Automated Response Beta Kick-Off

Antonio Sanchez | Product Marketing
Malcolm Palmer | Product Management (Threat Intel Center)
John Pirc | Product Management (Response/Asset Groups/Mobile App)
January 29, 2020
Agenda

• Response Overview

• Demo
  • Threat Intel Center
  • Asset Groups
  • Approval

• Resources
Alert Logic: A New Response Equation

Context
Define application environments and associated risks.
Focus efforts on most critical environments first
Measure progress

Automation
Automate response to routine incidents

Adaptive Security
Disrupt kill chain early
Bring work in balance with resources

Built for the Cloud
Threat Intel Center

Definition

- BETA covers Alert Logic Analytics content for incidents and observations
- View and understand incident analytic properties to be used as triggers for Automated Response:
  - Name and Summary
  - Description and Recommendation
  - Threat Level
  - Threat Classification
  - Log Sources and Log Message Types
  - IDS Signatures
  - Response Actions and Parameters

Examples

- Investigate Analytics
  - Filter
  - Search
  - Customize List

- Possible Response Actions and Parameters
  - Quarantine {victim}
  - Block {attacker}
Asset Groups

Definition
- A set of hosts, containers, or services that share common characteristics
- Membership changes dynamically over time such as:
  - Auto-scaling instances
  - Containers
  - New microservices
  - New marketing application

Examples
- Compliance
  - My PCI Environment
  - My HIPAA Environment
  - My Compliance Environment (PCI + HIPAA)
- Application
  - My e-Commerce application
  - My back-office applications
  - My SaaS applications
How Context Influences Action

- Is Joe's laptop compromised or is it the CFO's?
- Is it the T-shirt giveaway registration app or the e-commerce system?
- Is it a service that has access to PHI? Cardholder data?

Risk to the Business

Urgency of Response

Automated Action that is Appropriate
Alert Logic: A New Response Equation

Built for the Cloud

Embedded SOAR

Context
- Define application environments and associated risks.
- Focus efforts on most critical environments first
- Measure progress

Automation
- Automate response to routine incidents

Adaptive Security
- Disrupt kill chain early
- Bring work in balance with resources
Trustable Automation

Stage 1: Human Approval
- Review before automation acts

Stage 2: Automation with Guardrails
- Whitelist key assets to avoid automation gone awry

Stage 3: Automation Auditing
- Trust but verify

Audit

Rollback
Human Approval Made Easy
Contextual, Risk-based Automation

Determine where and how playbooks should act based on risk analysis

High Risk Environments
Mission Critical and/or Complex
- Human Approval
  - Review before automation acts

Low Risk Environments
Some Tolerance of Downtime and/or Simple Environments
- Full Automation
  - Periodically audit after automation acts

Configure an asset group to define the environment for playbook action

Edit an Asset Group
- Details
- Configuration

Choose assets and asset tags to include in your asset group. To learn more, click here

Select Asset Filters (5 Selected) • Search

Name
- 99002334368
  - ca-central-1
  - vpc-dc1155db4
- subnet-48b4132
- subnet-9fa4fe8c
- subnet-ce552ba6
- ap-northeast-2
  - vpc-596be64
- eu-north-1
- us-west-2
- us-east-2
- eu-west-3
Demo
About the Beta Environment

Platform

Playbook

Approval

Outcomes

Block Attacker

Disable User Account
Threat Intel Center
Threat Intel Center (Getting Started)
## Threat Intel Center Landing Page

### Analytics

<table>
<thead>
<tr>
<th>Name</th>
<th>Summary</th>
<th>Threat Level</th>
<th>Telemetry</th>
</tr>
</thead>
<tbody>
<tr>
<td>accessanomaly</td>
<td>Access to Anomalous Resource from 9%distinct%</td>
<td>Medium</td>
<td>None</td>
</tr>
<tr>
<td>accessunauth</td>
<td>Access to Unauthorized Resource from 9%distinct%</td>
<td>Medium</td>
<td>None</td>
</tr>
<tr>
<td>app/cve20000800</td>
<td>CVE-2000-0800 Linux rpc.kostad String Parsing Error RCE attack from 1.2.3.4</td>
<td>High</td>
<td>IDS</td>
</tr>
<tr>
<td>app/cve20176553</td>
<td>CVE-2017-6553 Quest Privilege Manager buffer overflow attempt from 1.2.3.4</td>
<td>High</td>
<td>IDS</td>
</tr>
<tr>
<td>app/educatedscholar</td>
<td>EDUCATEDSCHOLAR SMB attack attempt from 1.2.3.4</td>
<td>High</td>
<td>IDS</td>
</tr>
<tr>
<td>app/esteemaudit</td>
<td>ESTEEMAUDIT 2 Stage information Disclosure from 1.2.3.4</td>
<td>High</td>
<td>IDS</td>
</tr>
<tr>
<td>app/eternalblue</td>
<td></td>
<td>High</td>
<td>Log</td>
</tr>
</tbody>
</table>
### Customize Table

