Fast, laser-focused incident response with intelligent orchestration

IBM Resilient - THE NEXT GENERATION OF INCIDENT RESPONSE

Helmut Deuter
Speciality Sales  IBM Security DACH

March 2019
Agenda

- IBM Security
- The SOAR market
- About IBM Resilient
- What is Intelligent Orchestration
- Our Platform and Demo
- Q&A
IBM Security Immune System

ON PREM | CLOUD | HYBRID

- AppScan
- Application Security on Cloud
  - SDLC Consulting
  - X-Force Red

MOBILE
- MaaS360
  - Mobile Device Management

ENDPOINT
- BigFix
  - Managed Detection & Response

APPs
- AppExchange
  - Application Security on Cloud

DATA
- QRadar
- Watson
- Resilient
- i2

IDENTITY & ACCESS
- Guardium
- Key Manager
- Multi-cloud Encryption
- Critical Data Protection Services

ADVANCED FRAUD
- Trusteer
  - Financial Malware Research

NETWORK
- QRadar Incident Forensics
- QRadar Network Insights
  - Managed Network Security
  - Secure SD-WAN

SECURITY ORCHESTRATION & ANALYTICS
- SECURITY ECOSYSTEM
  - App Exchange
    - Hybrid Cloud Security Services
  - Identity Governance
  - Access Manager
  - Cloud Identity
  - zSecure
    - Identity Management Services

THREAT INTEL
- X-Force Exchange
- X-Force IRIS

SECURITY ECOSYSTEM
- App Exchange
  - Hybrid Cloud Security Services
- Identity Governance
- Access Manager
- Cloud Identity
- zSecure
  - Identity Management Services

PRODUCTS
- X-Force Exchange
- X-Force IRIS

SERVICES
- Hybrid Cloud Security Services
- Identity Governance
- Access Manager
- Cloud Identity
- zSecure
  - Identity Management Services

IBM Security Operations Consulting
- X-Force Command Centers
  - X-Force IRIS

X-Force Managed Detection & Response
- X-Force IRIS

ON PREM | CLOUD | HYBRID

- Products
- Services
Supported by hundreds of open integrations
IBM Resilient: The Market Leader in Incident Response

Next-Generation IR Platform with Intelligent Orchestration

**Largest and most trusted IRP install base in the world**
More than 300 customers globally
Customers in more than 30 countries

**Part of the largest enterprise security organization in the world**
Resilient is the hub of IBM Security’s Immune System
Expanding customer support and services resources

**Only incident response platform with built-in intelligent orchestration**
IBM Resilient Partner Ecosystem delivered through IBM Security App Exchange
Technology-agnostic platform delivers enterprise-grade integrations with IT and security tools
Includes orchestration and automation capabilities
"This is the decade of response...sophisticated, robust, and resilient."

– Bruce Schneier
Chief Technology Officer, IBM Resilient
and Special Advisor, IBM Security
Decade Of Response: Good Security Requires All Three Areas

**Prevention**
Help to continuously stop attacks and remediate vulnerabilities

**Detection**
Identify the most important threats with advanced analytics and forensics

**Response**
Respond to incidents in integrated and organized fashion

---

**Detection and Prevention**

72% of organizations spending in Prevention technology

Detection and Response are rising but don’t have the same priority as Prevention

---

**Response**

- Orchestration and Automation of Incident Response
- Leading Analysis Firms like Gartner recommend investing in Incident Response solutions
The growth of the Security Orchestration, Automation & Response (SOAR) market

The challenges from an increasingly hostile threat landscape, combined with a lack of people, expertise and budget are driving organizations toward SOAR technologies.”

INNOVATION INSIGHT FOR SECURITY ORCHESTRATION AUTOMATION AND RESPONSE
NOVEMBER 30, 2017

Gartner
Intelligent Orchestration – Drive response. Improve security.

