

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

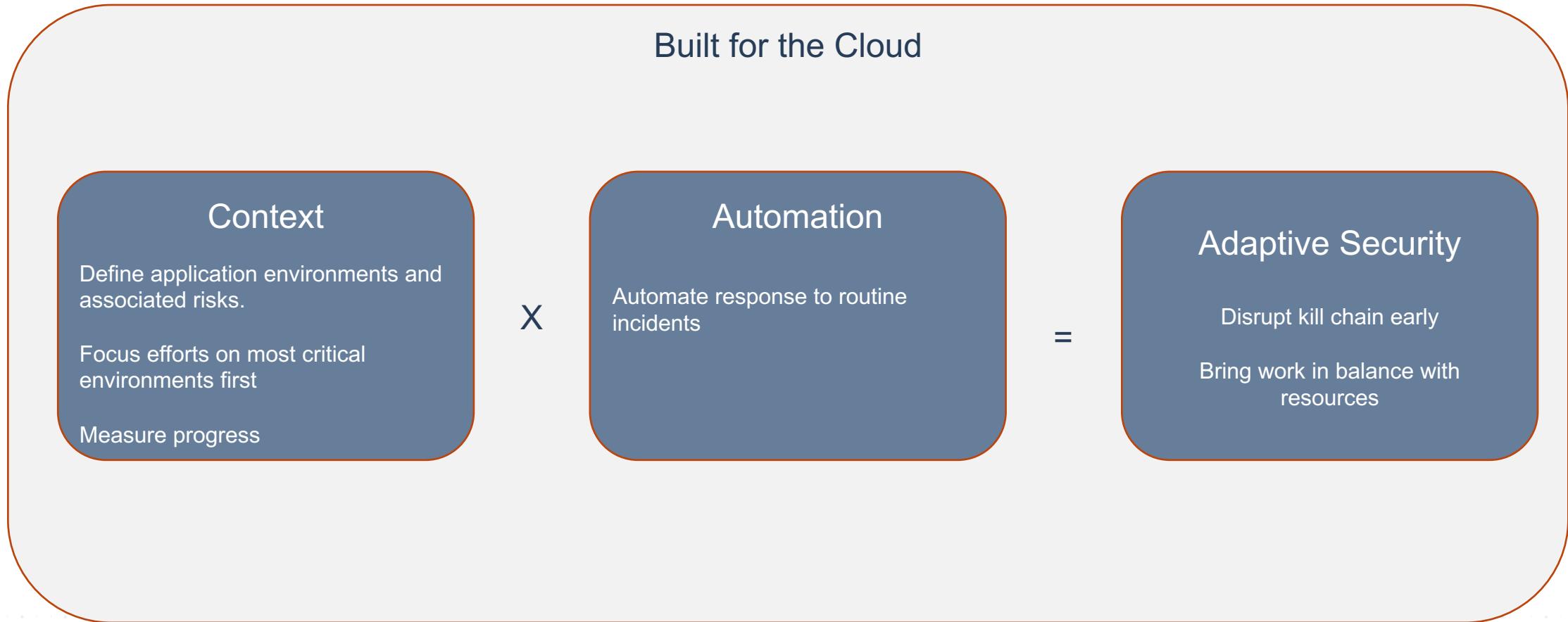


Agenda

- Response Overview
- Demo
 - Threat Intel Center
 - Asset Groups
 - Approval
- Resources



Alert Logic: A New Response Equation



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

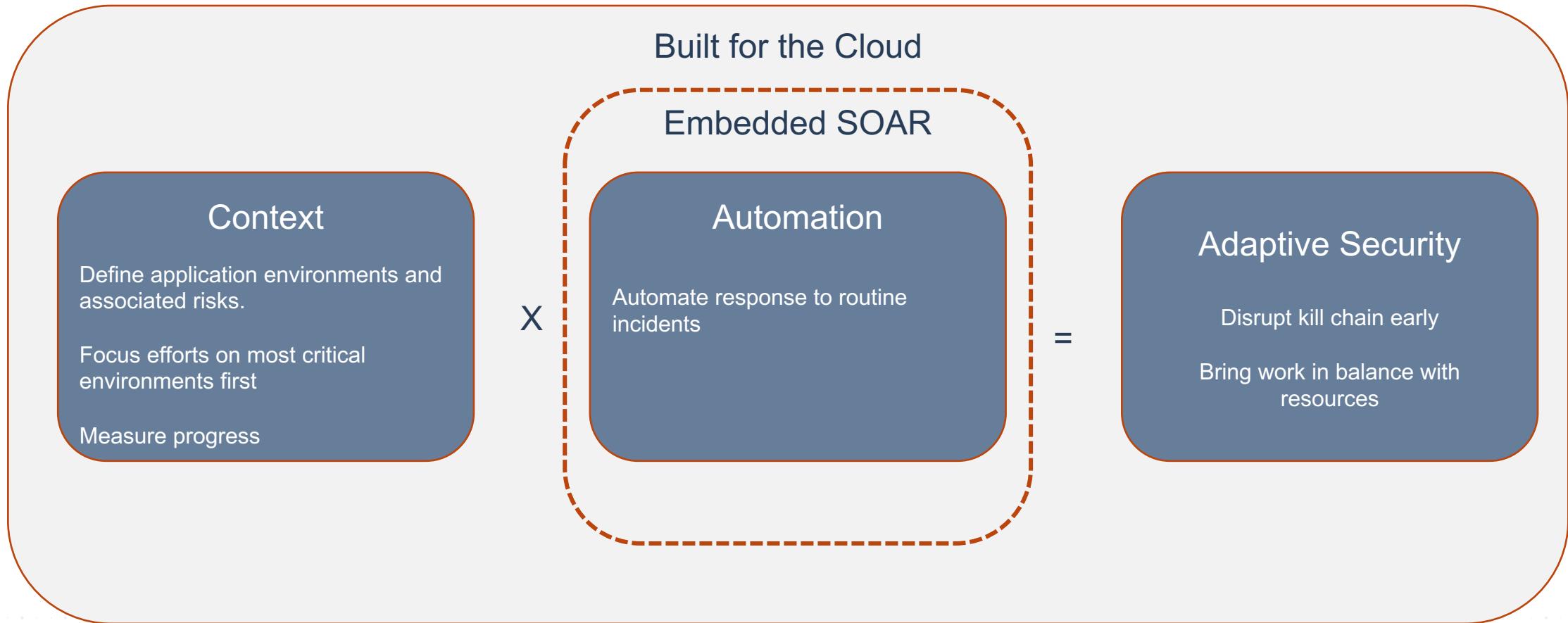
- Is Joe's laptop compromised or is it the CFO's?
- Is it the T-shirt giveaway registration app or the e-commerce system?
- Is it a service that has access to PHI? Cardholder data?

Risk to the Business

Urgency of Response

Automated Action that is Appropriate

Alert Logic: A New Response Equation



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

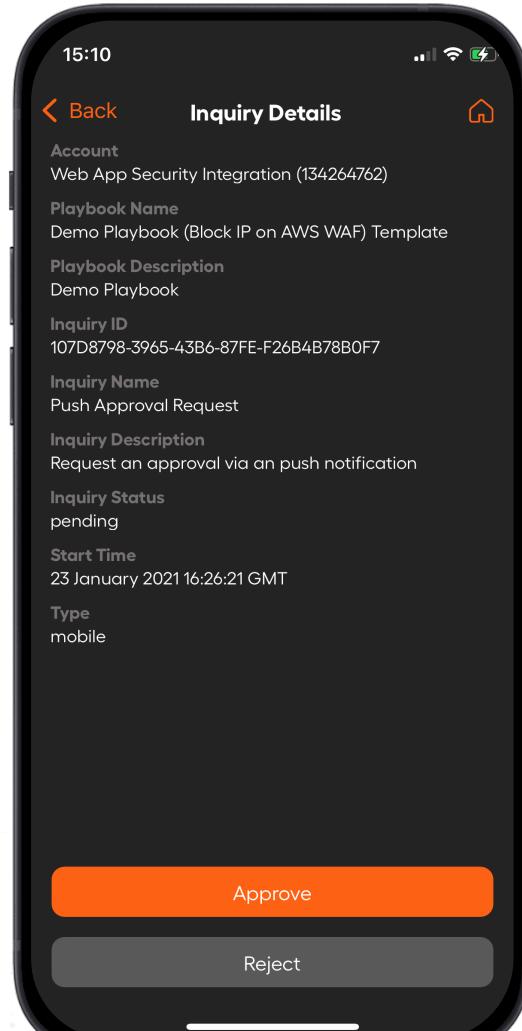
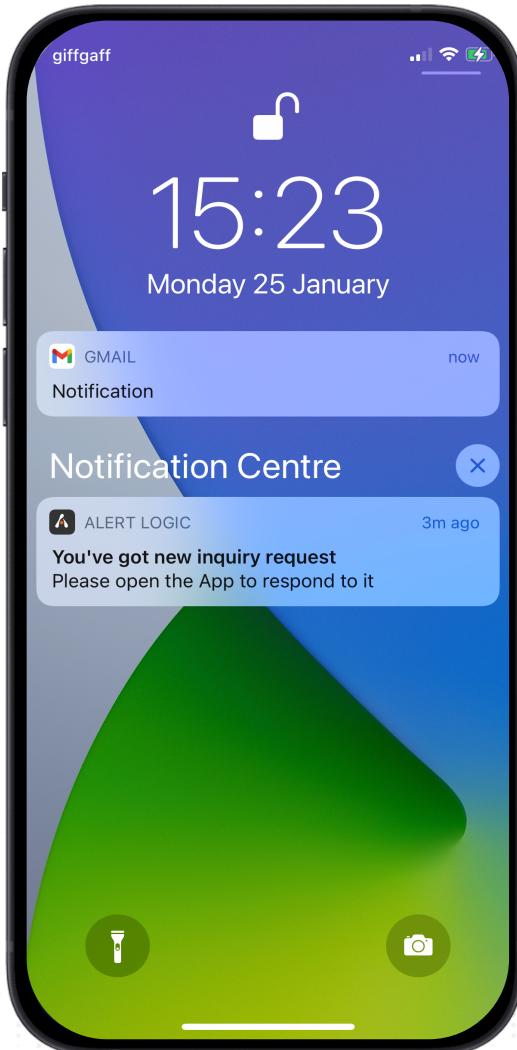
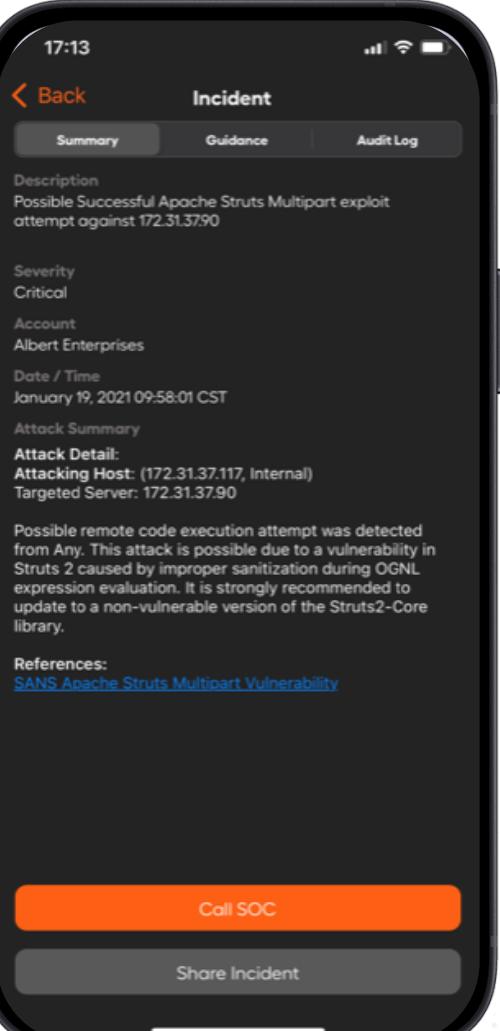
- Trust but verify



