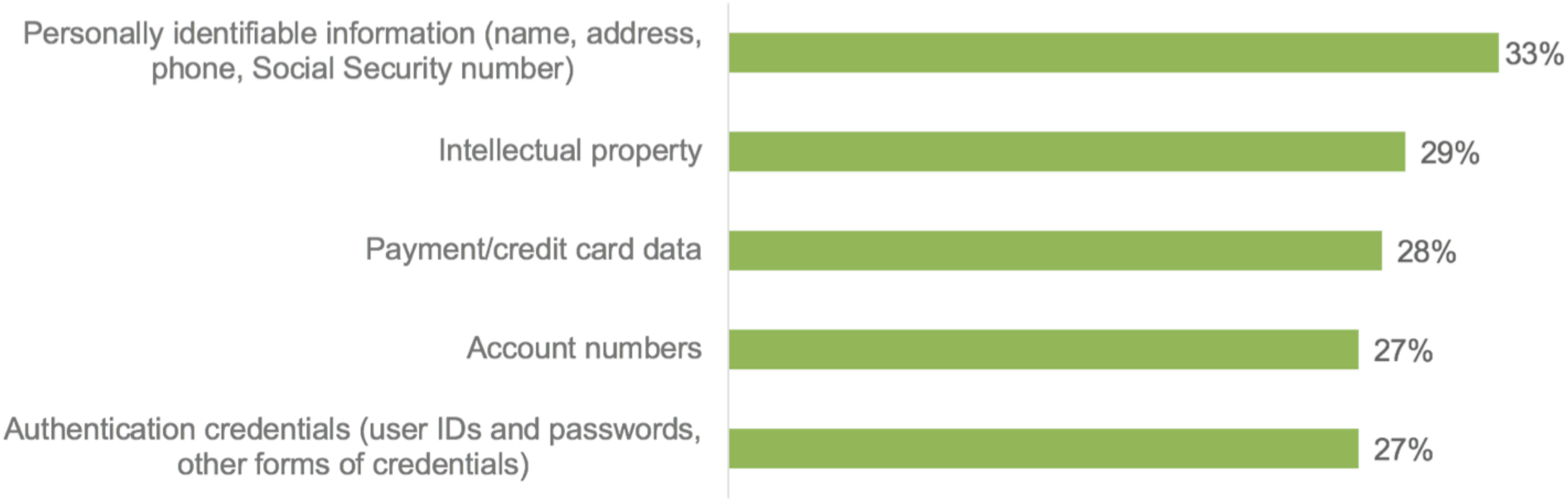


In these cases 35% were due to software exploits, 36% were due to web application attack, and 22% due to stolen credentials

In these cases 55% were due to malicious intent, 38% were due to inadvertent misuse, and 7% were a combination of both

