



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

Built for the Cloud

Context

Define application environments and associated risks.

Focus efforts on most critical environments first

Measure progress

X

Automation

Automate response to routine incidents

=

Adaptive Security

Disrupt kill chain early

Bring work in balance with resources

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

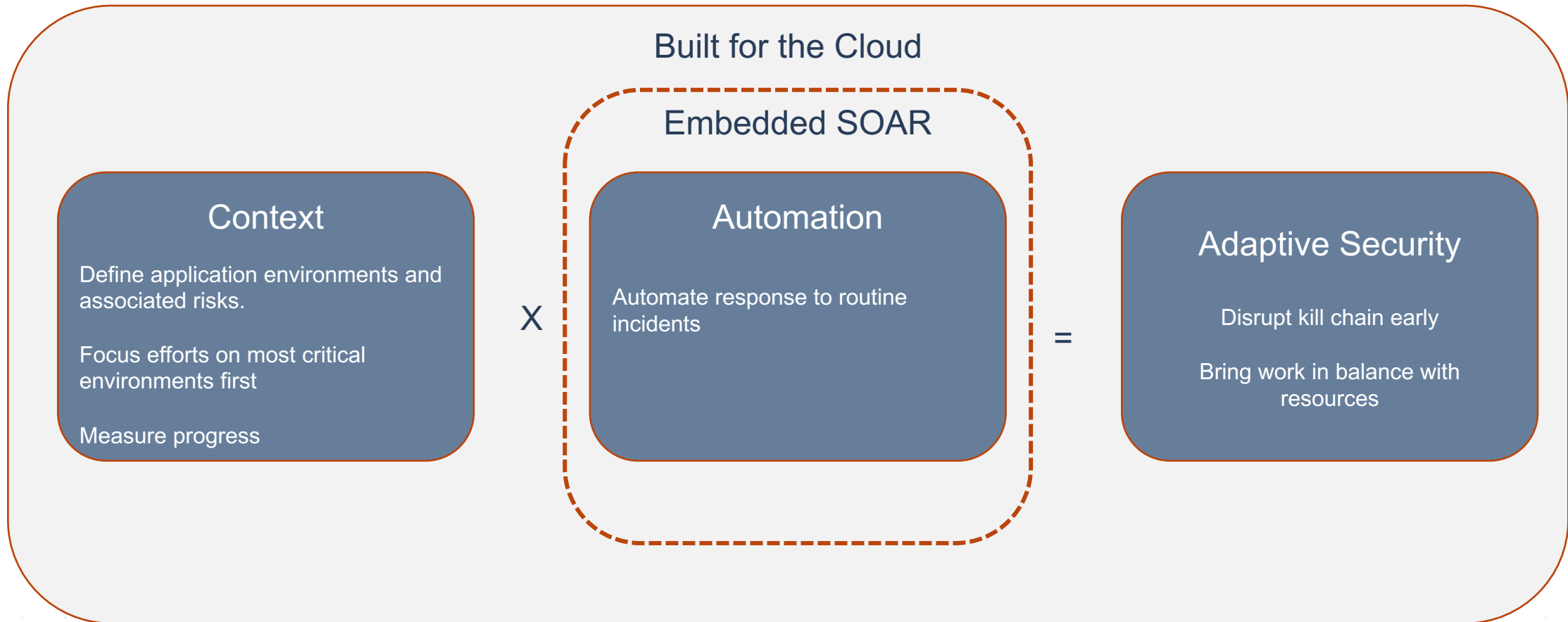
- Is Joe's laptop compromised or is it the CFO's?
- Is it the T-shirt giveaway registration app or the e-commerce system?
- Is it a service that has access to PHI? Cardholder data?

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



Incident

Summary Guidance Audit Log

Description: Possible Successful Apache Struts Multipart exploit attempt against 172.31.37.90

Severity: Critical

Account: Albert Enterprises

Date / Time: January 19, 2021 09:58:01 CST

Attack Summary: Possible remote code execution attempt was detected from Any. This attack is possible due to a vulnerability in Struts 2 caused by improper sanitization during OGNL expression evaluation. It is strongly recommended to update to a non-vulnerable version of the Struts2-Core library.