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

1 Details — 2 Configuration

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

Assets Tags Expression

Select Asset Filters (5 Selected) Search Q

Name	Location	Cloud	Tags	Count
990023346368				16 18 55 0
ca-central-1				1 3 0
vpc-dc155db4				3 0
subnet-48cb4132				
subnet-9fecfec3				
subnet-ce552ba6				
ap-northeast-2				1 4 0
vpc-0f64be64				4 0
eu-north-1				1 3 0
us-west-2				1 5 0
us-east-2				1 3 0
eu-west-3				1 3 0
eu-central-1				1 2 0

wla-us-east-1-int-windows-logs

Architecture	x86_64	<input checked="" type="checkbox"/> <input type="checkbox"/>
Availability Zone	us-east-1d	<input checked="" type="checkbox"/> <input type="checkbox"/>
Instance ID	i-06f1e8d6f4a1fa233	<input checked="" type="checkbox"/> <input type="checkbox"/>
Instance Name	wla-us-east-1-int-windows-logs	<input checked="" type="checkbox"/> <input type="checkbox"/>
Instance Type	t2.small	<input checked="" type="checkbox"/> <input type="checkbox"/>
Launch Time	1585766677	<input checked="" type="checkbox"/> <input type="checkbox"/>
Private DNS Name		<input type="text"/> <input type="button"/>

CANCEL UPDATE

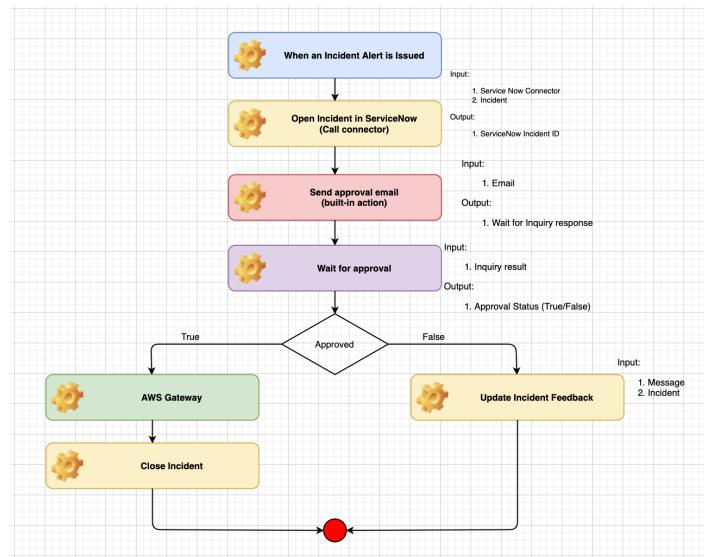
Demo

About the Beta Environment

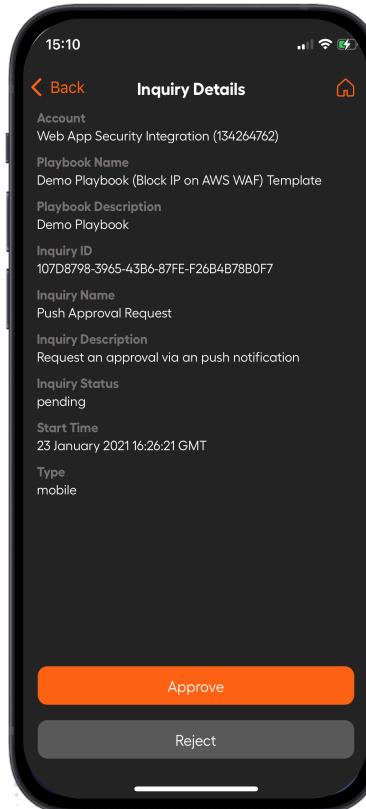
Platform



Playbook



Approval



Outcomes

Block Attacker

Disable User Account



Threat Intel Center

Threat Intel Center (Getting Started)

The screenshot shows the AWS CloudTrail Metrics Dashboard. The left sidebar includes links for Dashboards, Respond, Investigate, Threat Intel Center (which is highlighted with a red box), Validate, Configure, Manage, and Support. The main area displays several cards:

- Open CVE Count:** 0
- Open Security Remediations:** 211
- Vulnerability Trend by Severity:** A line chart showing the count of vulnerabilities over time from December 28 to January 27. The Y-axis ranges from 10 to 1k. The legend indicates four severity levels: High (red), Medium (orange), Low (yellow), and Info (grey).
- Vulnerabilities by Deployment:** A bar chart showing the count of vulnerabilities for different log sources. The X-axis lists deployment IDs: 990023346368, WLA Integration Log Source, 055103733742, 674305394241, 582159568573, and 707124421633. The Y-axis ranges from 0 to 1k. The legend indicates four severity levels: High (red), Medium (orange), Low (yellow), and Info (grey).
- Top Security Remediations by Impacted Assets:** A table listing remediations and their asset counts.

Name	Asset Count
Determine if privileged access is needed.	138
Enable S3 Logging and Object Versioning	109
Enable log metric filters and alarms.	98
Ensure rotation for customer created CMKs is enabled.	72
Base IAM policy on 'least-privileged'	29
Add traffic restrictions to default security group	16
Enable AWS support role	6

At the bottom right, there are buttons for "EXPORT TO CSV" and "INVESTIGATE".

Threat Intel Center Landing Page

The screenshot displays the Threat Intel Center landing page with the 'Analytics' tab selected. The interface includes search filters, a main table of threat intelligence items, and a detailed view for one specific item.

Search Filters (Left Sidebar):

- Threat Level:
 - Critical: 125
 - High: 683
 - Medium: 273
 - Low: 76
- Telemetry:
 - logmsgs: 16
 - Log: 315
 - IDS: 775
 - None: 51
- Response Actions:
 - Quarantine: 339
 - Block: 519
 - None: 299
- Threat Classification:
 - ubad:anomaly: 2
 - susp_config_change: 1
 - malware: 1
 - logreview:anomaly: 10
 - firewall:activity: 5

Analytics Section (Main Content):

Table Headers: Name, Summary, Threat Level, Telemetry

Table Data:

Name	Summary	Threat Level	Telemetry
accessanomaly	Access to Anomalous Resource from %distinct%	Medium	None
accessunauth	Access to Unauthorized Resource from %distinct%	Medium	None
AdminAppAccess	['VENDOR'] User ['SOURCE_USERNAME'] Attempting to Access Admin Application	Medium	logmsgs
AdminPrivilegeGrant	['VENDOR'] User ['DESTINATION_USERNAME'] Granted Admin Privileges by ['SOURCE_USERNAME']	Medium	logmsgs
app/cve20000800	CVE-2000-0800 Linux rpc.kstadb String Parsing Error RCE attack from 1.2.3.4	High	IDS
app/cve20176553	CVE-2017-6553 Quest Privilege Manager buffer overflow attempt from 1.2.3.4	High	IDS
app/educatedscholar	EDUCATEDSCHOLAR SMB attack attempt from 1.2.3.4	High	IDS
app/esteemaudit	ESTEEMAUDIT 2 Stage Information Disclosure from 1.2.3.4	High	IDS
app/eternalblue		High	Log

Detail View (Right Sidebar):

AdminPrivilegeGrant

Summary: ['VENDOR'] User ['DESTINATION_USERNAME'] Granted Admin Privileges by ['SOURCE_USERNAME']

Threat Level: Medium

Telemetry: logmsgs

Technology: AE

Visibility: Incident

Log Source: Microsoft Windows, Okta SSO

Logs: Okta User Granted Administrator Privileges, Ossec Windows User Account Changed, ProtoBase User Account Information, ProtoBase User Account Modified, Windows Special Groups have Been Assigned To A New Logon, Windows System Security Access Granted, Windows User Account Changed

Signatures: None

Customize Table

Investigate | Threat Intelligence Center

Analytics 1.1k

search filters

Threat Level

- Critical 125
- High 683
- Medium 273
- Low 76

Telemetry

- logmsgs 16
- Log 315
- IDS 775
- None 51

Response Actions

- Quarantine 339
- Block 519
- None 299

Threat Classification

- ubad:anomaly 2
- susp_config_change 1
- malware 1
- logreview:anomaly 10
- firewall:activity 5
- evolution 1
- endpoint-high:av-xinfect-yhosts 1

Choose Columns (4 of 15 Shown)

- Logs
- Name
- Recommendations
- Response Actions

Analytics

Summary	Threat Level	Telemetry
Access to Anomalous Resource from %distinct%	Medium	None
Access to Unauthorized Resource from %distinct%	Medium	None
['VENDOR'] User ['SOURCE_USERNAME'] Attempting to Access Admin Application	Medium	logmsgs
['VENDOR'] User ['DESTINATION_USERNAME'] Granted Admin Privileges by ['SOURCE_USERNAME']	Medium	logmsgs
CVE-2000-0800 Linux rpc.kstated String Parsing Error RCE attack from 1.2.3.4	High	IDS
CVE-2017-6553 Quest Privilege Manager buffer overflow attempt from 1.2.3.4	High	IDS
EDUCATEDSCHOLAR SMB attack attempt from 1.2.3.4	High	IDS
ESTEEMAUDIT 2 Stage Information Disclosure from 1.2.3.4	High	IDS
	High	Log
ETERNALBLUE svrnet.sys RCE possible success from 1.2.3.4	High	IDS

accessanomaly

Summary

Access to Anomalous Resource from %distinct%

Threat Level

Medium

Telemetry

None

Technology

AE

Visibility

Incident

Log Source

None

Logs

Not Applicable

Signatures

None

Filter Analytics List

The screenshot shows the Alert Logic Threat Intelligence Center interface. The left sidebar contains filter options: 'Analytics' (1.1k), 'search filters' (with 'CLEAR ALL FILTERS' button), 'Threat Level' (set to 'Critical' with 13 results), 'Telemetry' (Log: 7, IDS: 6), 'Response Actions' (Block: 13), and 'Threat Classification' (None: 13). The main content area is titled 'Analytics' and lists 15 security events. Each event includes a summary, threat level (all Critical), and telemetry type (IDS or Log). The first event is highlighted.