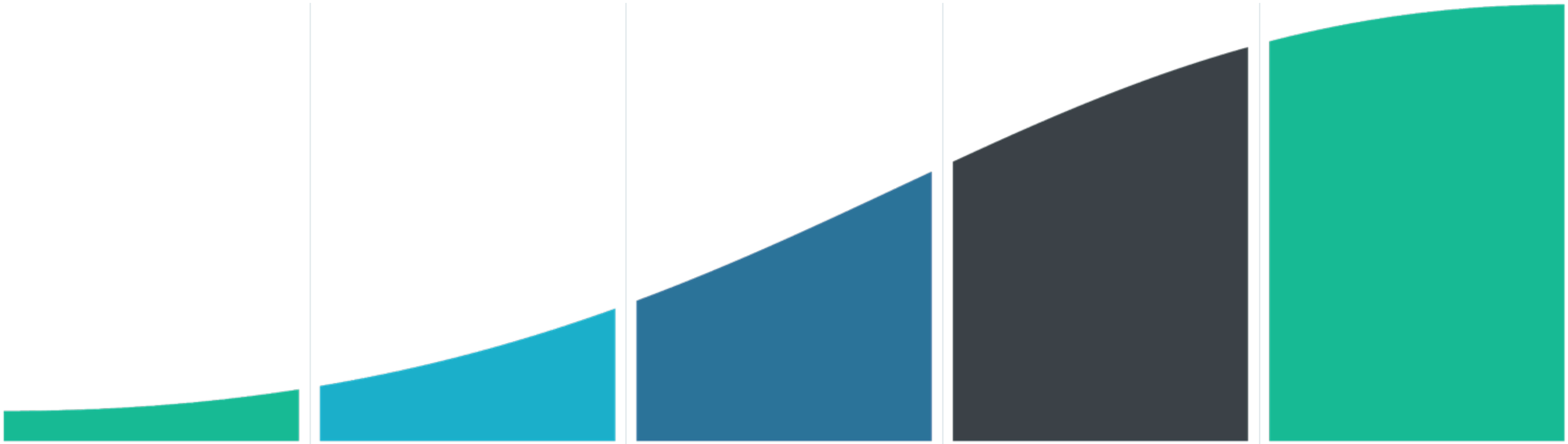
1Base: 1,147 Network Path Security decision-makers who have experienced a breach in the past 12 months
Source: Forrester's Business Technographics Global Security Survey, 2018

Most Common Data Types Breached



Base: 546 Network Path Security decision-makers who have experienced a breach in the past 12 months
Source: Forrester Data Global Business Technographics Security Survey, 2018

What does your current IDR program look like?



• No analyst specialization	• Analyst has multiple responsibilities	• Team defined roles	• Strong, diverse skills	• Complete team
• No formal process	• Incident plans	• Response plans practiced	• Response process monitored & measured	• Process optimized and leverages automation
• Only Log gathering	• Logs maintained, SysLog not analyzed	• SIEM (no tuning) causes alert fatigue	• SIEM semi-tuned	• Fully tuned with automation enabled

What does your current IDR program look like?

1. Innovation leads to a growing set of data
2. Customers see security as a brand trait
3. Threat detection requires a specialized skill set

Common Challenges		
Headcount	Threat Detection Expertise	Visibility gaps
24x7 coverage	SecOps unity	Disparate systems
Investigations	Ad-hoc process	Alert fatigue

- No analyst specialization
- No formal process
- Only log gathering

- Analyst has multiple responsibilities
- Incident plans
- Logs maintained SysLog not analyzed