**Analytics**

- **Choose Columns (4 of 15 Shown)**
  - Name
  - Recommendations
  - Response Actions

#### Summary
- Access to Anomalous Resource from Vendors
  - Threat Level: Medium
  - Telemetry: None
- Access to Unauthorized Resource from Vendors
  - Threat Level: Medium
  - Telemetry: None
- [VENDOR] User [SOURCE_USERNAME] Attempting to Access Admin Application
  - Threat Level: Medium
  - Telemetry: Logmsgs
  - Threat Level: Medium
  - Telemetry: Logmsgs

#### AdminPrivilegeGrant
- **app/cve20000800**
  - CVE-2000-0800 Linux rpc.mountd String Parsing Error RCE attack from 1.2.3.4
  - Threat Level: High
  - Telemetry: IDS
- **app/cve20176553**
  - CVE-2017-6553 Quest Privilege Manager buffer overflow attempt from 1.2.3.4
  - Threat Level: High
  - Telemetry: IDS
- **app/educedscholar**
  - EDUCEDSCHOLAR SMB attack attempt from 1.2.3.4
  - Threat Level: High
  - Telemetry: IDS
- **app/esteemaudit**
  - ESTEEMAUDIT 2 Stage Information Disclosure from 1.2.3.4
  - Threat Level: High
  - Telemetry: IDS
- **app/eternalblue**
  - ETERNALBLUE Sniffnet.sys RCE possible success from 1.2.3.4
  - Threat Level: High
  - Telemetry: IDS
- **app/eternalblue_success**
  - ETERNALBLUE Sniffnet.sys RCE possible success from 1.2.3.4
  - Threat Level: High
  - Telemetry: IDS
## Filter Analytics List

### Analytics

<table>
<thead>
<tr>
<th>Name</th>
<th>Summary</th>
<th>Threat Level</th>
<th>Telemetry</th>
</tr>
</thead>
<tbody>
<tr>
<td>successful_sqli/sqli_success</td>
<td>Successful SQL injection from 1.2.3.4</td>
<td>Critical</td>
<td>IDS</td>
</tr>
<tr>
<td>successful_sqli/sqli_error</td>
<td>Possible Successful SQL injection from 1.2.3.4</td>
<td>Critical</td>
<td>Log</td>
</tr>
<tr>
<td>successful_sqli/roamer_php_webshell_success</td>
<td>Successful Roamer PHP Web Shell Access By 1.2.3.4</td>
<td>Critical</td>
<td>IDS</td>
</tr>
<tr>
<td>successful_sqli/cve20157857</td>
<td>Possible Successful CVE-2015-7857 SQL injection attempt from 1.2.3.4</td>
<td>Critical</td>
<td>IDS</td>
</tr>
<tr>
<td>successful_sqli/apache.struts_scan_success</td>
<td>Successful Apache Struts CVE-2013-2251 scan from 1.2.3.4</td>
<td>Critical</td>
<td>IDS</td>
</tr>
<tr>
<td>bf_success/xmrtpcs</td>
<td>Successful Unix BruteForce Login detected from 1.2.3.4</td>
<td>Critical</td>
<td>Log</td>
</tr>
<tr>
<td>bf_success/unix</td>
<td>Successful Unix BruteForce Login detected from 1.2.3.4</td>
<td>Critical</td>
<td>Log</td>
</tr>
<tr>
<td>bf_success/tomcat</td>
<td>Possible Successful Tomcat Login from 1.2.3.4</td>
<td>Critical</td>
<td>IDS</td>
</tr>
<tr>
<td>bf_success/remote_root_login_ssh</td>
<td>Successful Remote SSH Root Login from 1.2.3.4</td>
<td>Critical</td>
<td>Log</td>
</tr>
</tbody>
</table>
## Search Analytics List

### Analytics

**Search Filters:**
- Threat Level: Critical
- Telemetry: Log
- Response Actions: Quarantine
- Threat Classification: None