Name	Summary	Threat Level	Telemetry
successful_sqli/sqli_success	Successful SQL Injection from 1.2.3.4	Critical	IDS
successful_sqli/sqli_error	Possible Successful SQL Injection from 1.2.3.4	Critical	Log
successful_sqli/roamer_php_webshell_success	Successful Roamer PHP Web Shell Access By 1.2.3.4	Critical	IDS
successful_sqli/cve20157857s	Possible Successful CVE-2015-7857 SQL Injection attempt from 1.2.3.4	Critical	IDS
successful_sqli/apache_struts_scan_success	Successful Apache Struts CVE-2013-2251 scan from 1.2.3.4	Critical	IDS
bf_success/xmlrpcs		Critical	Log
bf_success/unix	Successful Unix Bruteforce Login detected from 1.2.3.4	Critical	Log
bf_success/tomcat	Possible Successful Tomcat Login from 1.2.3.4	Critical	IDS
bf_success/remote_root_login_ssh	Successful Remote SSH Root Login from 1.2.3.4	Critical	Log

Details for the first event:

- successful_sqli/apache_struts_scan_success
- Summary: Successful Apache Struts CVE-2013-2251 scan from 1.2.3.4
- Threat Level: Critical
- Telemetry: IDS
- Logs: 251
- Technology: NGX
- Visibility: Incident
- Log Source: None
- Logs: Not Applicable
- Signatures: 1102154, 1102167, 1102179

Search Analytics List

Investigate | Threat Intelligence Center

Analytics 1.1k

search filters

CLEAR ALL FILTERS

Threat Level Critical 125

Telemetry Log 30
IDS 95

Response Actions Quarantine 101
Block 13
None 11

Threat Classification None 125

Analytics

Choose Columns (6 of 15 Shown) ▾

powershell

Name	Summary	Threat Level	Telemetry	Logs	Signatures
postcomp/resbv9545	Potential lateral movement using PowerShell and WMIC detected on 1.2.3.4	Critical	Log	Windows Process Created	None
postcomp/powershell_sv_create	Suspicious service created with PowerShell on 1.2.3.4	Critical	Log	Windows PowerShell Provider Started, Windows Service Installed	None
postcomp/powershell_nishang	PowerShell Nishang Usage Detected on 1.2.3.4	Critical	Log	Windows PowerShell Operational Log, Windows Sysmon File Created, Windows Sysmon Process Created, Windows	None
postcomp/powershell_empire	PowerShell Empire Usage Detected on 1.2.3.4	Critical	Log	Windows PowerShell Operational Log	None
postcomp/monero_miner_dropper_carbon_downloaded	Powershell script to execute Monero (XMR) miner XMRig downloaded on 1.2.3.4	Critical	IDS	Not Applicable	1102125

postcomp/monero_miner_carbon_powershell

Summary Powershell script to retrieve Carbon dropper for Monero (XMR) miner XM Rig downloaded on 1.2.3.4

Threat Level Critical

Telemetry IDS

Technology NGX

Visibility Incident

Log Source None

Logs Not Applicable

Signatures 1102123

Open Analytic Details

The screenshot shows a web-based threat intelligence interface. At the top, there's a navigation bar with a logo, user information (Malcolm Palmer, Respond Only Acc...), and a location (US-EAST-1 (US)). Below the header, a search bar contains the text "Investigate | Threat Intelligence Center". A red box highlights a specific alert message: "Metasploit PowerShell backdoor installation detected on ['ip_address']". This alert is preceded by a red circular icon. Below this, a large red box encloses the "Analytic Details" section. This section includes fields for Name (postcomp/metasploit_ps_persistence), Summary (Metasploit PowerShell backdoor installation detected on ['ip_address']), Description (a detailed explanation of the detection), Recommendations (remediation steps), Threat Level (Critical), and Visibility (Incident). Further down, there's a table comparing Technology (NGX), Telemetry (Log), Log Source (Log), and Log Message Types (Windows PowerShell Engine State Changed). Another table compares Signatures (None) and CWE (None) against Threat Classification (None). At the bottom, another red box highlights the "Response Actions" section, which lists "Quarantine" and "victim" under "Response Action Parameters". The footer features the Alert Logic logo.

Malcolm Palmer ▾ Respond Only Acc... ▾ | US-EAST-1 (US)

Investigate | Threat Intelligence Center

Metasploit PowerShell backdoor installation detected on ['ip_address']

Analytic Details

Name
postcomp/metasploit_ps_persistence

Summary
Metasploit PowerShell backdoor installation detected on ['ip_address']

Description
We have detected the installation of a persistent backdoor on ['ip_address']. As post-compromise activity, an attacker can utilize a crafted Managed Object File (MOF) to execute PowerShell commands. Local administrator rights are required in order to be successful, and this installation can result in further propagation, data loss, and/or loss of integrity.

Recommendations
Remediation Recommendations: A compromised host should be isolated from the network and cleaned. You will want to remove the back doors installed and check the system logs for other actions taken. Once a system is compromised usually one of the first things done by an attacker is creating a secondary access channel. Assume that additional modifications have been made to the system beyond the initial breach.

Threat Level
Critical

Visibility
Incident

Technology	Telemetry	Log Source	Log Message Types
NGX	Log	Log	Windows PowerShell Engine State Changed

Signatures	CVE	CWE	Threat Classification
None			None

Response Actions

Response Action Parameters
Quarantine victim



Asset Groups

Asset Groups (Getting Started)

John Pirc | Web App Security I... | US-EAST-1 (US)

Dashboards

WHAT'S NEW

Data for the last: 7d 14d 30d Custom range: 27 Dec 2020 - 26 Jan 2021

Open CVE Count: 0 INVESTIGATE

Open Remediations: 211 INVESTIGATE

Vulnerability Trend by Severity

Count of Vulnerabilities

Dec 27 Dec 29 Dec 31 Jan 02 Jan 04 Jan 06 Jan 08 Jan 10 Jan 12 Jan 14 Jan 16 Jan 18 Jan 20 Jan 22 Jan 24 Jan 26

High Medium Low Info

Vulnerabilities by Deployment

Top Remediations by Impacted Assets

Name	Asset Count
Determine if privileged access is needed.	138

Asset Groups

Manage

Support

The screenshot shows the Alert Logic dashboard interface. On the left, a sidebar lists various security modules: Respond, Investigate, Validate, Configure, Deployments, Log Management, Application Registry, Certificates and Keys, WAF, PCI Scanning, Connectors, Asset Groups (which is highlighted with a red box), Manage, and Support. The main dashboard area displays several cards: 'Open CVE Count' (0), 'Open Remediations' (211), 'Vulnerability Trend by Severity' (a line chart showing counts for High, Medium, Low, and Info severity levels over time), 'Vulnerabilities by Deployment' (a bar chart showing deployment counts), and 'Top Remediations by Impacted Assets' (a table with one entry). The top navigation bar includes user information (John Pirc) and a location dropdown (Web App Security I... | US-EAST-1 (US)). The overall theme is dark with light-colored text and highlights.

Asset Groups Landing Page

The screenshot shows a web-based application interface for managing asset groups. At the top, there is a dark header bar with the Alert Logic logo, the user name "John Pirc", the project name "Web App Security I...", and the location "US-EAST-1 (US)". Below the header, a secondary navigation bar includes a "Configure | Asset Groups" link. A prominent orange button with a white plus sign and the text "Add an Asset Group" is located on the left side. To its right, a descriptive text explains that asset groups allow for organizing assets and configuring notifications or ticketing system connections. A search bar with a magnifying glass icon is positioned at the top right. The main content area is titled "Asset Groups" and displays three entries in a table format:

Asset Group Name	Last Updated	Assets	Action
Robs Things	Last Updated: 20 Jan 2021	478 Assets	View
Matts Hosts	Last Updated: 29 Dec 2020	2 Assets	View
Asset Group Demo	Last Updated: 20 Jan 2021	1566 Assets	View

Adding an Asset Group

The screenshot shows a user interface for managing asset groups. At the top, there's a navigation bar with a logo, the user's name "John Pirc", a dropdown menu, and the location "Web App Security I... | US-EAST-1 (US)". Below the navigation is a header with a gear icon and the text "Configure | Asset Groups". A large orange button with a white plus sign is labeled "Add an Asset Group". A tooltip for this button is visible, containing the text "Asset Group" and "Linked Asset Group". To the right of the button is a search bar with the placeholder "search" and a magnifying glass icon. The main content area is titled "Asset Groups" and lists three existing groups: "Robs Things", "Matts Hosts", and "Asset Group Demo". Each group entry includes the group name, last update date, the number of assets (478, 2, or 1566), and a "View" link.

John Pirc | Web App Security I... | US-EAST-1 (US)

Configure | Asset Groups

Add an Asset Group

Asset Group

Linked Asset Group

search

Robs Things

Last Updated: 20 Jan 2021

478 Assets

Matts Hosts

Last Updated: 29 Dec 2020

2 Assets

Asset Group Demo

Last Updated: 20 Jan 2021

1566 Assets

Adding an Asset Group (Step 1)

Add an Asset Group



1 Details — 2 Configuration

Provide details about your new asset group

1

Name *
PCI

3

Criticality Rating
3

2

Description *
Assets in Scope

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.)