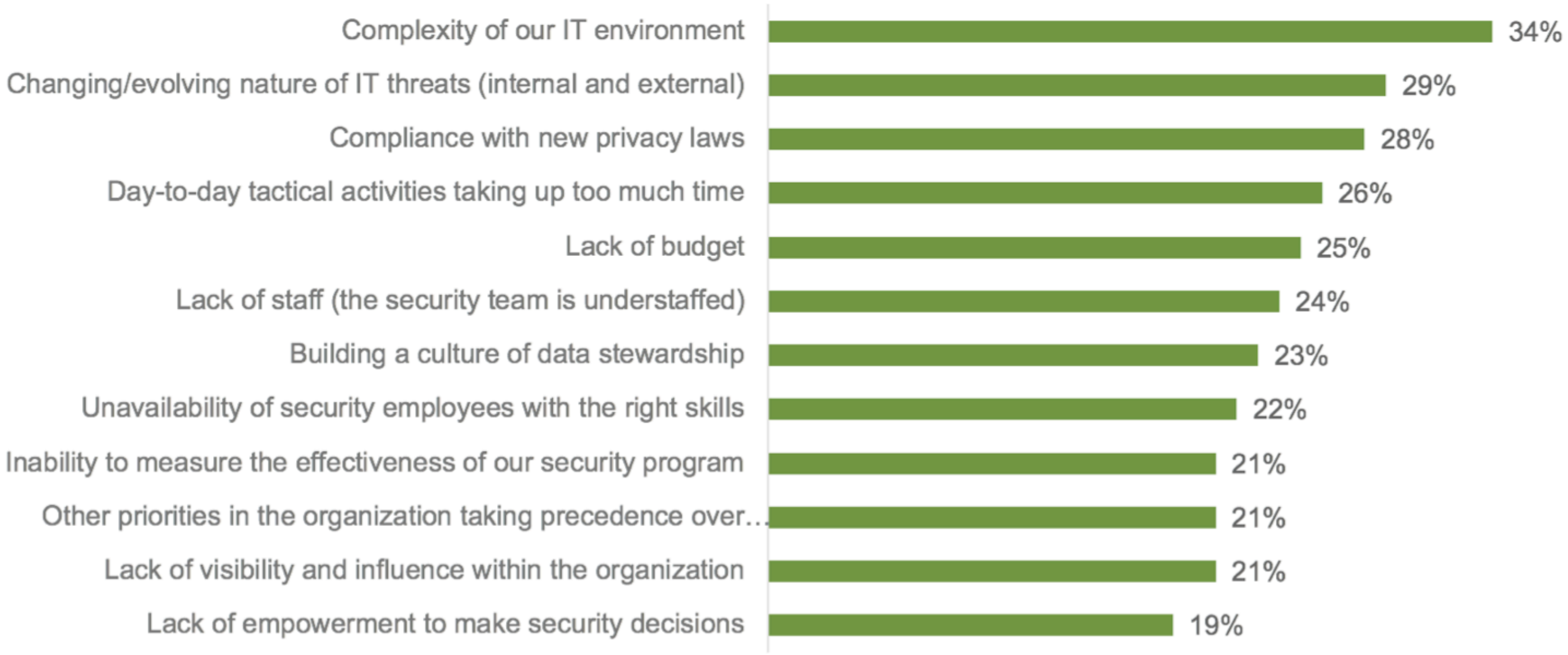
- Team defined roles
- Response plans practiced
- SIEM (no tuning) causes alert fatigue

- Strong, diverse skills
- Response process monitored & measured
- SIEM semi-tuned

- Complete team
- Process optimized and leverages automation
- Fully tuned with automation enabled

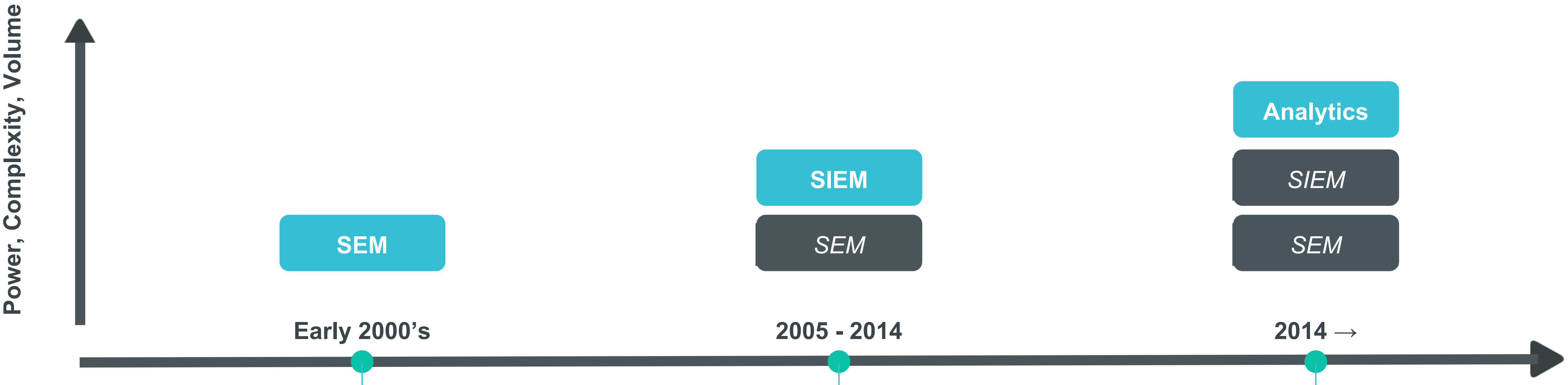
Cybersecurity is complex.