**Table:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Summary</th>
<th>Threat Level</th>
<th>Telemetry</th>
<th>Logs</th>
<th>Signatures</th>
</tr>
</thead>
<tbody>
<tr>
<td>postcomp/resbv9545</td>
<td>Potential lateral movement using PowerShell and WMI detected on 1.2.3.4</td>
<td>Critical</td>
<td>Log</td>
<td>Windows Process Created</td>
<td>None</td>
</tr>
<tr>
<td>postcomp/powershell_svc_create</td>
<td>Suspicious service created with PowerShell on 1.2.3.4</td>
<td>Critical</td>
<td>Log</td>
<td>Windows PowerShell Provider Started, Windows Service Installed</td>
<td>None</td>
</tr>
<tr>
<td>postcomp/powershell_nishang</td>
<td>PowerShell Nishang Usage Detected on 1.2.3.4</td>
<td>Critical</td>
<td>Log</td>
<td>Windows PowerShell Operational Log, Windows Sysmon File Created, Windows Sysmon Process Created, Windows</td>
<td>None</td>
</tr>
<tr>
<td>postcomp/powershell_empire</td>
<td>PowerShell Empire Usage Detected on 1.2.3.4</td>
<td>Critical</td>
<td>Log</td>
<td>Windows PowerShell Operational Log</td>
<td>None</td>
</tr>
<tr>
<td>postcomp/monero_miner_dropper, carbon_downloaded</td>
<td>PowerShell script to execute Monero (XMR) miner XMRig downloaded on 1.2.3.4</td>
<td>Critical</td>
<td>IDS</td>
<td>Not Applicable</td>
<td>1102125</td>
</tr>
</tbody>
</table>

**Summary:**
- **Postcomp/monero_miner_dropper, carbon_downloaded**
  - Powerful script to retrieve Carbon dropper for Monero (XMR) miner XMRig downloaded on 1.2.3.4
  - Threat Level: Critical
  - Telemetry: Log
  - Response Actions: None
  - Threat Classification: None
  - Log Source: None
  - Log Not Applicable
  - Signatures: 1102125
Open Analytic Details

Metasploit PowerShell backdoor installation detected on '[ip_address]'
Asset Groups
Asset Groups (Getting Started)
Asset Groups Landing Page

Add an Asset Group

You can organize your assets in groups and then configure automated notifications or ticketing system connections for them and more. To add an asset group, you can select assets and tags or link multiple asset groups together.

Asset Groups

<table>
<thead>
<tr>
<th>Asset Group</th>
<th>Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robs Things</td>
<td>478</td>
</tr>
<tr>
<td>Last Updated: 20 Jan 2021</td>
<td></td>
</tr>
<tr>
<td>Matts Hosts</td>
<td>2</td>
</tr>
<tr>
<td>Last Updated: 29 Dec 2020</td>
<td></td>
</tr>
<tr>
<td>Asset Group Demo</td>
<td>1566</td>
</tr>
<tr>
<td>Last Updated: 20 Jan 2021</td>
<td></td>
</tr>
</tbody>
</table>
Adding an Asset Group

Asset Groups

<table>
<thead>
<tr>
<th>Asset Group</th>
<th>Assets</th>
<th>View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robs Things</td>
<td>478</td>
<td></td>
</tr>
<tr>
<td>Last Updated: 20 Jan 2021</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mats Hosts</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Last Updated: 29 Dec 2020</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Group Demo</td>
<td>1566</td>
<td></td>
</tr>
<tr>
<td>Last Updated: 20 Jan 2021</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Adding an Asset Group (Step 1)

1. **Details**
   - **Name**
     - PCI
   - **Description**
     - Assets in Scope

2. **Configuration**
   - **Criticality Rating**
     - 3

Provide details about your new asset group.

Rate the importance of protecting this group. (Ex. If your scale is Info, Low, Medium, and High, select 0-3 to weight the Threat Risk Index score according to your scale.)
# Adding an Asset Group (Step 2)

Add an Asset Group

## Details

- **Assets**
- **Tags**

Choose assets and asset tags to include in your asset group. To learn more, [click here](#).

### Select Asset Filters (5 Selected)

<table>
<thead>
<tr>
<th>Name</th>
<th>Location</th>
<th>Cloud</th>
<th>Available</th>
<th>Assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>990023346368</td>
<td>16</td>
<td>18</td>
<td>55</td>
<td>0</td>
</tr>
<tr>
<td>674305394241</td>
<td>16</td>
<td>11</td>
<td>33</td>
<td>0</td>
</tr>
<tr>
<td>Alert Logic Collector Support Deployment</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>WLA Integration Log Source</td>
<td>16</td>
<td>21</td>
<td>57</td>
<td>3</td>
</tr>
<tr>
<td>055103733742</td>
<td>16</td>
<td>7</td>
<td>20</td>
<td>1</td>
</tr>
<tr>
<td>582159568573</td>
<td>16</td>
<td>7</td>
<td>22</td>
<td>0</td>
</tr>
<tr>
<td>707124421633</td>
<td>16</td>
<td>12</td>
<td>38</td>
<td>0</td>
</tr>
</tbody>
</table>