References: [SANS Apache Struts Multipart Vulnerability](#)

Call SOC

Share Incident

Notification Centre

ALERT LOGIC

You've got new inquiry request

Please open the App to respond to it

Inquiry Details

Account: Web App Security Integration (134264762)

Playbook Name: Demo Playbook (Block IP on AWS WAF) Template

Playbook Description: Demo Playbook

Inquiry ID: 107D8798-3965-43B6-87FE-F26B4B78B0F7

Inquiry Name: Push Approval Request

Inquiry Description: Request an approval via an push notification

Inquiry Status: pending

Start Time: 23 January 2021 16:26:21 GMT

Type: mobile

Approve

Reject

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

Name				
990023346368	16	18	55	0
ca-central-1	1	3	0	0
vpc-dc155db4		3	0	
subnet-48cb4132				
subnet-9feafec3				
subnet-ce552ba6				
ap-northeast-2	1	4	0	0
vpc-0f64be64		4	0	
eu-north-1	1	3	0	0
us-west-2	1	5	0	0
us-east-2	1	3	0	0
eu-west-3	1	3	0	0

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

CANCEL

UPDATE



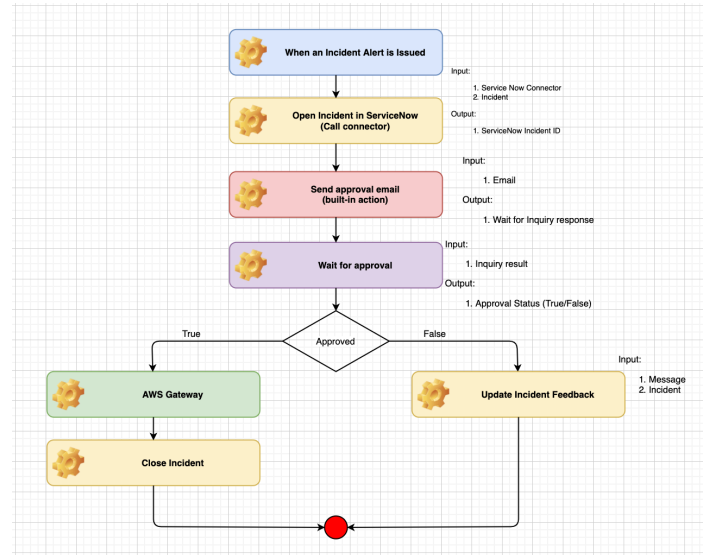
Demo

About the Beta Environment

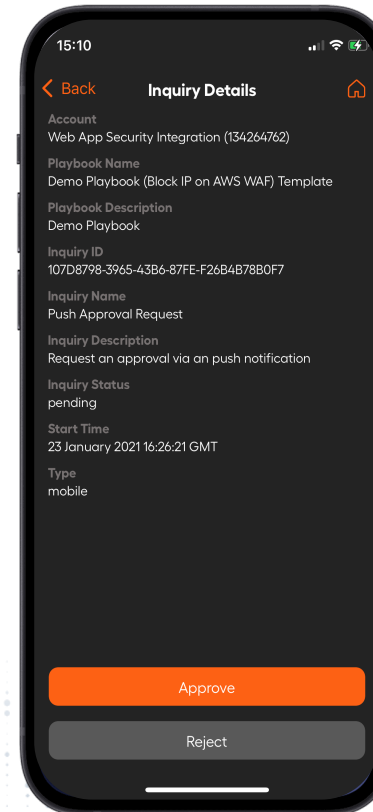
Platform



Playbook



Approval



Outcomes

Block Attacker

Disable User Account



Threat Intel Center

Threat Intel Center (Getting Started)

The screenshot displays the AWS Threat Intel Center dashboard. At the top, the user is identified as Malcolm Palmer, with the context 'Web App Security L...' and 'US-EAST-1 (US)'. The dashboard includes a navigation menu on the left with 'Threat Intel Center' highlighted in red. The main content area features several key metrics and charts:

- Count:** A large '0' representing the total count of items.
- Open CVE Count:** A large '211' representing the number of open CVEs.
- Vulnerability Trend by Severity:** A line chart showing the count of vulnerabilities over time, categorized by severity: High (red), Medium (orange), Low (yellow), and Info (grey).
- Vulnerabilities by Deployment:** A stacked bar chart showing the distribution of vulnerabilities across different deployment environments, categorized by severity.
- Top Security Remediations by Impacted Assets:** A table listing the most common remediations and the number of assets affected.