CANCEL

SAVE AND CONTINUE

Adding an Asset Group (Step 2)

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

Tags

Expression

Select Asset Filters (5 Selected)

▼ Search



Name				
> 990023346368	16	18	55	0
> 674305394241	16	11	33	0
> Alert Logic Collector Support Deployment	1	0	0	0
> WLA Integration Log Source	16	21	57	3
> 055103733742	16	7	20	1
> 582159568573	16	7	22	0
> 707124421633	16	12	38	0

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.

CANCEL

ADD

Adding an Asset Group (Step 3)

Add an Asset Group

X

1 Details — 2 Configuration

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

Assets

Tags

Expression

Select Asset Filters (5 Selected)

Search



Name	Location	Cloud	Network	Compute
WLA Integration Log Source	eu-central-1	16	21	57
eu-central-1		1	3	0
us-west-1		1	2	0
us-east-1		2	7	2
cas-dev-wla-us-east-1-int		1	1	
vpc-be8c16d9		6	1	
subnet-86a2118a				
subnet-0f1df346		1		

1

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.



CANCEL

ADD

Adding an Asset Group Inclusions (Step 4)

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 Tags Expression

Select Asset Filters (5 Selected) ▾ Search

Name	Location	Cloud	Network	Compute
<input checked="" type="checkbox"/> AWS Fargate Demo	<input checked="" type="checkbox"/> sa-east-1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	<input checked="" type="checkbox"/> eu-west-2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	<input checked="" type="checkbox"/> ca-central-1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	<input checked="" type="checkbox"/> eu-north-1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	<input checked="" type="checkbox"/> ap-southeast-2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	<input checked="" type="checkbox"/> ap-east-1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	<input checked="" type="checkbox"/> us-west-2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

1 AWS Fargate Demo

2 ssehic-wsm-test

Architecture: x86_64

Availability Zone: us-west-2a

Instance ID: i-07f6082e466fa3b87

Instance Name: ssehic-wsm-test

CANCEL ADD

Adding an Asset Group Exclusions (Step 5)

Add an Asset Group

X

1 Details — 2 Configuration

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

Assets **Tags** **Expression**

Select Asset Filters (5 Selected) ▾ Search 🔍

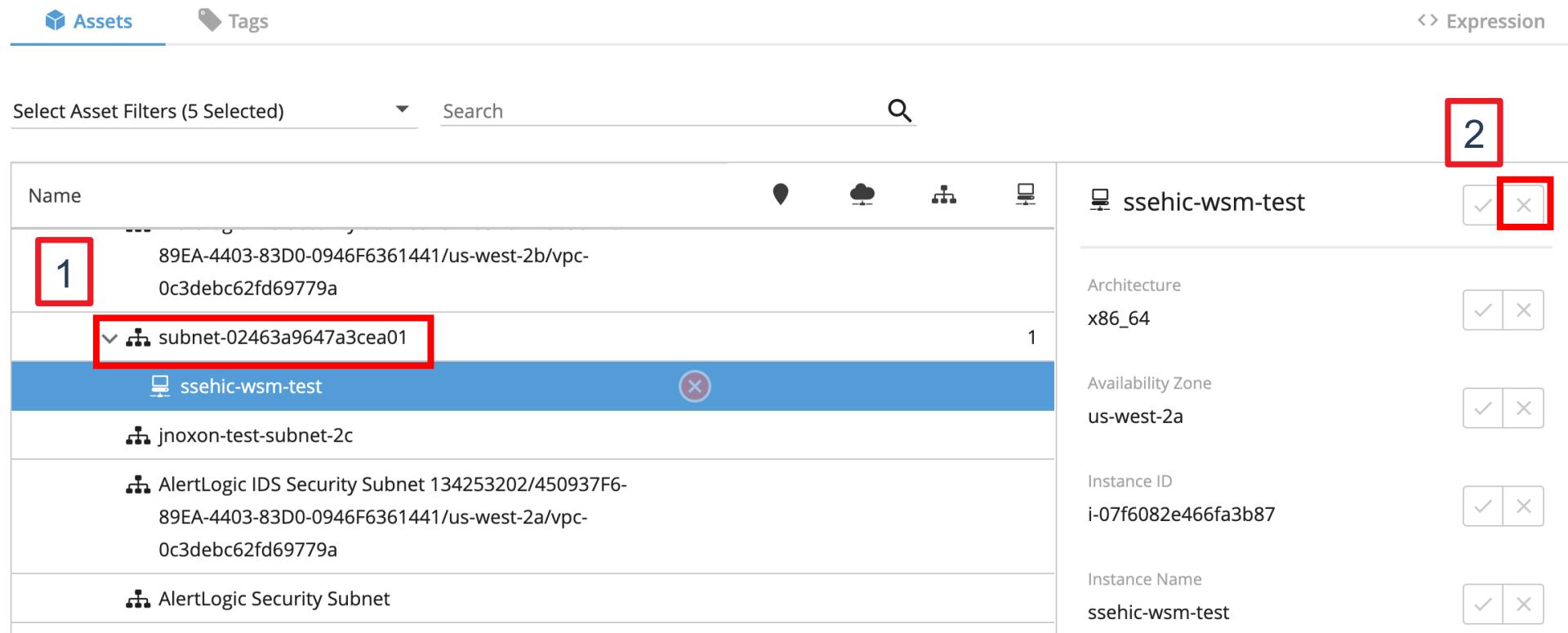
Name	Location	Count
89EA-4403-83D0-0946F6361441/us-west-2b/vpc-0c3debc62fd69779a	1	
subnet-02463a9647a3cea01	1	
ssehic-wsm-test	1	
jnoxon-test-subnet-2c	1	
AlertLogic IDS Security Subnet 134253202/450937F6-89EA-4403-83D0-0946F6361441/us-west-2a/vpc-0c3debc62fd69779a	1	
AlertLogic Security Subnet	1	

1 **2**

ssehic-wsm-test

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)

Edit an Asset Group

X

1 Details — 2 Configuration

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

Assets

Tags

↳ Expression

Search



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

CANCEL

UPDATE



Working with Asset Group Expressions

Edit an Asset Group X

1 Details — 2 Configuration

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

Assets

Tags

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](#)

The screenshot shows the Expression Editor interface. A red box labeled '1' highlights the 'Expression' tab at the top of the editor window. Another red box labeled '2' highlights the 'EDIT' button in the top right corner of the editor window. The editor window displays the following JSON code:

```
1 {  
2   "scopes": [  
3     {  
4       "include": [  
5         "host:/aws/us-east-1/host/i-0c8c2c7299a76395f"  
6       ]  
7     }  
8   ]  
9 }
```

At the bottom right of the editor window, there are 'CANCEL' and 'UPDATE' buttons.



CANCEL

UPDATE

30

Creating Linked Asset Groups

The screenshot shows the Alert Logic web application interface for managing asset groups. At the top, there is a navigation bar with the Alert Logic logo, user name "John Pirc", a dropdown menu for "Web App Security I...", and a location indicator "US-EAST-1 (US)". Below the navigation bar, the page title is "Configure | Asset Groups". A large orange button labeled "+ Add an Asset Group" is prominently displayed. A tooltip for this button provides instructions: "You can add 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." The "Linked Asset Group" option in this tooltip is highlighted with a red box. Below the button, there is a search bar with the placeholder "search" and a magnifying glass icon. The main content area is titled "Asset Groups" and lists several groups:

Asset Group Name	Last Updated	Number of Assets	Action
Rob's Things	20 Jan 2021	478 Assets	View
Matt's Hosts	29 Dec 2020	2 Assets	View
Asset Group Demo	20 Jan 2021	1566 Assets	View
PCI	26 Jan 2021	2 Assets	Hide

At the bottom of the screen, there is a footer with the Alert Logic logo and the number "31".

Creating Linked Asset Groups (cont)

Add a Linked Asset Group

1 Details — 2 Configuration

Provide details about your new asset group

1

Name *

Compliance

3

Criticality Rating

3

2

Description *

Critical Assets in Scope

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.)

CANCEL

SAVE AND CONTINUE

Creating Linked Asset Groups (cont)

Add a Linked Asset Group

X

1 Details — 2 Configuration

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

PCI, Matts Hosts

1

2

PCI, Matts Hosts

-
- Robs Things
- Matts Hosts
- Asset Group Demo
- PCI

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.

CANCEL

ADD

Creating Linked Asset Groups (cont)

The screenshot shows the Alert Logic web application interface. At the top, there is a dark header bar with the Alert Logic logo, user name "John Pirc", a dropdown menu "Web App Security I...", and location "US-EAST-1 (US)". Below the header is a navigation bar with a gear icon and the text "Configure | Asset Groups". A search bar with the placeholder "search" and a magnifying glass icon is also present.

The main content area is divided into two sections: "Asset Groups" and "Linked Asset Groups".

Asset Groups:

- Robs Things: Last Updated: 20 Jan 2021, 478 Assets, View
- Matts Hosts: Last Updated: 29 Dec 2020, 2 Assets, View
- Asset Group Demo: Last Updated: 20 Jan 2021, 1566 Assets, View
- PCI: Last Updated: 26 Jan 2021, 2 Assets, View

Linked Asset Groups:

- Compliance: Last Updated: 26 Jan 2021, 2 Groups, View

A red rectangular box highlights the "Compliance" entry in the "Linked Asset Groups" section.

Asset Groups and Exposures

John Pirc ▾ Albert Enterprises ▾ | US-WEST-1 (US)

≡ Respond | Exposures HELP

Category	Value	Description	Affected Assets	Exposure Instances	Open	View
Security	2.5k	<input type="checkbox"/> Determine if privileged access is needed. ● 114 ○ 0 ○ 0 ○ 0 TRI 400.35	42	114	>	Open
IAM Access Analyzer	94		94	94	>	View
External	41		38	49	>	View
Deployment	1.4k	<input type="checkbox"/> Review the IAM Access Analyzer findings for this account. ● 94 ○ 0 ○ 0 ○ 0 TRI 343.57	22	205	>	View
AWS Production Deployment	430		7	188	>	View
Fargate Demo	409		3	84	>	View
Ozone	299	<input type="checkbox"/> Restrict access to/from non-required IP addresses ● 40 ○ 6 ○ 0 ○ 3 TRI 332.58	15	15	>	View
Development Azure Environment	12		73	73	>	View
Production Data Center	7	<input type="checkbox"/> Upgrade OpenBSD OpenSSH to version 8.3.0 ● 29 ○ 155 ○ 21 ○ 0 TRI 318.99				
Training-Lab-Test						
Platform	2.2k					
AWS	299					
Azure	19					
Data Center						
Asset Group	398					
JP Test	75	<input type="checkbox"/> Enable log metric filters and alarms. ● 0 ○ 84 ○ 0 ○ 0 TRI 211.30				
AWS Production Web Servers						
Select a deployment to view additional asset filters.						