Select an asset in the list

Properties appear here for including in your asset group. You can exclude specific assets within the selection. Review or edit the expression in the Expression tab.
# Adding an Asset Group (Step 3)

## Add an Asset Group

1. Details
2. Configuration

Choose assets and asset tags to include in your asset group. To learn more, click here

### Assets

<table>
<thead>
<tr>
<th>Name</th>
<th>Location</th>
<th>Properties</th>
<th>Group</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLA Integration Log Source</td>
<td></td>
<td>16</td>
<td>21</td>
<td>57</td>
</tr>
<tr>
<td>eu-central-1</td>
<td></td>
<td>1</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>us-west-1</td>
<td></td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>us-east-1</td>
<td></td>
<td>2</td>
<td>7</td>
<td>2</td>
</tr>
<tr>
<td>cas-dev-wla-us-east-1-int</td>
<td></td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>vpc-be8c16d9</td>
<td></td>
<td>6</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>subnet-86a2118a</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>subnet-0f1df346</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Select asset in the list
Properties appear here for including in your asset group. You can exclude specific assets within the selection. Review or edit the expression in the Expression tab.
Adding an Asset Group Inclusions (Step 4)

1. Select "Fargate Demo" under the "Assets" tab.
2. Click the "ADD" button to add the selected asset group.
Adding an Asset Group Exclusions (Step 5)

Add an Asset Group

Choose assets and asset tags to include in your asset group. To learn more, click here

Assets

Select Asset Filters (5 Selected)

Name

89EA-4403-83D0-0946F6361441/us-west-2b/vpc-0c3debc62fd69779a

subnet-02463a9647a3cea01

ssehic-wsm-test

AlertLogic IDS Security Subnet 134253202/450937F6-89EA-4403-83D0-0946F6361441/us-west-2a/vpc-0c3debc62fd69779a

AlertLogic Security Subnet

Architecture

x86_64

Availability Zone

us-west-2a

Instance ID

i-07f6082e466fa3b87

Instance Name

ssehic-wsm-test

CANCEL  ADD
Adding an Asset Group (Step 6)

Choose assets and asset tags to include in your asset group. To learn more, click here

Assets

Tags

Search

Select a tag in the list
Properties appear here for including in your asset group. You can exclude specific tags within the selection. Review or edit the expression in the Expression tab.

- user
  - arn:aws:iam::248216933490:user/wsm-jenkins
- user
  - arn:aws:iam::248216933490:user/mzimmerman
- Name
  - Public subnet
- aws:cloudformation:logical-id
  - TestNode2
- Name
  - AlertLogic Security Group 134230027/B34144EE-8128-4585-AE58-E897BF941EAC/vpc-0ba675b4661da54ae
- Name
  - AlertLogic IDS Security Route Table 134230027/A9F85FFB-F31B-4B9F-B1F0-0F385E9F343D/us-west-2a/voc-
Working with Asset Group Expressions

Edit an Asset Group

1. Details
2. Configuration

Choose assets and asset tags to include in your asset group. To learn more, click here

Assets, Tags

Expression Editor

```
1 {
2   "scopes": [
3     {
4       "include": ["host://aws/us-east-1/host/1-0c8c2c7299a7639f"
5     ]
6   }
7 
8 }
9 }
```

Editor Tips

As you include or exclude assets and tags, Alert Logic creates an expression. You can create the expression manually instead or edit it. To get started, review the supported JSON fields:

scopes
includes
excludes
asset_types

View the schema and learn more
## Creating Linked Asset Groups

### Add an Asset Group

You can add your assets to groups and then configure automated notifications or ticketing system connections for them and more. To add an asset group, you can select assets and tags or link them.

### Asset Groups

<table>
<thead>
<tr>
<th>Asset Group</th>
<th>Number of Assets</th>
<th>View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robs Things</td>
<td>478</td>
<td>View</td>
</tr>
<tr>
<td>Matts Hosts</td>
<td>2</td>
<td>View</td>
</tr>
<tr>
<td>Asset Group Demo</td>
<td>1566</td>
<td>View</td>
</tr>
<tr>
<td>PCI</td>
<td>2</td>
<td>View</td>
</tr>
</tbody>
</table>
Creating Linked Asset Groups (cont)

Add a Linked Asset Group

1 Details  2 Configuration

Provide details about your new asset group

1 Name *
   Compliance

2 Description *
   Critical Assets in Scope

3 Criticality Rating
   3

Rate the importance of protecting this group. (Ex. If your scale is Info, Low, Medium, and High, select 0-3 to weight the Threat Risk Index score according to your scale.)
Creating Linked Asset Groups (cont)

Add a Linked Asset Group

You can create an asset group that includes other asset groups.