At the bottom of the dashboard, there is a 'Support' link and an 'EXPORT TO CSV' button.

Threat Intel Center Landing Page

Investigate | Threat Intelligence Center

Analytics 1.1k

Analytics

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

Choose Columns (4 of 15 Shown)

search

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.kstatd 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

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 Logo, Windows System Security Access Granted, Windows User Account Changed

Signatures
None

Customize Table

Malcolm Palmer | Web App Security L... | US-EAST-1 (US)

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

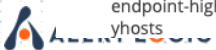
Choose Columns (4 of 15 Shown)

- []
- Logs
- Name
- Recommendations
- Response Actions

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
app/cve2000800 CVE-2000-0800 Linux rpc.kstatd 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
app/eternalblue_success ETERNALBLUE srvnet.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

Alert Logic | Investigate | Threat Intelligence Center

Malcolm Palmer | Web App Security I... | US-EAST-1 (US)

Analytics 1.1k

search filters

CLEAR ALL FILTERS X

Threat Level

Critical 13

Telemetry

Log 7

IDS 6

Response Actions

Block 13

Threat Classification

None 13

Analytics

Choose Columns (4 of 15 Shown)

search

Name	Summary	Threat Level	Telemetry
> successful_sql/sql_success	Successful SQL Injection from 1.2.3.4	Critical	IDS
> successful_sql/sql_error	Possible Successful SQL Injection from 1.2.3.4	Critical	Log
> successful_sql/roamer_php_webshell_success	Successful Roamer PHP Web Shell Access By 1.2.3.4	Critical	IDS
> successful_sql/cve20157857s	Possible Successful CVE-2015-7857 SQL Injection attempt from 1.2.3.4	Critical	IDS
> successful_sql/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

successful_sql/apache_struts_scan_success

Summary
Successful Apache Struts CVE-2013-2251 scan from 1.2.3.4

Threat Level
Critical

Telemetry
IDS

Technology
NGX

Visibility
Incident

Log Source
None

Logs
Not Applicable

Signatures
1102154,1102167,1102179

Search Analytics List

Malcolm Palmer | Web App Security I... | US-EAST-1 (US)

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_svc_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 XMRig 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



Metasploit PowerShell backdoor installation detected on ['ip_adre...']

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

NGX

Telemetry

Log

Log Source

Log

Log Message Types

Windows PowerShell Engine State Changed

Signatures

None

CVE

CWE

Threat Classification

None

Response Actions

Quarantine

Response Action Parameters

victim

Asset Groups

Asset Groups (Getting Started)

The screenshot displays the Alert Logic dashboard interface. At the top right, the user is identified as John Pirc, with the role 'Web App Security I...' and the region 'US-EAST-1 (US)'. The main navigation menu on the left includes 'Dashboards', 'Respond', 'Investigate', 'Validate', 'Configure', 'Deployments', 'Log Management', 'Application Registry', 'Certificates and Keys', 'WAF', 'PCI Scanning', 'Connectors', 'Asset Groups' (highlighted with a red box), 'Manage', and 'Support'. The dashboard content is organized into several panels. The top row features 'Open CVE Count' (0) and 'Open Remediations' (211), both with 'INVESTIGATE' buttons. To the right is a 'Vulnerability Trend by Severity' line chart showing counts for High, Medium, Low, and Info vulnerabilities from Dec 27 to Jan 26. The bottom row includes 'Vulnerabilities by Deployment' (partially visible) and a 'Top Remediations by Impacted Assets' table.

Name	Asset Count
Determine if privileged access is needed.	138

Asset Groups Landing Page



☰ ⚙️ Configure | Asset Groups



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.

search



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

Adding an Asset Group

The screenshot shows a web application interface for managing asset groups. At the top, there is a dark navigation bar with a logo on the left and user information on the right: "John Pirc", "Web App Security I...", and "US-EAST-1 (US)". Below this is a light gray header with a hamburger menu icon, a gear icon, and the text "Configure | Asset Groups".

