Future-Ready Detection & Response

SOC, SIEM, or MDR?

ASMGi & Rapid7

03/07/2019
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?
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
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

- Lost/stolen asset 15%
- Third-party incident 21%
- Internal attack 23%
- External attack 41%

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

- Personally identifiable information (name, address, phone, Social Security number) — 33%
- Intellectual property — 29%
- Payment/credit card data — 28%
- Account numbers — 27%
- Authentication credentials (user IDs and passwords, other forms of credentials) — 27%

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
- 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
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

<table>
<thead>
<tr>
<th>Common Challenges</th>
<th>Headcount</th>
<th>Threat Detection Expertise</th>
<th>Visibility gaps</th>
</tr>
</thead>
<tbody>
<tr>
<td>24x7 coverage</td>
<td>SecOps unity</td>
<td>Disparate systems</td>
<td></td>
</tr>
<tr>
<td>Investigations</td>
<td>Ad-hoc process</td>
<td>Alert fatigue</td>
<td></td>
</tr>
</tbody>
</table>

Cybersecurity is complex.
Top Security Challenges

- Complexity of our IT environment: 34%
- Changing/evolving nature of IT threats (internal and external): 29%
- Compliance with new privacy laws: 28%
- Day-to-day tactical activities taking up too much time: 26%
- Lack of budget: 25%
- Lack of staff (the security team is understaffed): 24%
- Building a culture of data stewardship: 23%
- Unavailability of security employees with the right skills: 22%
- Inability to measure the effectiveness of our security program: 21%
- Other priorities in the organization taking precedence over security: 21%
- Lack of visibility and influence within the organization: 21%
- Lack of empowerment to make security decisions: 19%

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

Graph: Evolution of Power, Complexity, Volume from Early 2000's to 2014 with stages of SEM, SIEM, and Analytics.
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 practiced
- Response plans monitored & measured
- Response 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

Advance Security through technology and expertise that simplify the complex.
Rapid7 MDR’s Outcome-Driven Services Approach

People
- MDR SOC
  - Spotters
  - Hunters
  - Responders
- Customer Advisor

Process
- Detect
- Investigate
- Contain
  - Remediate
- Mitigate

tools:
- insightIDR
  - Cloud SIEM
  - Endpoint Detection

- Insight Agent
  - Attacker Behavior Analytics
  - User Behavior Analytics
  - Deception Technologies
  - Orchestration & Automation
Thank You