Matching Rule
- All Assets in Selected Groups
  Includes every asset that exists in any of the selected asset groups.
- Overlapping Assets Only
  Includes only assets that exist in all of the selected asset groups.

1. Details
   - PCI, Matts Hosts
     - [ ] Matts Hosts
     - [ ] PCI
   - [ ] Robs Things

2. Configuration
   - [ ] Asset Group Demo
Creating Linked Asset Groups (cont)

<table>
<thead>
<tr>
<th>Asset Groups</th>
<th>Amount</th>
<th>View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robs Things</td>
<td>478</td>
<td></td>
</tr>
<tr>
<td>Last Updated: 20 Jan 2021</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Matts Hosts</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Last Updated: 29 Dec 2020</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Group Demo</td>
<td>1566</td>
<td></td>
</tr>
<tr>
<td>Last Updated: 20 Jan 2021</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCI</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Last Updated: 26 Jan 2021</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Linked Asset Groups</th>
<th>Amount</th>
<th>View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Last Updated: 26 Jan 2021</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Asset Groups and Exposures

- **Determine if privileged access is needed.**
  - 114 Affected Assets | 114 Exposure Instances
  - TRI 400.35

- **Review the IAM Access Analyzer findings for this account.**
  - 94 Affected Assets | 94 Exposure Instances
  - TRI 343.57

- **Restrict access to/from non-required IP addresses**
  - 40 Affected Assets | 49 Exposure Instances
  - TRI 332.58

- **Upgrade OpenBSD OpenSSH to version 8.3.0**
  - 29 Affected Assets | 205 Exposure Instances
  - TRI 318.99

- **Upgrade Apache Http_server to version 2.4.44**
  - 7 Affected Assets | 188 Exposure Instances
  - TRI 281.03

- **Enable log metric filters and alarms.**
  - 0 Affected Assets | 84 Exposure Instances
  - TRI 211.30

- **Apply non-default NACLs to all VPC subnets**
  - 15 Affected Assets | 15 Exposure Instances
  - TRI 120.00

Select a deployment to view additional asset filters.
Asset Groups and Exposures

Select a deployment to view additional asset filters.
Asset Groups and Health

Select a deployment to view additional asset filters.
Asset Groups and Health

1. **Deployment**
   - Ozone

2. **Asset Group**
   - JP Test
   - Info Dev Test

3. **Asset Groups**
   - AN_VPC
     - Ozone | 10.0.0.0/16
   - Legacy
     - Ozone | 10.0.0.0/16
   - Test VPC
     - Ozone | 10.0.0.0/16
   - TST_VPC
     - Ozone | 10.0.0.0/16
   - vpc-7718f91e
     - Ozone | 172.31.0.0/16
Getting Started from the Dashboard (Playbook)
Defining the Playbook

Click here to get started
Defining the Playbook (cont)

Add a Playbook

1. **Details**
   - **Input**, **Variables**, **Result**
   - Provide information about your playbook and the criteria for carrying it out

2. **Name**: Beta Day (Informational Playbook)

3. **Description**: Demo

Playbook is Active?
Defining the Playbook (cont)

1. Input Parameters

This list contains the input parameters for this playbook. You can also add your custom parameters that you want to make available for tasks in this playbook.

- account_id
  Alert Logic MDR Account ID
- payload_type
  Alert Logic MDR Payload Type
- payload
  Alert Logic MDR Payload Object

2. Variables

Result
Defining the Playbook (cont)

Add a Playbook

This list contains the variables available for use in this playbook and their descriptions.
Defining the Playbook (cont)

You can define variables to include in the overall result of your playbook. For each variable, enter its name and a default value or an expression in Yet Another Query Language (YAQL) format that a playbook action sets. The result appears in the Output section of the playbook history.

Variable | Value
Defining the Playbook (cont)

Creating a Task
We currently have 26 tasks and we are going to select Email Approval Request.
Defining the Playbook (cont)

Task Details:

Name
send_approval_email0

Action
send_approval_email

Description
Request an approval via an email

☐ Repeat this action
Defining the Playbook (cont)

Creating a Condition
Defining the Playbook (cont)
Defining the Playbook (cont)

TBA
Defining the Playbook (cont)
Defining the Playbook (cont)
### Defining the Playbook (cont)

#### Conditions

1. **Name:** Approved
2. **Condition:** `<% succeeded() %>`
3. **Do:**

List of items to publish:

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
</table>
Defining the Playbook (cont)
Defining the Playbook (cont)
Defining the Playbook (cont)

Task Details:

Name
incident_complete2

Action
incident_complete

Description
Close incident and provide reason for closing an incident.