The main content area features a prominent orange circular button with a white plus sign and the text "Add an Asset Group". Below this button is a dropdown menu with two options: "Asset Group" (highlighted with a red box) and "Linked Asset Group".

Below the dropdown is a search bar with the placeholder text "search" and a magnifying glass icon.

The section titled "Asset Groups" contains a table with three rows of 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

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

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.)

2

Description *
Assets in Scope

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
> 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



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



1

Name					
▼ AWS Fargate Demo	✓	18	65	202	73
> sa-east-1	✓		1	3	0
> eu-west-2	✓		1	3	0
> ca-central-1	✓		1	4	0
> eu-north-1	✓		1	3	0
> ap-southeast-2	✓		1	3	0
> ap-east-1	✓		1	3	0
▼ us-west-2		11	70	16	

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 ×

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



2

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

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 ×

1 Details — 2 Configuration







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

Assets

Tags

<> Expression

Search

 user arn:aws:iam::248216933490:user/wsm-jenkins	<p>Select a tag in the list</p> <p>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>
 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/vpc-	

CANCEL

UPDATE



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

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](#)

1

<> Expression

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

2

CANCEL

UPDATE

Creating Linked Asset Groups

The screenshot shows the Alert Logic interface for managing Asset Groups. At the top, there is a navigation bar with the user name 'John Pirc', the current project 'Web App Security I...', and the region 'US-EAST-1 (US)'. Below this is a secondary navigation bar with a menu icon and the text 'Configure | Asset Groups'. The main content area features a large orange button with a plus sign and the text 'Add an Asset Group'. A dropdown menu is open below this button, showing two options: 'Asset Group' and 'Linked Asset Group'. The 'Linked Asset Group' option is highlighted with a red rectangular box. Below the dropdown, there is a search bar with the placeholder text 'search' and a magnifying glass icon. The main section is titled 'Asset Groups' and contains a table of existing asset groups. The table has four rows, each representing an asset group with its name, last updated date, number of assets, and a 'View' or 'Hide' action.

Description	Criticality Rating
Rob's Things Last Updated: 20 Jan 2021	478 Assets View
Matt's 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 Hide

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

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.)

2

Description *
Critical Assets in Scope

CANCEL

SAVE AND CONTINUE

Creating Linked Asset Groups (cont)

Add a Linked Asset Group



1 Details — 2 Configuration

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

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 interface. At the top, there is a dark header with the user name 'John Pirc', the role 'Web App Security I...', and the region 'US-EAST-1 (US)'. Below the header is a navigation bar with a menu icon, a gear icon, and the text 'Configure | Asset Groups'. A search bar is located on the right side of the main content area. The main content is divided into two sections: 'Asset Groups' and 'Linked Asset Groups'. The 'Asset Groups' section contains a table with four rows: 'Robs Things' (478 Assets, last updated 20 Jan 2021), 'Matts Hosts' (2 Assets, last updated 29 Dec 2020), 'Asset Group Demo' (1566 Assets, last updated 20 Jan 2021), and 'PCI' (2 Assets, last updated 26 Jan 2021). The 'Linked Asset Groups' section contains one row: 'Compliance' (2 Groups, last updated 26 Jan 2021), which is highlighted with a red border.