Asset Group JP Test 398 AWS Production Web Servers 75

Select a deployment to view additional asset filters.

Asset Groups and Exposures

John Pirc ▾ Albert Enterprises ▾ | US-WEST-1 (US)

☰ 🛡 Respond | Exposures ? HELP

Category	Deployment	Platform	Asset Group	Assets	Instances	Open	View
Medium	Ozone	AWS	JP Test	10 Affected Assets	34 Exposure Instances	Open	View
Low				1 Affected Assets	28 Exposure Instances	Open	View
Info				8 Affected Assets	12 Exposure Instances	Open	View
				10 Affected Assets	20 Exposure Instances	Open	View
				1 Affected Assets	16 Exposure Instances	Open	View
				1 Affected Assets	18 Exposure Instances	Open	View
				4 Affected Assets	4 Exposure Instances	Open	View

94 | 0 | 0 | 0 | TRI 343.57

Security

Determine if privileged access is needed.
34 | 0 | 0 | 0 | TRI 119.40

Security

Enable log metric filters and alarms.
0 | 28 | 0 | 0 | TRI 70.43

Security

Restrict access to/from non-required IP addresses
8 | 3 | 0 | 1 | TRI 70.29

Security

Add traffic restrictions to default security group
0 | 20 | 0 | 0 | TRI 40.01

Security

Upgrade OpenBSD OpenSSH to version 8.3.0
6 | 9 | 1 | 0 | TRI 35.75

Security

Upgrade Php to version 7.3.21
4 | 14 | 0 | 0 | TRI 35.03

Security

Use AWS SSL security policy for ELB
4 | 0 | 0 | 0 | TRI 32.00

Medium 156

Low 31

Info 41

Category Security 398

IAM Access Analyzer 94

Deployment Ozone 398

Platform AWS 398

Asset Group JP Test 398

Select a deployment to view additional asset filters.

Asset Groups and Health

The screenshot shows the Atera Cloud interface with the following details:

Header: John Pirc ▾ Albert Enterprises ▾ | US-WEST-1 (US)

Left Sidebar (Respond | Health):

- Health Status:** Healthy (18)
- Deployment Status:** Disposed (0), Concluded (✓)
- Search Filters:** Platform (AWS: 13, Data Center: 3, Azure: 2), Protection Level (Essentials: 14, Professional: 4), Deployment (AWS Production: 8, Deployment: 1, Ozone: 5, Production Data Center: 3, Development Azure Environment: 2).
- Note:** Select a deployment to view additional asset filters.

Red Box 1: Points to the "Deployment" section under "Ozone".

Middle Section (Networks List):

- View Options:** Networks (selected), Sort by Name (dropdown with up/down arrows), search bar, magnifying glass icon.
- Configuration List:**
 - alb-ent-backup (Development Azure Environment | 10.2.0.0/16) - View
 - AlbertEnterprises-vnet (Development Azure Environment | 10.0.0.0/16) - View
 - AN_VPC (Ozone | 10.0.0.0/16) - View
 - DR (Production Data Center | 172.1.0.0/24) - View
 - Legacy (Ozone | 10.0.0.0/16) - View
 - Peered VPC (AWS Production Deployment | 10.0.0.0/16) - View

Asset Groups and Health

The screenshot shows the Alert Logic platform interface with the following highlights:

- 1**: A red box surrounds the "Deployment" dropdown menu, which is set to "Ozone".
- 2**: A red box surrounds the "Asset Group" dropdown menu, which lists "JP Test" and "Info Dev Test", both with a count of 5.
- 3**: A red box surrounds the list of VPC assets, which includes:
 - 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)

Alert Logic logo is visible in the bottom left corner.

Getting Started from the Dashboard (Playbook)

The screenshot shows the Alert Logic dashboard interface. On the left, a sidebar menu is open under the 'Dashboards' section, showing options like Respond, Incidents, Exposures, Health, and Automated Response (which is highlighted with a red box). The main dashboard area displays several cards:

- Open CVE Count:** 0
- Open Remediations:** 211
- Vulnerability Trend by Severity:** A line chart showing the count of vulnerabilities over time across four severity levels: High (red), Medium (orange), Low (yellow), and Info (grey).
- Vulnerabilities by Deployment:** A chart showing the count of vulnerabilities across different deployment environments.
- Top Remediations by Impacted Assets:** A table listing remediations and their asset counts.

At the bottom left, there's a 'Support' link with a question mark icon. The top right corner shows user information: John Pirc, Web App Security I..., and US-EAST-1 (US).

Name	Asset Count
Determine if privileged access is needed.	138

Defining the Playbook

The screenshot shows the Splunk interface for managing Playbooks. The top navigation bar includes the Splunk logo, user name 'John Pirc', and environment 'Web App Security I... | US-EAST-1 (US)'. The left sidebar has sections for 'search filters', 'Playbook Type' (Incidents selected), and 'Playbook Status' (Active selected). The main area has tabs for 'Playbooks' (selected), 'Playbook History', and 'Inquiries'. A large orange button with a '+' icon and the text 'Add a Playbook' is centered. Below it is a table listing existing Playbooks:

Playbook Name	Edit	Inquiries	History	Delete
Automated Response SKO Demo (Do Not Delete)				
Beta Day (Informational Playbook)				
Carl Inquiry Verification				
Carl Push Approval Test				
Channels test				
Colson				

A red arrow points from a callout box containing the text 'Click here to get started' to the 'Add a Playbook' button.

Defining the Playbook (cont)

The screenshot shows a software interface for defining a new playbook. On the left, there's a sidebar with a logo, the text "Respond | Playbooks", and a "Add a Playbook" button. The main area is a modal window titled "Add a Playbook". Inside, there are four tabs: "Details" (which is selected and highlighted with a red box), "Input", "Variables", and "Result". Step 1, "Details", contains instructions: "Provide information about your playbook and the criteria for carrying it out". Step 2, "Name", has a field with the value "Beta Day (Informational Playbook)" which is also highlighted with a red box. Step 3, "Description", has a field with the value "Demo" which is also highlighted with a red box. At the bottom of the "Details" section is a toggle switch labeled "Playbook is Active ?" which is turned on. In the top right corner of the modal, there are "CANCEL" and "OK" buttons.

Add a Playbook

1 Details

Provide information about your playbook and the criteria for carrying it out

Name *

2 Beta Day (Informational Playbook)

Description *

3 Demo

Playbook is Active ?

CANCEL OK

Defining the Playbook (cont)

The screenshot shows the Alert Logic interface with a modal dialog titled "Add a Playbook". The dialog has four tabs: "Details" (disabled), "Input" (selected and highlighted with a red box), "Variables", and "Result". The "Input" tab contains a list of parameters:

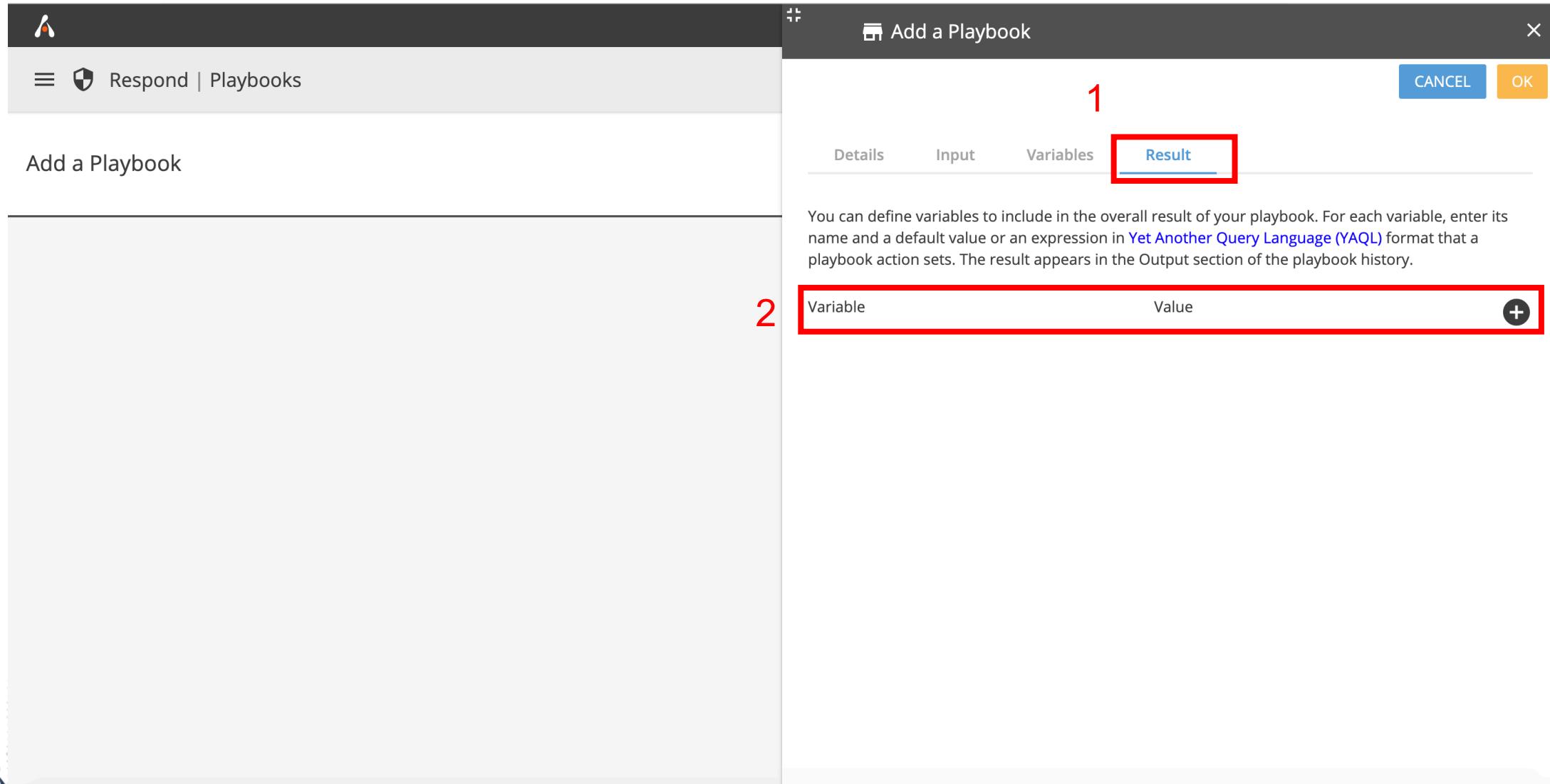
- account_id: Alert Logic MDR Account ID
- payload_type: Alert Logic MDR Payload Type
- payload: Alert Logic MDR Payload Object

A red box highlights the "Input" tab and the list of parameters. A red number "1" is positioned above the "Input" tab, and a red number "2" is positioned next to the list of parameters.