☐ Repeat this action
Defining the Playbook (cont)
Validating a Playbook

Beta Day (Informational Playbook)

Playbook Context

Alert Logic: send_approval_email0

Condition: Approved

Condition: Rejected

Alert Logic: incident_complete2

Alert Logic: incident_add_feedback1

Playbook valid!!!
Testing a Playbook

incident_payload:

```json
{
  "accountId": 2,
  "asset_deployment_type": "aws",
  "asset_host_name": "10.1.2.3",
  "asset_native_account_id": 2,
  "assets": [],
  "attacker": {
    "account": 2,
    "instanceId": "i-0a159b2a553285e0a",
    "ip": "10.10.10.12",
    "port": 40014,
    "region": "us-east-2"
  },
  "attacker_country_code": "BR",
  "attacker_country_name": "Brazil",
  "attacker_set": [
    {
      "ip": "86.34.222.99"
    },
    {
      "value": "SomeAttacker"
    }
  ],
  "closed_time": "2020-08-18T11:24:27.765796+00:00"
}
```
Setting a Playbook in Motion

Create a Notification

Alert Notifications

Lists your notifications for incidents and correlation observations that alert you to potential threats in near real time.

Incidents

Darwin Test for info level notifications
Most recent notification sent: Jan 26 2021 17:00:46 GMT-6
2 Recipients
View

High Incident Alert
Most recent notification sent: Jan 26 2021 11:54:37 GMT-6
2 Recipients
View

Info Dev Test Incident Notification
Most recent notification sent: No notifications sent.
1 Recipients
View

Nancy's High Incident Alert
Most recent notification sent: No notifications sent.
1 Recipients
View
Setting a Playbook in Motion (cont)

Select Incident
Setting a Playbook in Motion (cont)

1. Create an Incident Notification

Alert Logic sends you notifications when new or escalated incidents meet the criteria you set.

Details

- **Name**: 
- **Notification Is Active**: 

Send a notification for incidents created in my account that match the following criteria:

**Recipients**

- Subscribe yourself, other users, or a connector to receive this notification.
- **Subscribe User(s)**: 
- **Subscribe Connector**: none
- **Subscribe Playbook**: none

**Notification Delivery**

- **Select User(s)**
- **Select All**
- **John Pirc** john.pirc@alertlogic.com (creator)

**Escalation**

Select escalations if you want to be notified when Alert Logic escalates an incident, regardless of threat level.

- **Escalated Incidents**: 

**Threat Levels**

If you select escalations and threat levels, incidents must match both criteria to trigger a notification.

- **Filter(s)**

```text
{{threat}} Threat Incident (ID:{{incident_id}}) : {{attack_summary}}
```
Setting a Playbook in Motion (cont)

Create an Incident Notification

Alert Logic sends you notifications when new or escalated incidents meet the criteria you set.

Recipients

Subscribe yourself, other users, or a connector to receive this notification.

- Subscribe User(s) (1)
- Subscribe Connector (none)
- Subscribe Playbook (none)

Notification Delivery

Select User(s)

- Select All
- John Pirc john.pirc@alertlogic.com (creator)

Email Subject

{{threat}} Threat Incident (ID:{{incident_id}}): {{attack_summary}}

Details

1. Name *

- Notification Is Active

Send a notification for incidents created in my account that match the following criteria:

Escalations

Select escalations if you want to be notified when Alert Logic escalates an incident, regardless of threat level.

- Escalated Incidents

Threat Levels

Select the threat levels for incidents.

- Critical Threat Level
- High Threat Level
- Medium Threat Level
- Low Threat Level

Select Medium

If you select escalations and threat levels, incidents must match both criteria to trigger a notification.
Setting a Playbook in Motion (cont)

Create an Incident Notification

Alert Logic sends you notifications when new or escalated incidents meet the criteria you set.

Details

Name *
Beta Day (Demo)

Notification is Active
Send a notification for incidents created in my account that match the following criteria:

Escalations

Select escalations if you want to be notified when Alert Logic escalates an incident, regardless of threat level.

Escalated Incidents

Threat Levels

If you select escalations and threat levels, incidents must match both criteria to trigger a notification.

Recipients

Subscribe yourself, other users, or a connector to receive this notification.

Subscribe User(s) (1)
Subscribe Connector (none)

Notification Delivery

Select Playbook

Add Note to Incident
Austin Texas
Automated Response SKO Demo (Do Not Delete)
Beta Day (Informational Playbook)
Carl Inquiry Verification
Carl Push Approval Test
Upcoming Notifications Change

Create an Incident Notification

Alert Logic sends you notifications when new or escalated incidents meet the criteria you set.