**Incident escalation, creation, and management**
- Incident ingestion and escalation
- Customizable incident management
- Central incident system of record

**Collaboration**
- Email collaboration
- Task allocation and accountability
- News feed and activity dashboard

**Team management**
- Metrics and KPIs
- Analytics dashboard and reporting
- Simulations
- Workspaces
- Role-based access control

---

**Case Management**
- Incident escalation, creation, and management
- Collaboration and team management
- Reporting and analytics

**Orchestration & Automation**
- Dynamic Playbooks
- Scripting, rules engine, and drag-and-drop visual workflow editor
- Ecosystem of integrations, playbooks, best practices, and developer toolkits
- Automated incident enrichment

**AI & Human Intelligence**
- AI-augmented incidence response and thread intelligence integrated and threat intelligence
- Best practices, IR expertise, and privacy rules engine
  (NIST, CERT, SANS)
Current IR Challenges

Persistent skill shortage – 77 percent of organizations have difficulty hiring and retaining IT security professionals

Constantly growing volume and severity of attacks – 65 percent of organizations say severity is increasing

Complex and growing regulatory landscape – GDPR and others

Complex SOC environment – the average SOC has 75 security tools (per Symantec)
Orchestrating and Automating Across Your SOC

Resilient creates a single hub for your SOC that allows you to outsmart, outpace, and outmaneuver threats by:

• **Guided Response** with combined human and machine intelligence, customizable dynamic playbooks, and analytics
• **Improved Visibility** - across your threat landscape
• **Better Compliance** - Aligns security and privacy professionals to avoid regulatory penalties for non-compliance
Resilient Use Case: Fusion Center

**Resilient Use Case: Fusion Center**

- **Incident Response Platform**
  - **Automatically Enriched Threat Data:** Vulnerability Management, Passive DNS
  - **Manually Invoked Remediation:** IT Help Desk, Forensics
  - **Action Module**
    - **Endpoint Security:** CARBON, BLACK, TANiUM
    - **Malware:** paloalto, FireEye
    - **Web Gateway:** BLUE COAT

**IBM Resilient**
Some vendors use the terms “automation” and “orchestration” interchangeably as synonyms, although they are not the same concept. Automation is a subset of orchestration.”

INNOVATION INSIGHT FOR SECURITY ORCHESTRATION AUTOMATION AND RESPONSE
NOVEMBER 30, 2017
Demonstration
Resilient

You have been logged out.

jessica.c@uk.ibm.com
Password

Log in to your account

Forgot your password?
© Copyright IBM Corporation 2016
Ransomware Indicators Reported

Summary
- ID: 5654
- Severity: 3
- Impact:
- Risk:
- Phase: Initial
- Date Created: 02/20/2018
- Date Occurred: 02/06/2018
- Incident Type: Ransomware

People
- Created By: Jessica Cholerton
- Owner: Jessica Cholerton
- Members: Tycho Schmidt, Andrew Yostas

Related Incidents
No related incidents.

Attachments
- 5621screeshot20180221-14_

Newsfeed
- Jessica Cholerton added attachment 5621screeshot20180221-145102.png to the incident 4 minutes ago
- Jessica Cholerton updated the task list on the incident

Description
Ransomware indicators on 3 laptops in Marketing Team. Reported by phone. Screenshot sent to SDC.

Tasks
- Data's
- Breach
- Notes & Attachments
- Members
- News Feed
- Stats & Timeline
- Artifacts

Users & Systems

Tasks
- 0% Complete

Initial
- Confirm Ransomware

Respond
- Data Breach - Organizational

- Investigate exposure of PI

Filter: All  Selected  Add Task

Task Name  Owner  Due Date  Flags  Actions
Activity Dashboard

News Feed

- **9 minutes ago**
  - Orchestration Engine added file `proofpoint_eml_sample.eml` to incident Proofpoint Alert #5612 Category: Phishing

- **9 minutes ago**
  - Jessica Cholerton updated the task list on incident Proofpoint Alert #5612 Category: Phishing

- **9 minutes ago**
  - Jessica Cholerton created the incident Proofpoint Alert #5612 Category: Phishing

- **12 minutes ago**
  - Jessica Cholerton removed the artifact `arnie jacobsen` from incident Arcsight Alert: #001113

- **2 hours ago**
  - Benoit Restagni added a row to the Data Table Task History on incident Potential unknown malware on end-point

- **2 hours ago**
  - Benoit Restagni created milestone Phase Change on incident Potential unknown malware on end-point

- **2 hours ago**
  - Benoit Restagni changed the status on task Identify the risk of harm that the data breach poses to Closed on incident Potential unknown malware on end-point

- **2 hours ago**
  - Benoit Restagni changed the phase on incident Potential unknown malware on end-point to Engage

Tasks Due Soon

You have no tasks due soon.