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

Linked Asset Group	Groups	Last Updated	View
Compliance	2	26 Jan 2021	View

Asset Groups and Exposures

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

Respond | Exposures HELP

Category	Count	Item	Affected Assets	Exposure Instances	Open	View
Security	2.5k	<input type="checkbox"/> Determine if privileged access is needed.	44	114	>	▼
IAM Access Analyzer	94	● 114 ● 0 ○ 0 ⓘ 0 TRI 400.35				
External	41	IAM Access Analyzer, Security				
Deployment		<input type="checkbox"/> Review the IAM Access Analyzer findings for this account.	94	94	>	▼
AWS Production Deployment	1.4k	● 94 ● 0 ○ 0 ⓘ 0 TRI 343.57				
Fargate Demo	430	Security				
Ozone	409	<input type="checkbox"/> Restrict access to/from non-required IP addresses	38	49	>	▼
Development Azure Environment	299	● 40 ● 6 ○ 0 ⓘ 3 TRI 332.58				
Production Data Center	12	Security				
Training-Lab-Test	7	<input type="checkbox"/> Upgrade OpenBSD OpenSSH to version 8.3.0	22	205	>	▼
		● 29 ● 155 ○ 21 ⓘ 0 TRI 318.99				
Platform		Security				
AWS	2.2k	<input type="checkbox"/> Upgrade Apache Http_server to version 2.4.44	7	188	>	▼
Azure	299	● 7 ● 170 ○ 11 ⓘ 0 TRI 281.03				
Data Center	19	Security				
Asset Group		<input type="checkbox"/> Enable log metric filters and alarms.	3	84	>	▼
JP Test	398	● 0 ● 84 ○ 0 ⓘ 0 TRI 211.30				
AWS Production Web Servers	75	Security				
		<input type="checkbox"/> Apply non-default NACLs to all VPC subnets	15	15	>	▼
		● 15 ● 0 ○ 0 ⓘ 0 TRI 120.00				
		Security				
			73	73	>	▼

Select a deployment to view additional asset filters.

Asset Groups and Exposures

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

Respond | Exposures

HELP

Severity	Count	Assets	Instances	Open	View	
High	170	94	0	0	0	TRI 343.57
Medium	156	34	0	0	0	TRI 119.40
Low	31	0	28	0	0	TRI 70.43
Info	41	8	3	0	1	TRI 70.29

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.

Category	Assets	Instances	Open	View
Security	10	34	>	∨
Determine if privileged access is needed.	Affected Assets	Exposure Instances	Open	View
Security	1	28	>	∨
Enable log metric filters and alarms.	Affected Assets	Exposure Instances	Open	View
Security	8	12	>	∨
Restrict access to/from non-required IP addresses	Affected Assets	Exposure Instances	Open	View
Security	10	20	>	∨
Add traffic restrictions to default security group	Affected Assets	Exposure Instances	Open	View
Security	1	16	>	∨
Upgrade OpenBSD OpenSSH to version 8.3.0	Affected Assets	Exposure Instances	Open	View
Security	1	18	>	∨
Upgrade Php to version 7.3.21	Affected Assets	Exposure Instances	Open	View
Security	4	4	>	∨
Use AWS SSL security policy for ELB	Affected Assets	Exposure Instances	Open	View

Asset Groups and Health

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

Respond | Health

Healthy 18

Disposed

Concluded

search filters

Platform

- AWS 13
- Data Center 3
- Azure 2

Protection Level

- Essentials 14
- Professional 4

1 Deployment

- AWS Production Deployment 8
- Ozone 5
- Production Data Center 3
- Development Azure Environment 2

Select a deployment to view additional asset filters.

View Networks

Sort by Name

search

Configuration	alb-ent-backup	View
Development Azure Environment 10.2.0.0/16		
Configuration	AlbertEnterprises-vnet	View
Development Azure Environment 10.0.0.0/16		
AN_VPC	View	
Ozone 10.0.0.0/16		
DR	View	
Production Data Center 172.1.0.0/24		
Legacy	View	
Ozone 10.0.0.0/16		
Peered VPC	View	
AWS Production Deployment 10.0.0.0/16		

Asset Groups and Health

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

Respond | Health 3

SEARCH FILTERS

CLEAR ALL FILTERS x

Platform AWS 5

Tag
Name: Test VPC 1
Name: TST_VPC 1
Name: Legacy 1
Name: AN_VPC 1

Region
US West (Oregon) 4
Asia Pacific (Mumbai) 1

1 Protection Level Essentials 5

2 Asset Group JP Test 5
Info Dev Test 5

3

<input checked="" type="checkbox"/>	AN_VPC Ozone 10.0.0.0/16	View
<input checked="" type="checkbox"/>	Legacy Ozone 10.0.0.0/16	View
<input checked="" type="checkbox"/>	Test VPC Ozone 10.0.0.0/16	View
<input checked="" type="checkbox"/>	TST_VPC Ozone 10.0.0.0/16	View
<input checked="" type="checkbox"/>	vpc-7718f91e Ozone 172.31.0.0/16	View

Getting Started from the Dashboard (Playbook)

The screenshot displays the Alert Logic dashboard interface. At the top right, the user is identified as John Pirc, with the context 'Web App Security I...' and 'US-EAST-1 (US)'. The main navigation bar includes 'Dashboards' and 'WHAT'S NEW'. A left-hand navigation menu is open, with 'Automated Response' highlighted in a red box. The dashboard content area features several widgets: 'Open CVE Count' showing 0, 'Open Remediations' showing 211, and 'Vulnerability Trend by Severity' which is a line chart showing counts for High, Medium, Low, and Info vulnerabilities over time. Below these are 'Vulnerabilities by Deployment' and 'Top Remediations by Impacted Assets' table.