Details

Name *

Notification Is Active

Send a notification for incidents created in my account that match the following criteria:

Escalations

Select escalations if you want to be notified when Alert Logic escalates an incident, regardless of threat level.

Escalated Incidents

Threat Levels

If you select escalations and threat levels, incidents must match both criteria to trigger a notification.

Filter(s)

- Critical Threat Level
- High Threat Level
- Medium Threat Level
- Low Threat Level

Transferring this step to the Playbook

Notification Delivery

Select User(s)

- Select All
- John Pirc john.pirc@alertlogic.com (creator)

Email Subject

{threat} Threat Incident ID:{(incident_id)} : {attack_summary}
Relocation of (Threat Rating, Classification, Asset Groups, etc. to the Playbook)

Configuration | Automated Response

ServiceNow and AWS WAF Block
This is my playbook, there are many like it, but this one is mine.

Incident Response

Alert Logic Incident Generated

ServiceNow Create new Customer Service Case

AWS AWS WAF Block

Conditions If Succeeded

ServiceNow Update Customer Service Case

Alert Logic Close Incident

Conditions If Failed
Setting a Playbook in Motion (cont)

Lists your notifications for incidents and correlation observations that alert you to potential threats in near real time.

**Create a Notification**

<table>
<thead>
<tr>
<th>Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Beta Day (Demo)</strong></td>
</tr>
<tr>
<td>Most recent notification sent: No notifications sent.</td>
</tr>
<tr>
<td><strong>Darwin Test for info level notifications</strong></td>
</tr>
<tr>
<td>Most recent notification sent: Jan 26 2021 17:00:46 GMT-6</td>
</tr>
<tr>
<td><strong>High Incident Alert</strong></td>
</tr>
<tr>
<td>Most recent notification sent: Jan 26 2021 11:54:37 GMT-6</td>
</tr>
<tr>
<td><strong>Info Dev Test Incident Notification</strong></td>
</tr>
<tr>
<td>Most recent notification sent: No notifications sent.</td>
</tr>
</tbody>
</table>
Running an on-demand Playbook
Running an on-demand Playbook
Setting a Playbook in Motion (cont)

ID: 9sysx5 | Web App Security Integration
SQL Injection, Null Byte, Path Traversal Attempts from 7....
26th Jan 2021 11:54:29 GMT-6

Investigation Report

Topology

Audit Log

26th Jan 2021 11:54 GMT-6
Alert Logic created an incident.
Setting a Playbook in Motion (cont)
Setting a Playbook in Motion (cont)

Execution record created successfully. Go to Playbook History

ID: 9sysx5 | Web App Security Integration
SQL Injection, Null Byte, Path Traversal Attempts from 7....
26th Jan 2021 11:54:29 GMT-6

Investigation and Recommendation
Evidence

Investigation Report

Topology

Audit Log
Notification History

Audit Log
26th Jan 2021 11:54 GMT-6
Alert Logic created an incident.
Hello Alert Logic MDR Customer,

This IP ['7.33.6.77'] is bad

Please click on a link below to authorize the AWS WAF Block action:

Approve  Reject
Response Incident Update

ID: 9sysxs5 | Web App Security Integration
SQL Injection, Null Byte, Path Traversal Attempts from 7....
26th Jan 2021 11:54:29 GMT-6

Audit Log
26th Jan 2021 18:06 GMT-6
RESPONDER USER (AUTH ACCOUNT); Incident updated - Threat presents a valid risk, Taking action to mitigate the threat.
We need more information on IP
7.33.6.77

26th Jan 2021 11:54 GMT-6
Alert Logic created an incident.
# Playbook History

## Playbook Execution History

**Playbook Execution History**

<table>
<thead>
<tr>
<th>Playbook</th>
<th>Start</th>
<th>End</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beta Day (Informational Playbook)</td>
<td>Jan 26 2021 18:03:49 GMT-6</td>
<td>Jan 26 2021 18:06:50 GMT-6</td>
<td>incident</td>
<td>succeeded</td>
</tr>
<tr>
<td>Add Note to Incident</td>
<td>Jan 26 2021 17:18:52 GMT-6</td>
<td>Jan 26 2021 17:18:54 GMT-6</td>
<td>incident</td>
<td>failed</td>
</tr>
<tr>
<td>Add Note to Incident</td>
<td>Jan 26 2021 17:18:37 GMT-6</td>
<td>Jan 26 2021 17:18:38 GMT-6</td>
<td>incident</td>
<td>failed</td>
</tr>
<tr>
<td>Add Note to Incident</td>
<td>Jan 26 2021 17:18:30 GMT-6</td>
<td>Jan 26 2021 17:18:32 GMT-6</td>
<td>incident</td>
<td>failed</td>
</tr>
<tr>
<td>Add Note to Incident</td>
<td>Jan 26 2021 17:18:23 GMT-6</td>
<td>Jan 26 2021 17:18:24 GMT-6</td>
<td>incident</td>
<td>failed</td>
</tr>
<tr>
<td>Channels test</td>
<td>Jan 26 2021 16:28:18 GMT-6</td>
<td>Jan 26 2021 16:28:36 GMT-6</td>
<td>incident</td>
<td>succeeded</td>
</tr>
</tbody>
</table>
Playbook History (cont)
Playbook History (cont)