Need Help?

Documentation

All the information you need to get up and running.

Resource Library

Comprehensive resources for breach notification rules and security incident response best practices.
Proofpoint Alert #5612 Category: Phishing

Summary
ID 5663
Severity 3
Impact --
Risk --
Phase Engage

Date Created 02/26/2018
Date Occurred 02/21/2018

Incident Type Phishing

Description
Proofpoint Alert
Email flagged as potential phishing attack.

Artifacts

There are no members.

Related Incidents
#5652 Proofpoint Alert Frankfurt
#5632 Proofpoint Alert #3434

Attachments
SKMST_C20171116424367.doc
proofpoint_xml_sample.eml

Newsfeed
API Name: ransomware_bpmn_2
Description: Ransomware Workflow
Object Type: Incident
Updated Breach Notification Process

150 global regulations – including GDPR – in product to help customers to remain compliant with the complex breach notification requirements

Integrated breach notification with the wider Cyber Security Incident Response plan – one central place of incident management

Full simulation and table-top capabilities to train Privacy & IR teams on consistent, repeatable procedures

New GDPR breach notification regulations for all 28 EU member states
## 98.8% Reduction in Response Time

### [Customer Use Case]

<table>
<thead>
<tr>
<th>Action</th>
<th>Before Resilient IRP</th>
<th>With Resilient IRP</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Escalate via SIEM, EDR, or NGFW</td>
<td>5 min</td>
<td>10 sec</td>
<td>Escalate suspicious endpoint activity incident from QRadar</td>
</tr>
<tr>
<td>Identify affected assets – CMDB/AD/IAM</td>
<td>5-10 min</td>
<td>10 sec</td>
<td>CMDB lookup on laptop and Active Directory user lookup</td>
</tr>
<tr>
<td>Check IOCs against Threat Intelligence Feeds</td>
<td>5 min</td>
<td>10 sec</td>
<td>Incident includes hash that is tied to known Locky variant</td>
</tr>
<tr>
<td>Correlate historical incidents and data</td>
<td>10-20 min</td>
<td>instant</td>
<td>2 other incidents in the last month have the same hash and outbound traffic, pointing to a larger campaign</td>
</tr>
<tr>
<td>Manual Enrichment – Pull activity from endpoints, external networks, VPN logs, DNS records, network infrastructure, and endpoint forensics.</td>
<td>30-55 min</td>
<td>30 sec</td>
<td>Use carbon black to pull process tree from laptop, DNS from web proxy to find C2 server</td>
</tr>
<tr>
<td>Incident Tracking – Maintain detailed notes and tasks throughout the incident lifecycle</td>
<td>N/A</td>
<td>instant</td>
<td>Resilient automatically tracks tasks and actions completed as part of an incident response, all analyst notes are stored in the platform</td>
</tr>
<tr>
<td>Escalate via SIEM, EDR, or NGFW</td>
<td>N/A</td>
<td>instant</td>
<td>Everything done in Resilient is logged and cannot be modified. When subpoenaed in court, management can just print out the log</td>
</tr>
<tr>
<td>Report incident status and provide visibility to management</td>
<td>N/A</td>
<td>instant</td>
<td>Executive dashboards and external notifications give management real-time insight without any extra effort from the SOC</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>85 min</strong></td>
<td><strong>1 min</strong></td>
<td></td>
</tr>
</tbody>
</table>
THANK YOU

FOLLOW US ON:
- ibm.com/security
- securityintelligence.com
- ibm.com/security/community
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2018. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM’s current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.