Defining the Playbook (cont)

The screenshot shows a software interface for defining a playbook. On the left, there's a sidebar with a logo and the text "Respond | Playbooks". The main area is a dialog box titled "Add a Playbook". Inside the dialog, there are four tabs at the top: "Details", "Input", "Variables", and "Result". The "Variables" tab is highlighted with a red border. Below the tabs, a message reads: "This list contains the variables available for use in this playbook and their descriptions." At the bottom right of the dialog are two buttons: "CANCEL" and "OK".

Defining the Playbook (cont)



The screenshot shows the 'Add a Playbook' dialog box from a software interface. The dialog has a dark header bar with the title 'Add a Playbook'. Below the header are four tabs: 'Details' (disabled), 'Input', 'Variables', and 'Result'. The 'Result' tab is highlighted with a red border and has a red number '1' above it. To the right of the tabs are 'CANCEL' and 'OK' buttons. The main content area contains a descriptive text about defining variables for the result. A red number '2' is placed next to the first row of a table below this text, which is also outlined in red.

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)

The screenshot shows the Alert Logic Respond interface for defining a Playbook. The top navigation bar includes the Alert Logic logo, user name "John Pirc", dropdown menus for "Web App Security I..." and "US-EAST-1 (US)", and links for "VALIDATE", "TEST", "CANCEL", and a large orange "SAVE" button.

The main workspace is titled "Beta Day (Informational Playbook)" under the "Demo" category. It features a "Playbook Context" section with a house icon and a counter "1". A red box highlights the "+" button next to the counter, with a red arrow pointing from the text "Creating a Task" below it to this button.

Defining the Playbook (cont)

The screenshot shows the AIOps Platform interface for defining a playbook. At the top, the navigation bar includes the AIOps logo, user name 'John Pirc', project 'Web App Security I...', location 'US-EAST-1 (US)', and a search bar. Below the navigation is a secondary header with a shield icon and the text 'Respond | Playbooks'. The main content area is titled 'Beta Day (Informational Playbook)' and has a 'Demo' status indicator. On the right, there are buttons for 'VALIDATE', 'TEST', 'CANCEL', and a large orange 'SAVE' button. The central part of the screen displays a 'Playbook Context' modal with a red number '1' above its title bar. Inside the modal, a red box highlights a dropdown menu titled 'Add task:' with a search bar. The dropdown lists several task options, each preceded by a small icon: 'Alert Logic: Execute Alert Logic SDK Action', 'Alert Logic: Call Connector', 'Microsoft: Post incident to Microsoft Teams connector', 'Slack: Post incident to Slack connector', 'ServiceNow: Create ServiceNow incident', and 'Alert Logic: Add Incident Feedback'. A red arrow points from a callout bubble on the right towards the 'Add task:' dropdown. The callout bubble contains the text: 'We currently have 26 tasks and we are going to select Email Approval Request'.

Playbook Context

Add task:

Search

1

- Alert Logic: Execute Alert Logic SDK Action
- Alert Logic: Call Connector
- Microsoft: Post incident to Microsoft Teams connector
- Slack: Post incident to Slack connector
- ServiceNow: Create ServiceNow incident
- Alert Logic: Add Incident Feedback

We currently have 26 tasks and we are going to select Email Approval Request

Defining the Playbook (cont)

The screenshot shows the Alert Logic interface with the following details:

- Left Sidebar:** Shows a navigation menu with "Respond | Playbooks" selected.
- Central Area:** A "Playbook Context" section is visible, with a task entry for "Alert Logic send_approval_email0".
- Right Panel:** A modal window titled "send_approval_email0" is open, divided into tabs: Task (highlighted with a red box), Request, Response, and Publish.
- Task Details Section:** Contains fields for Name (set to "send_approval_email0"), Action (set to "send_approval_email"), Description (set to "Request an approval via an email"), and a checkbox for "Repeat this action".
- Buttons:** The modal has "CANCEL" and "OK" buttons in the bottom right corner.

Defining the Playbook (cont)

The screenshot shows the Alert Logic Playbook editor interface. At the top, there's a navigation bar with the Alert Logic logo, user name "John Pirc", location "Web App Security I...", and region "US-EAST-1 (US)". Below the navigation is a header bar with a shield icon and the text "Respond | Automated Response". The main area is titled "incident Beta Day (Informational Playbook) Demo". On the right, there are buttons for "VALIDATE", "TEST", "CANCEL", and "SAVE" (in an orange box). The central part of the screen displays a workflow step. It starts with a "Playbook Context" step, followed by an "Alert Logic" step labeled "send_approval_email0". This step has three icons below it: a red-bordered square with the number "1", a question mark in a circle, and a downward arrow. A red arrow points from a box labeled "Creating a Condition" to the red-bordered square icon.

Playbook Context

Alert Logic
send_approval_email0

1 ? ↴

Creating a Condition

Defining the Playbook (cont)

The screenshot shows the Alert Logic Playbook Editor interface. On the left, a sidebar displays 'Respond | Playbooks' and a 'Playbook Context' section. A central workspace contains a 'Condition' block labeled '<% succeeded() %>' and an 'Alert Logic' block labeled 'send_approval_email'. A red box labeled '1' highlights the 'user_ids' input field in the 'send_approval_email' block, which currently contains 'John Pirc (john.pirc@alertlogic.com)'. A red box labeled '2' highlights the 'subject' input field, which is empty. A red box labeled '3a' highlights the 'message' input field, which contains the text 'This IP <% ctx().payload.attacker_ip%> is bad'. A red box labeled '3b' highlights the 'VARIABLES' dropdown menu in the 'message' field.

ALERT LOGIC

Respond | Playbooks

Playbook Context

Condition
<% succeeded() %>

Alert Logic
send_approval_email

send_approval_email0

VARIABLES

account_id *
<% ctx().account_id %>

user_ids 1

Select All

John Pirc (john.pirc@alertlogic.com)

Custom subject to use in the email. If not specified, the default is used.

subject 2

message 3a

This IP <% ctx().payload.attacker_ip%> is bad

VARIABLES 3b

VARIABLES

CANCEL OK

49

Defining the Playbook (cont)

The screenshot shows the Alert Logic interface for defining a playbook. The main window title is "send_approval_email0". Below the title, there are four tabs: "Task", "Request", "Response", and "Publish". The "Response" tab is highlighted with a red box and is currently active. A red arrow points from a red box labeled "TBA" to the "Response" tab. In the background, there is a sidebar titled "Playbook Context" and a list of playbooks, with one named "Alert Logic send_approval_email" visible.

Defining the Playbook (cont)

The screenshot shows the Alert Logic interface with the following details:

- Left Sidebar:** Shows a navigation menu with "Respond | Playbooks" selected. Below it are "Playbook Context" and "Alert Logic send_approval_email0".
- Right Panel:** A modal window titled "send_approval_email0" with tabs for Task, Request, Response, and Publish. The "Publish" tab is highlighted with a red border.
- Conditions Section:** Contains fields for "Name" (with a "VARIABLES" dropdown) and "If".
- Do Section:** Contains a "List of items to publish" table with columns for "Key" and "Value".
- Buttons:** "CANCEL" and "OK" buttons at the top right of the modal.

A red arrow points from the word "TBA" in the "Name" field to the "Publish" tab, indicating where the value should be entered.

Defining the Playbook (cont)

The screenshot shows the Alert Logic Playbook Context interface. On the left, a sidebar lists "Playbook Context" and "Alert Logic send_approval_email". A central dialog box displays a condition: "Condition <% succeeded() %>". To the right, a larger configuration dialog is open, titled "? <% succeeded() %>".

Configuration Dialog:

- Conditions:** A section labeled "Conditions" contains a single entry: "Name: Rejected" (marked with red box 1).
- If:** A section labeled "If" contains the expression "<% failed() %>" (marked with red box 2).
- Do:** A section labeled "Do:" contains the action "Fail" (marked with red box 2).
- Variables:** A dropdown menu labeled "VARIABLES" is shown (marked with red box 2).
- Search:** A search bar with placeholder text "Search" and a magnifying glass icon.
- Task default status:** Options "Success" and "Fail" are listed, with "Fail" selected (marked with red box 2).
- Playbook Inputs:** A list of variables:
 - account_id
 - payload_type
 - payload
 - payload_accountId
 - payload_asset_deployment_type
 - payload_asset_host_name
 - payload_asset_native_account_id

Defining the Playbook (cont)

The screenshot shows the Alert Logic Respond interface for defining a playbook. On the left, a sidebar lists "Playbook Context" and "Alert Logic send_approval_email". In the center, a condition block is selected, displaying the condition "`<% succeeded() %>`". A modal window titled "`<% succeeded() %>`" is open, showing the configuration for this condition. The modal has three numbered steps:

- 1**: The condition name "Approved" is highlighted with a red box.
- 2**: The "VARIABLES" dropdown menu is highlighted with a red box.
- 3**: The "Do:" section, which contains the condition expression "`<% succeeded() %>`", is highlighted with a red box.

At the bottom right of the modal, there are "CANCEL" and "OK" buttons.

Defining the Playbook (cont)

The screenshot shows the Alert Logic Respond interface for defining a playbook. The main window title is "incident_add_feedback1". The navigation bar includes "Respond | Playbooks" and tabs for "Task" (which is selected and highlighted with a red box), "Request", "Response", and "Publish". A "Playbook Context" icon is also present. In the foreground, a modal dialog titled "Condition Approved" is open, showing a condition step with a question mark icon and the text "Approved". Below the main window, there is a list of logic steps: "Playbook Context", "Alert Logic send_approval_email", and another "Condition Approved" step. The "Task Details" section contains the following information:

- Name: incident_add_feedback1
- Action: incident_add_feedback
- Description: Add a feedback note to an existing incident.
- Repeat this action

Buttons for "CANCEL" and "OK" are located in the top right corner of the main window.