<table>
<thead>
<tr>
<th>Name</th>
<th>Action</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>send_approval_email0</td>
<td>send_approval_email</td>
<td>failed</td>
</tr>
</tbody>
</table>

**Input**

```json
{
  "account_id": "134264762",
  "user_ids": [
    "198F396F-8848-4183-0B88-084CF995B028"
  ],
  "message": "This IP ['7.33.6.77'] is bad"
}
```

**Output**

```json
{
  "output": null,
  "errors": [
    {
      "type": "error",
      "message": "Execution failed. See result for details."
    }
  ]
}
```
# Inquires (Pending Playbooks)

## Playbooks

<table>
<thead>
<tr>
<th>Playbook</th>
<th>Status</th>
<th>Start Time</th>
<th>End Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beta Day (Informational Playbook)</td>
<td>succeeded</td>
<td>Jan 26 2021 18:03:52 GMT-6</td>
<td>Jan 26 2021 18:06:43 GMT-6</td>
</tr>
<tr>
<td>Channels test</td>
<td>succeeded</td>
<td>Jan 26 2021 16:28:21 GMT-6</td>
<td>Jan 26 2021 16:28:31 GMT-6</td>
</tr>
<tr>
<td>Channels test</td>
<td>succeeded</td>
<td>Jan 26 2021 16:27:21 GMT-6</td>
<td>Jan 26 2021 16:27:52 GMT-6</td>
</tr>
<tr>
<td>Channels test</td>
<td>pending</td>
<td>Jan 26 2021 16:23:12 GMT-6</td>
<td></td>
</tr>
<tr>
<td>Test Multiple Email Recipients</td>
<td>succeeded</td>
<td>Jan 25 2021 14:14:00 GMT-6</td>
<td>Jan 25 2021 14:15:11 GMT-6</td>
</tr>
<tr>
<td>Automated Response SKO Demo (Do Not Delete)</td>
<td>pending</td>
<td>Jan 25 2021 13:44:54 GMT-6</td>
<td></td>
</tr>
</tbody>
</table>
Inquires (Pending Playbooks)

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Status</th>
<th>Date/Time Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Demo (Do Not Delete)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Beta Day (Informational Playbook)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>email</td>
<td></td>
<td></td>
</tr>
<tr>
<td>channels</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mobile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>send_approval_email</td>
<td></td>
<td></td>
</tr>
<tr>
<td>send_approval_channels</td>
<td></td>
<td></td>
</tr>
<tr>
<td>send_approval_push</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RequestBlockApproval</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Channels test</td>
<td>pending</td>
<td>Jan 26 2021 16:23:12 GMT-6</td>
</tr>
<tr>
<td>ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B6277B19-CB6E-4696-8436-25BDA749B3D5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>send_approval_channels</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>test</td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>pending</td>
<td></td>
</tr>
<tr>
<td>Start at</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jan 26 2021 16:23:12 GMT-6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logs</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Test Multiple Email Recipients: succeeded Jan 25 2021 14:14:00 GMT-6
2. Test Multiple Email Recipients: succeeded Jan 25 2021 13:09:26 GMT-6
3. Test Multiple Email: succeeded Jan 25 2021 12:48:41
Questions
Resources

• Alert Logic Beta Forum
  • Beta Support - Requires Login

• Technical documentation
  • Threat Intelligence
  • Asset Groups
  • Automated Response

• Video
  • Beta Kick-off On-Demand Webinar
  • YouTube: Alert Logic Automated Response Overview
Thank You
Simple Workflow

Demo Playbook (Block IP on AWS WAF) Template

- **Playbook Context**
- **ServiceNow**
  - CreateServiceNowIncident
- **Input**
  - log_snow_id
- **Alert Logic**
  - RequestBlockApproval

- **Condition**
  - If approved
  - If rejected

- **AWS**
  - BlockIP_RegionalWAF

- **Alert Logic**
  - UpdateIncident
  - CloseIncident
Complex Workflow