The RSA Perspective

The attack surface is expanding

Security teams are missing attacks

Attackers are becoming more sophisticated

Teams need to increase experience & efficiency

Existing strategies & controls are failing

Tools & processes must adapt to today’s threats
Cyber-Espionage Detection

99% Percent of successful attacks that went undiscovered by logs

83% Percent of incidents that took weeks or more to discover

- VERIZON 2014 DATA BREACH INVESTIGATIONS REPORT
Cyber-Espionage Detection

85% Percent of cases where victims learned about their breach from an external party

83% Percent of incidents that took weeks or more to discover

- VERIZON 2014 DATA BREACH INVESTIGATIONS REPORT
Attackers Are Getting Stronger

Attacker Capabilities

Time To Discovery

- VERIZON 2014 DATA BREACH INVESTIGATIONS REPORT
SECURITY & RISK CHALLENGES

Detecting & Stopping Threats

Cloud

Customers

Partners

Third-Parties

On-Prem

Shadow IT

Mobile

Employees

BYOD

Managing Identities & Access

Preventing Fraud & Cybercrime

Ensuring Compliance

© Copyright 2015 EMC Corporation. All rights reserved.
Be the hunter, not the hunted
TRANSFORM

Intelligence-Driven Security
See More

Visibility

Packets, Logs, Endpoints, NetFlow

Capture Time Data Enrichment

Business & Compliance Context
understand Everything

- Correlate Multiple Data Sources
- Endpoint Threat Detection
- Out-of-the-box Content
- Big Data & Data Science

Analysis
Investigate & Remediate Faster

Prioritized & Unified Analyst Workflow

Investigate down to finest details

Integrate SOC Best Practices
Building an ASOC is a Journey

Incident Response is a **Key Force** of an organization’s security defenses & risk management
(10% of Organizations)*

Incident Response as an **Emerging** security function
(25% of Organizations)*

**Ad Hoc** Incident Response
(65% of Organizations)*

* "The Critical Incident Response Maturity Journey"
RSA White Paper – Dec 2013
### Capabilities Along Maturity Level

#### KPIs

<table>
<thead>
<tr>
<th>Initial</th>
<th>Managed</th>
<th>Defined</th>
<th>Quantitatively Managed / Optimizing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad Hoc</td>
<td>Emerging</td>
<td></td>
<td>Key Force</td>
</tr>
</tbody>
</table>

#### SecOps Capabilities Leveraged

<table>
<thead>
<tr>
<th>Incident Mgt</th>
<th>Clearing Known Alerts</th>
<th>Analyst Effectiveness</th>
<th>SOC Program Effectiveness</th>
<th>Risk Based View Of SOC Program</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>KPIs</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Alert aggregation</td>
<td>• Alert aggregation</td>
<td>• Alert aggregation</td>
<td>• Alert aggregation</td>
<td>• Alert aggregation</td>
</tr>
<tr>
<td>• Basic Workflow</td>
<td>• Business Context</td>
<td>• Business Context</td>
<td>• Business Context</td>
<td>• Business Context</td>
</tr>
<tr>
<td></td>
<td>• Multiple analyst workflow</td>
<td>• Multiple analyst workflow</td>
<td>• Multiple analyst workflow</td>
<td>• Multiple analyst workflow</td>
</tr>
<tr>
<td></td>
<td>• Prioritize based on context</td>
<td>• Prioritize based on context</td>
<td>• Prioritize based on context</td>
<td>• Prioritize based on context</td>
</tr>
<tr>
<td></td>
<td>• IR Procedures - OOTB</td>
<td>• IR Procedures - OOTB</td>
<td>• IR Procedures - OOTB</td>
<td>• IR Procedures - OOTB</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Business Context</td>
<td>• Customized IR procedures</td>
<td>• Customized IR procedures</td>
<td>• Customized IR procedures</td>
<td>• Customized IR procedures</td>
</tr>
<tr>
<td></td>
<td>• Tiered analyst workflow</td>
<td>• Tiered analyst workflow</td>
<td>• Tiered analyst workflow</td>
<td>• Tiered analyst workflow</td>
</tr>
<tr>
<td></td>
<td>• SOC Program Mgmt.</td>
<td>• SOC Program Mgmt.</td>
<td>• SOC Program Mgmt.</td>
<td>• SOC Program Mgmt.</td>
</tr>
<tr>
<td></td>
<td>• Team Management</td>
<td>• Team Management</td>
<td>• Team Management</td>
<td>• Team Management</td>
</tr>
<tr>
<td></td>
<td>• Shift management</td>
<td>• Shift management</td>
<td>• Shift management</td>
<td>• Shift management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Breach preparedness</td>
<td>• Breach preparedness</td>
<td>• Breach preparedness</td>
<td>• Breach preparedness</td>
<td>• Breach preparedness</td>
</tr>
<tr>
<td></td>
<td>• Continuous improvement</td>
<td>• Continuous improvement</td>
<td>• Continuous improvement</td>
<td>• Continuous improvement</td>
</tr>
<tr>
<td></td>
<td>• Security Control efficacy</td>
<td>• Security Control efficacy</td>
<td>• Security Control efficacy</td>
<td>• Security Control efficacy</td>
</tr>
<tr>
<td></td>
<td>• Risk based view of IR</td>
<td>• Risk based view of IR</td>
<td>• Risk based view of IR</td>
<td>• Risk based view of IR</td>
</tr>
<tr>
<td></td>
<td>• Link to overall GRC</td>
<td>• Link to overall GRC</td>
<td>• Link to overall GRC</td>
<td>• Link to overall GRC</td>
</tr>
</tbody>
</table>
RSA Security Operations Management

Domain

People

Process

Framework & Alignment

Technology

Incident Response

Breach Response

SOC Program Management

© Copyright 2014 EMC Corporation. All rights reserved.
Benefits

- Detect and analyze before attacks impact the business
- Investigate, prioritize, and remediate incidents
- Unleash the potential of your existing security team
- Evolve existing tools with better visibility & workflow