Defining the Playbook (cont)

The screenshot shows the Splunk Playbook Editor interface. On the left, there's a sidebar with a navigation bar labeled "Respond | Playbooks". Below it are two cards: "Playbook Context" and "Alert Logic send_approval_email". A "Condition Approved" card is currently selected, indicated by a grey background and a question mark icon. To the right of the sidebar, a detailed view of a playbook step is shown.

Playbook Step Details:

- Step Type:** Task
- Step Name:** incident_add_feedback1
- Buttons:** CANCEL (blue) and OK (orange) are visible in the top right.
- Request Tab:** This tab is highlighted with a red box and contains:
 - account_id *
<% ctx().account_id %>
 - incident_id *
<% ctx().payload.incidentId %>
 - customer_feedback *
We need more information on IP <% ctx().payload.attacker_lset.select(\$.ip)%>
 - customer_feedback_reason (1)
- Response Tab:** Contains a "further action" section with a dropdown menu:
 - further action
 - acceptable risk
 - compensating control
 - threat not valid
 - not concluded
 - other
- VARIABLES:** Three sections are labeled with red boxes:
 - 1: account_id
 - 2: incident_id
 - 3: customer_feedback
 - 4: customer_feedback_reason

Defining the Playbook (cont)

The screenshot shows the Alert Logic Respond | Playbooks interface. At the top, there's a navigation bar with a logo, the title "incident_complete2", and buttons for "CANCEL" and "OK". Below the navigation is a toolbar with icons for "Playbook Context", "Task" (which is highlighted with a red box), "Request", "Response", and "Publish".

The main area displays a workflow diagram:

- A "Playbook Context" block is at the top.
- An "Alert Logic" block labeled "send_approval_email" is connected below it.
- An arrow points from the "send_approval_email" block to a "Condition" block labeled "Approved".
- An arrow points from the "Approved" condition block to an "Alert Logic" block labeled "incident_complete2".

Below the diagram, there are several input fields and a checkbox:

- "Task Details:" section:
 - Name: incident_complete2
 - Action: incident_complete
 - Description: Close incident and provide reason for closing an incident.
 - Repeat this action
- At the bottom of the main area, there are three small circular icons with symbols: a plus sign, a question mark, and a downward arrow.

Defining the Playbook (cont)

The screenshot shows the Alert Logic Respond interface. On the left, a sidebar titled "Respond | Playbooks" lists "Playbook Context" and "Alert Logic send_approval_email". Below these, a condition "Approved" leads to an action "incident_complete2". A red box labeled "4" highlights the "incident_complete2" action. On the right, a detailed configuration dialog for "incident_complete2" is open. The dialog has tabs for "Task", "Request" (which is selected), "Response", and "Publish". The "Request" tab contains fields for "account_id" (with value <% ctx().account_id %>) and "incident_id" (with value <% ctx().payload.incidentId %>). The "Response" tab contains a "notes" field with the text "The following IP <% ctx().payload.attacker_ip %> is malicious and needs to be blocked". A red box labeled "3" highlights this notes field. The "Variables" section for the "Response" tab is shown below, with a red box labeled "2" highlighting it. The "Publish" tab is partially visible on the far right. At the bottom of the dialog, there are "VARIABLES" dropdowns, a "reason_code" field (highlighted by a red box labeled "4"), and a "further action" section with options: "acceptable risk", "compensating control", "threat not valid", "not concluded", and "other".

ALERT LOGIC

Validating a Playbook

John Pirc ▾ Web App Security I... ▾ | US-EAST-1 (US)

☰ 🛡 Respond | Playbooks

1

Beta Day (Informational Playbook)
Demo

VALIDATE TEST CANCEL SAVE

Playbook Context

Alert Logic send_approval_email0

Condition Approved Condition Rejected

Alert Logic incident_complete2 Alert Logic incident_add_feedback1

Playbook valid!!!

The screenshot shows the Alert Logic interface for validating a playbook. At the top, there's a navigation bar with user info (John Pirc), a dropdown for 'Web App Security I...', and a location indicator 'US-EAST-1 (US)'. Below that is a secondary navigation bar with 'Respond | Playbooks' and several action buttons: 'VALIDATE' (highlighted with a red box), 'TEST', 'CANCEL', and 'SAVE'. A large red box labeled '1' is positioned above the validate button. The main area displays a flowchart of the 'Beta Day (Informational Playbook)' with a demo status. The flow starts with 'Playbook Context', followed by 'Alert Logic send_approval_email0', which branches into two parallel paths: 'Condition Approved' leading to 'Alert Logic incident_complete2', and 'Condition Rejected' leading to 'Alert Logic incident_add_feedback1'. Each logic step has a delete icon ('X'). At the bottom, a prominent red box contains the message 'Playbook valid!!!'.

Testing a Playbook

≡ Test Playbook

CANCEL

RUN

1. Payload —— 2. Results

Incident Type

Incident

Incident Payload ⓘ

```
1  {
2    "accountId": 2,
3    "asset_deployment_type": "aws",
4    "asset_host_name": "10.1.2.3",
5    "asset_native_account_id": "2",
6    "assets": {},
7    "attacker": {
8      "account": "2",
9      "instanceId": "i-0a159b2a553285ebb",
10     "ip": "10.10.10.12",
11     "port": 40814,
12     "region": "us-east-2"
13   },
14   "attacker_country_code": "BR",
15   "attacker_country_name": "Brazil",
16   "attacker_lset": [
17     {
18       "ip": "86.34.222.99"
19     },
20     {
21       "value": "SomeAttacker"
22     }
23   ],
24   "closed_time": "2020-08-10T11:24:27.765796+00:00",
```



Setting a Playbook in Motion

The screenshot shows the Alert Logic web interface with the following details:

- Header:** John Pirc, Web App Security I..., US-EAST-1 (US)
- Sidebar (Manage):**
 - Alert Notifications (selected)
 - Respond
 - Investigate
 - Validate
 - Configure
 - Notifications** (highlighted with a red box)
 - Integrations
 - Users
 - Service Status
 - Escalation Preferences
 - Support
- Main Content:**
 - Alert Notifications:** Sub-section of Notifications.
 - Create a Notification:** A large orange button with a plus sign.
 - Incidents:** A table listing notifications.

Notification Type	Notification Name	Recipients	Action
Info	Darwin Test for info level notifications	2 Recipients	View
Info	High Incident Alert	2 Recipients	View
Info	Info Dev Test Incident Notification	1 Recipient	View
Info	Nancy's High Incident Alert	1 Recipient	View

Setting a Playbook in Motion (cont)

The screenshot shows the Alert Logic interface for managing notifications. On the left, there's a sidebar with filters for Active (0/6) and Inactive (0/7) notifications, search filters, and dropdowns for Type (Incidents), Account (Web App Security Integration), Subscribed User (Darwin d Garcia m, Kimberly Heintschel, Nancy Wang, Nancy Wang), and Subscribed Connector (ServiceNow Create Security Incident, Test webhook). The main area is titled 'Alert Notifications' and shows a list of notifications. A modal window titled 'Create a Notification' is open, showing options for '+ Add Notification' (Observation or Incident), sorting by name, and a search bar. The 'Incident' option is highlighted with a red box and an arrow points from it to a callout box labeled 'Select Incident'. The notification list includes:

- High Incident Alert (2 Recipients, View)
- Info Dev Test Incident Notification (1 Recipient, View)
- Nancy's High Incident Alert (View)
- Nancy's test (1 Recipient, View)

At the bottom, it says 'Most recent notification sent: Jan 26 2021 17:00:46 GMT-6'.

Setting a Playbook in Motion (cont)

! Create an Incident Notification

CANCEL

SAVE

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)

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) X

Email Subject

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

Setting a Playbook in Motion (cont)

Create an Incident Notification

CANCEL

SAVE

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

1 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

2 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

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) X

Email Subject

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

Select Medium

Setting a Playbook in Motion (cont)

Create an Incident Notification

CANCEL **SAVE**

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.

Filter(s)

Select All



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 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

CANCEL

SAVE

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

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}}`

Transferring this step to the Playbook

Relocation of (Threat Rating, Classification, Asset Groups, etc. to the Playbook)

ALERT LOGIC

Configuration | Automated Response

Incident Response

ServiceNow and AWS WAF Block

This is my playbook. there are many like it, but this one is mine.

```
graph TD; Start([Alert Logic Incident Generated]) --> Create[ServiceNow Create new Customer Service Case]; Create --> WAF[AWS WAF Block]; WAF --> IfSucceeded[Conditions If Succeeded]; WAF --> IfFailed[Conditions If Failed]; IfSucceeded --> Update[ServiceNow Update Customer Service Case]; Update --> Close([Alert Logic Close Incident]); IfFailed --> Notify([Alert Logic Send Notification]); Notify --> Close;
```

Incident Generated

Details Response

Name: Incident Generated

Action Description: When an Alert Logic Incident is generated.

Enable Playbook

This playbook will be executed:

Manually only

Automatically when an incident is generated matching the following criteria:

search

Threat Rating

Escalation

Classification

Detection Source

Asset Groups

Setting a Playbook in Motion (cont)

Manage | Notifications

Active 0/7 Inactive 0/7

Alert Notifications Schedules

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

Create a Notification

Group by Type Sort by Name search

Incidents

Beta Day (Demo) Most recent notification sent: No notifications sent.	1 Recipients	View
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

Subscribed User

- Darwin d Garcia m
- John Pirc
- Kimberly Heintschel
- Nancy Wang
- Nancy Wang

Subscribed Connector

- ServiceNow Create Security Incident
- Test webhook

Running an on-demand Playbook

A

John Pirc ▾ Web App Security I... ▾ | US-EAST-1 (US)

Dashboards

WHAT'S NEW

Incidents

Exposures

Health

Automated Response

Investigate

Validate

Configure

Manage

Support

Data for the last: 7d 14d 30d Custom range: 28 Dec 2020 - 27 Jan 2021

Open CVE Count 0 INVESTIGATE

Open Remediations 211 INVESTIGATE

Vulnerability Trend by Severity

Count of Vulnerabilities

1k
100
10

Dec 28 Dec 30 Jan 01 Jan 03 Jan 05 Jan 07 Jan 09 Jan 11 Jan 13 Jan 15 Jan 17 Jan 19 Jan 21 Jan 23 Jan 25 Jan 27

High Medium Low Info

Vulnerabilities by Deployment

1k

100

Top Remediations by Impacted Assets

Name	Asset Count
Determine if privileged access is needed.	138
Enable S3 Logging and Object	

68

Running an on-demand Playbook

John Pirc | Web App Security I... | US-EAST-1 (US)

UPDATED INCIDENTS EXPERIENCE | NOTIFICATIONS | HELP

Respond | Incidents

Classification

- application-attack 14.8k
- N/A 1

Show More...