Top Security Challenges



Base: 1,502 Security decision-makers
Source: Forrester Data Global Business Technographics Security Survey, 2018

Evolution of SIEM & Security Analytics



Perimeter Defense

- Focus on network security
- Basic event correlations
- Log management & retention
- Manual breach response
- High false-positive rates, limited scale

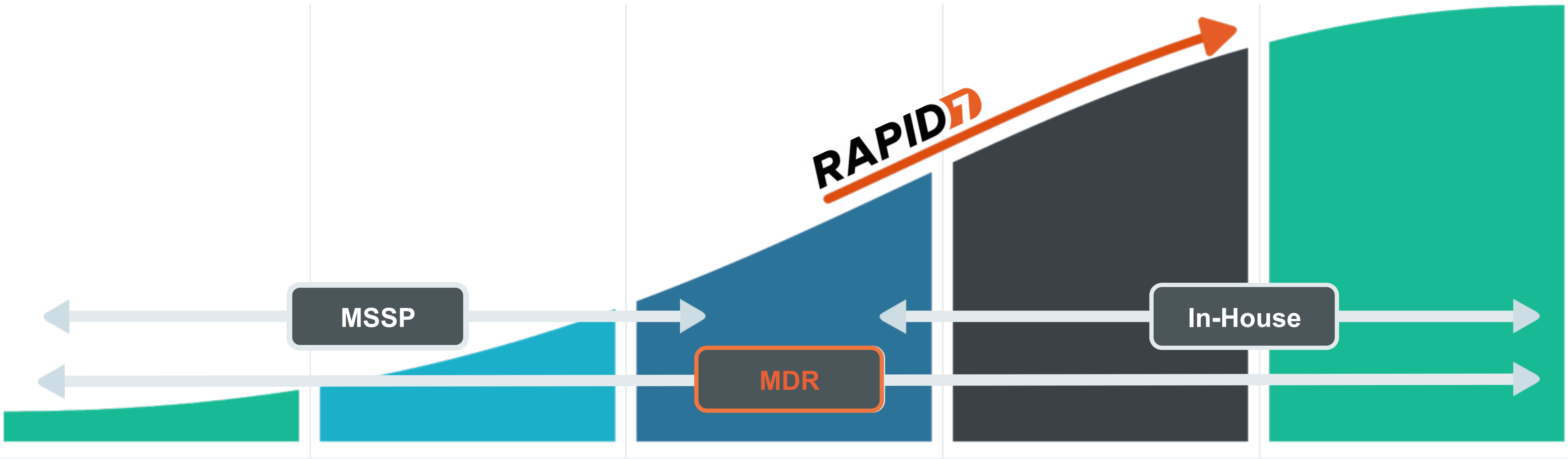
Compliance Driven

- Focus on detection, response, and reporting
- Advanced event correlations
- Multiple event sources
- Signature-based alerting
- Slow breach response
- Dependant on highly skilled analysts