Detection Source

- Web Log Analytics 14.8k
- N/A 1

Show More...

Correlation Name

- N/A 14.8k

Show More...

Deployments

Web App Security Integration

- WLA Integration Log Source 14.7k
- Manual Deployment 6
- Unknown 1

unknown

- WLA Integration Log Source 87

Show More...

Incident List

Last 30 Days

Choose Columns (12 of 13 Shown)

#	Date	ID	Summary	Threat	Class	Date	Correl	Incid	Depl	Acco	Attac	Target
1	26th Jan 2021 11:54:29 GMT-6	9sysx5	SQL Injection, Null Byte, Path Traversal Attempts from 7.33.6.77	Medium	application-attack	Web Log Analytics	0	0	WLA Integration Log Source	Web App Security Integration	7.33.6.77	suitablek id.com
	>		SQL Injection, Null Byte, Path Traversal Attempts from 7.33.6.77	Medium	application-attack	Web Log Analytics	0	0	WLA Integration Log Source	Web App Security Integration	35.6.0.4	suitablek id.com

Setting a Playbook in Motion (cont)

John Pirc | Web App Security I... | US-EAST-1 (US)

Respond | Incidents

UPDATED INCIDENTS EXPERIENCE NOTIFICATIONS HELP

2

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

OPEN IN IRIS UPDATE SNOOZE CLOSE PLAYBOOK

Investigation and Recommendation Evidence Search

Investigation Report

Audit Log Notification History

Audit Log

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

Topology

ALERT LOGIC

70

```
graph LR; Internet(( )) --- Cloud(( )); Cloud --- Application(( )); Application --- Computer(( )); Computer --- Network(( ));
```

Setting a Playbook in Motion (cont)

The screenshot shows the Alert Logic platform interface. On the left, an incident details page is displayed for an event ID: 9sysx5, titled "Web App Security Integration". The event type is "SQL Injection, Null Byte, Path Traversal Attempts from 7...." and it occurred on 26th Jan 2021 at 11:54:29 GMT-6. The severity is Medium. The "Investigation and Recommendation" tab is selected. On the right, a "Run playbook" modal is open, showing a dropdown menu for "playbook_id" with several options listed:

- Select --
- Add Note to Incident
- Austin Texas
- Automated Response SKO Demo (Do Not Delete)
- Beta Day (Informational Playbook)** (This option is highlighted with a red box)
- Carl Inquiry Verification

Red boxes are drawn around the following elements:

- The "Run playbook" button in the modal header.
- The "playbook_id" dropdown menu.
- The "Beta Day (Informational Playbook)" option in the dropdown list.

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....
Medium
26th Jan 2021 11:54:29 GMT-6

OPEN IN IRIS UPDATE SNOOZE CLOSE PLAYBOOK

Investigation and Recommendation Evidence Search 

Investigation Report  Audit Log Notification History

Audit Log

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

Topology



 72

Executing the Response Action (Email)

Alert Logic MDR Approval Request



Alert Logic Dev no-reply <no-reply@product.dev.alertlogic.com>

Today at 6:04 PM

To: Pirc, John

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

John Pirc | Web App Security I... | US-EAST-1 (US)

Respond | Incidents

UPDATED INCIDENTS EXPERIENCE NOTIFICATIONS HELP

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

OPEN IN IRIS UPDATED SNOOZE CLOSE PLAYBOOK

Investigation and Recommendation Evidence Search

Investigation Report

Topology

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

John Pirc | Web App Security I... | US-EAST-1 (US)

≡ Respond | Automated Response

search filters

Playbooks Playbook History Inquiries

Playbook

- SKO Simple Demo 519
- Test Multiple Email Recipients 8
- Automated Response SKO Demo (Do Not Delete) 5
- Add Note to Incident 4
- Channels test 4
- Mobile app push test 3
- Beta Day (Informational Playbook) 2
- Parallel Execution Example 1

Status

- succeeded 531
- failed 6
- requested 5
- running 4

Type

- incident 546

Playbook Execution History 25 Jan 2021 - 26 Jan 2021

Showing 5 columns of 5 Sort by Start Time Search

	Playbook	Start	End	Type	Status
▼	Beta Day (Informational Playbook)	Jan 26 2021 18:03:49 GMT-6	Jan 26 2021 18:06:50 GMT-6	incident	succeeded
▼	Add Note to Incident	Jan 26 2021 17:18:52 GMT-6	Jan 26 2021 17:18:54 GMT-6	incident	failed
▼	Add Note to Incident	Jan 26 2021 17:18:37 GMT-6	Jan 26 2021 17:18:38 GMT-6	incident	failed
▼	Add Note to Incident	Jan 26 2021 17:18:30 GMT-6	Jan 26 2021 17:18:32 GMT-6	incident	failed
▼	Add Note to Incident	Jan 26 2021 17:18:23 GMT-6	Jan 26 2021 17:18:24 GMT-6	incident	failed
▼	Channels test	Jan 26 2021 16:28:18 GMT-6	Jan 26 2021 16:28:36 GMT-6	incident	succeeded

Playbook History (cont)

John Pirc Web App Security I... | US-EAST-1 (US)

Respond | Automated Response

Playbook Execution History

25 Jan 2021 - 26 Jan 2021

Showing 5 columns of 5 ▾ Sort by Start Time ▾ Search

Playbook	Start	End	Type	Status
Beta Day (Informational Playbook)	Jan 26 2021 18:03:49 GMT-6	Jan 26 2021 18:06:50 GMT-6	incident	succeeded

1

2

3

4

Jan 26 2021 18:03:49 GMT-6

ID
70C757FE-B7EC-4E5E-8E91-148AFB043402

Playbook ID
60107e891365144aeafe666d

Status
succeeded

Type
incident

Start Time
Jan 26 2021 18:03:49 GMT-6

End Time
Jan 26 2021 18:06:50 GMT-6

Created By
John Pirc

Modified By
System

Input

```
{"account_id": "134264762", "payload": { "accountId": 134264762, "asset_deployment_type": "aws", "asset_host_name": "wla-us-east-1-int-linux-logs", "asset_native_account_id": "248216933490", "assets": { "asset": { "deployment": { }}}}}
```

Output

```
{"output": { "": "" }}
```

Playbook History (cont)

≡  Respond | Automated Response

Tasks

1

Name	Action	Status
send_approval_email0	send_approval_email	failed

Input

```
{  
  "account_id": "134264762",  
  "user_ids": [  
    "19BF396F-B848-4138-98B8-084CF995F028"  
  ],  
  "message": "This IP ['7.33.6.77'] is bad"  
}
```

Output

```
{  
  "output": null,  
  "errors": [  
    {  
      "type": "error",  
      "message": "Execution failed. See result for details.",  
      "task_id": "fail"  
    }  
  ]  
}
```

Inquiries (Pending Playbooks)

John Pirc | Web App Security I... | US-EAST-1 (US)

≡ ⚡ Respond | Automated Response

search filters 

Display name	Count
Email Approval Request	10
Channels Approval Request	3
Push Approval Request	3

Status	Count
pending	9
succeeded	7

Playbook	Count
Test Multiple Email Recipients	8
Channels test	3
Mobile app push test	3
Automated Response SKO Demo (Do Not Delete)	1
Beta Day (Informational Playbook)	1

Type	Count
email	10
channels	3

Playbooks Playback History **Inquiries**

 Inquiries 25 Jan 2021 - 26 Jan 2021  

Showing 4 columns of 4 Sort by Start Time  

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

 **send_approval_channels**
Channels test

ID
4B3D264B-7EC9-499D-91BC-6C048311C5
43

Status
succeeded

Task Name
send_approval_channels0

Type
channels

Start Time
Jan 26 2021 16:27:21 GMT-6

End Time
Jan 26 2021 16:27:52 GMT-6

Inquiries (Pending Playbooks)

A

John Pirc | Web App Security I... | US-EAST-1 (US)

≡ Respond | Automated Response

Demo (Do Not Delete)

Beta Day (Informational Playbook) 1

Type email 10
 channels 3
 mobile 3

Task name send_approval_email0 9
 send_approval_channels0 3
 send_approval_push0 3
 RequestBlockApproval 1

Channels test pending Jan 26 2021 16:23:12 GMT-6

ID 86277819-CBE6-4696-8436-258DA749B3D5 Name send_approval_channels

Playbook Channels test Playbook Description test

Status pending Type channels

Task name send_approval_channels0 Start at Jan 26 2021 16:23:12 GMT-6

Logs

1 2 3

PLAYBOOK RESPOND EXECUTION

Test Multiple Email Recipients succeeded Jan 25 2021 14:14:00 GMT-6 Jan 25 2021 14:15:11 GMT-6

Automated Response SKO Demo (Do Not Delete) pending Jan 25 2021 13:44:54 GMT-6

Test Multiple Email Recipients succeeded Jan 25 2021 13:09:26 GMT-6 Jan 25 2021 13:09:59 GMT-6

Test Multiple Email Recipients succeeded Jan 25 2021 12:48:41 Jan 25 2021 12:49:17

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

≡ Respond | Automated Response

incident
Demo Playbook (Block IP on AWS WAF) Template
Demo Playbook

VALIDATE TEST CANCEL SAVE

```
graph TD; A[Playbook Context] --> B[ServiceNow CreateServiceNowIncident]; B --> C[built-in log_snow_id]; C --> D[Alert Logic RequestBlockApproval]; D --> E{Condition If approved}; D --> F{Condition If rejected}; E --> G[AWS BlockIP_RegionalWAF]; F --> H[Alert Logic UpdateIncident]; G --> I{Condition On Success}; I --> J[Alert Logic CloseIncident];
```

The workflow starts with "Playbook Context", followed by "ServiceNow CreateServiceNowIncident", "built-in log_snow_id", and "Alert Logic RequestBlockApproval". This is followed by two parallel paths: "Condition If approved" leading to "AWS BlockIP_RegionalWAF", and "Condition If rejected" leading to "Alert Logic UpdateIncident". Finally, it leads to "Condition On Success" and "Alert Logic CloseIncident".

Complex Workflow