Enterprise-level Intelligent Security

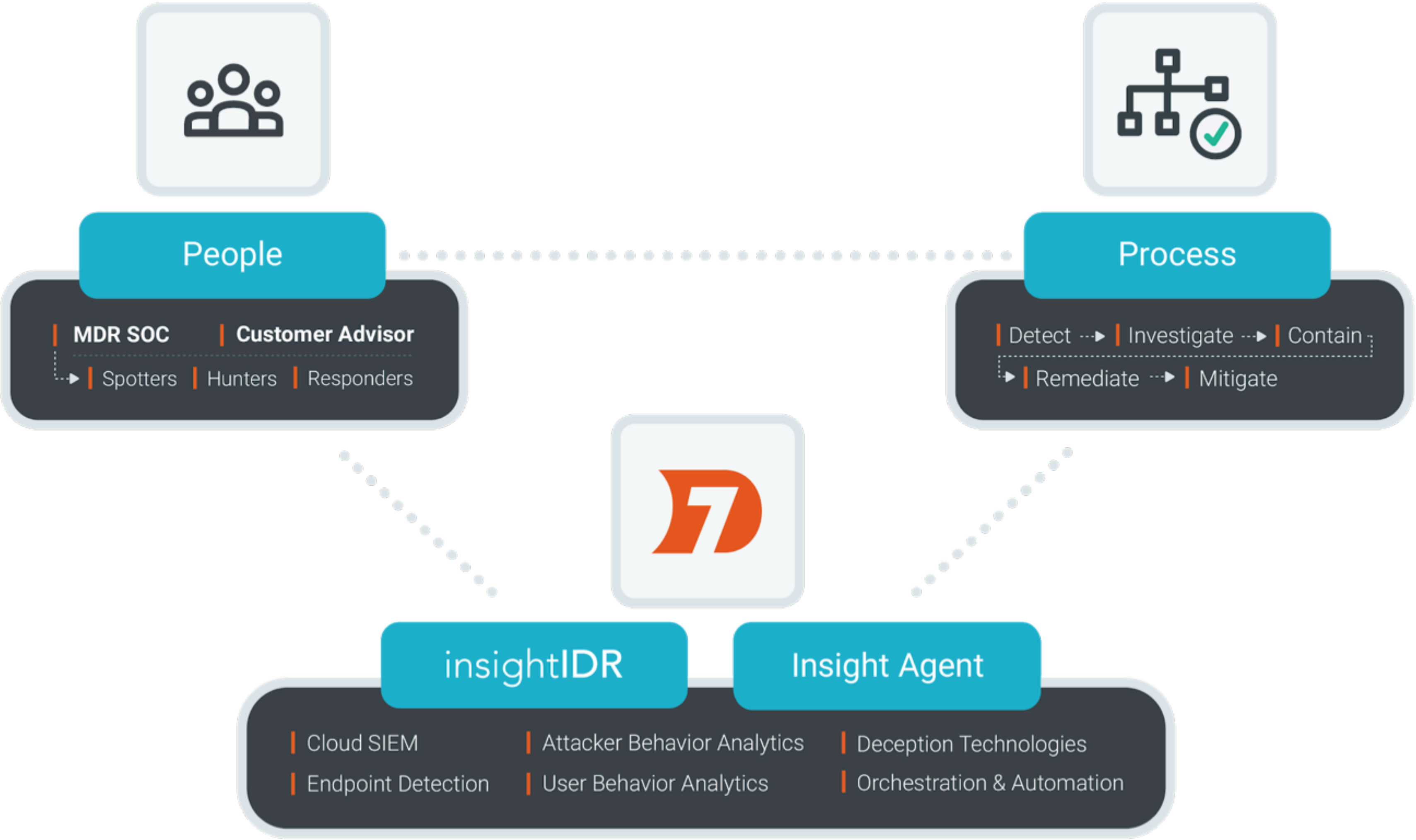
- Focus on network security
- Log ingested from apps, endpoints, and databases
- Advanced analytics with context
- Analyze User and Network behaviors
- Feeds from multiple log sources, NetFlow, reputation data, threat intel feeds
- Near real-time breach response and investigation
- Same day remediation

What does your current IDR program look like?



Advance Security through technology and expertise that simplify the complex.

Rapid7 MDR's Outcome-Driven Services Approach



People

MDR SOC | Customer Advisor

Spotters | Hunters | Responders

Process

Detect → Investigate → Contain → Remediate → Mitigate

insightIDR | Insight Agent

- Cloud SIEM
- Endpoint Detection
- Attacker Behavior Analytics
- User Behavior Analytics
- Deception Technologies
- Orchestration & Automation

ASMGi

Thank You

800 Superior Ave E, Ste 1050
Cleveland, OH 44114

Phone: 216.255.3040
Fax: 216.274.9647

Email: info@asmgi.com

www.asmgi.com