Open CVE Count: 0

Open Remediations: 211

Vulnerability Trend by Severity

Severity	Count of Vulnerabilities
High	~200
Medium	~250
Low	~5
Info	~80

Top Remediations by Impacted Assets

Name	Asset Count
Determine if privileged access is needed.	138

Defining the Playbook

The screenshot shows the 'Respond | Automated Response' interface. The top navigation bar includes the user name 'John Pirc', the current page 'Web App Security I...', and the region 'US-EAST-1 (US)'. The main content area is titled 'Playbooks' and features a search bar and a list of playbooks. A red callout box highlights the '+ Add a Playbook' button with the text 'Click here to get started'. The list of playbooks includes:

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

Defining the Playbook (cont)

Respond | Playbooks

Add a Playbook

1 **Details** Input Variables Result

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 'Add a Playbook' dialog in the Alert Logic interface. The left sidebar shows the navigation menu with 'Respond | Playbooks' and 'Add a Playbook'. The main dialog has a title bar 'Add a Playbook' with a close button. Below the title bar are 'CANCEL' and 'OK' buttons. A red '1' is placed above the 'Input' tab, which is highlighted with a red box. The 'Input' tab contains a list of parameters: 'account_id' (Alert Logic MDR Account ID), 'payload_type' (Alert Logic MDR Payload Type), and 'payload' (Alert Logic MDR Payload Object). A red '2' is placed to the left of this list, which is also enclosed in a red box. At the bottom right of the dialog is a '+ ADD PARAMETER' button.

Defining the Playbook (cont)

The screenshot shows a web interface for defining a playbook. On the left is a sidebar with the Alert Logic logo and navigation options: a hamburger menu, a shield icon, and the text 'Respond | Playbooks'. Below this is a large grey area with the text 'Add a Playbook'. On the right is a modal dialog titled 'Add a Playbook' with a close button (X) in the top right corner. At the bottom of the dialog are two buttons: 'CANCEL' (blue) and 'OK' (orange). The dialog has four tabs: 'Details', 'Input', 'Variables' (which is highlighted with a red border), and 'Result'. Below the tabs is a text description: 'This list contains the variables available for use in this playbook and their descriptions.'

Defining the Playbook (cont)

Respond | Playbooks

Add a Playbook

Add a Playbook

1

Details Input Variables **Result**

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.

2

Variable	Value
----------	-------

+

Defining the Playbook (cont)

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

Respond | Playbooks

Beta Day (Informational Playbook)
Demo

VALIDATE TEST CANCEL SAVE

Playbook Context

1 + ?

Creating a Task

Defining the Playbook (cont)

The screenshot displays the Splunk SOAR interface for defining a playbook. At the top, the header shows the user 'John Pirc', the environment 'Web App Security I...', and the region 'US-EAST-1 (US)'. Below the header, the breadcrumb 'Respond | Playbooks' is visible. The main content area shows a playbook named 'Beta Day (Informational Playbook)' with a 'Demo' tag. On the right side, there are buttons for 'VALIDATE', 'TEST', 'CANCEL', and 'SAVE'. A 'Playbook Context' panel is open, and a red '1' is placed below it. A dropdown menu titled 'Add task:' is open, showing a search bar and a list of tasks. The tasks listed are:

- 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

A red arrow points from a text box to the dropdown menu.

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

Defining the Playbook (cont)

The screenshot displays the Alert Logic 'Respond | Playbooks' interface. On the left, a sidebar shows 'Playbook Context' and 'Alert Logic send_approval_email'. The main area is titled 'send_approval_email0' and features a 'Task' tab highlighted with a red box. Below the tabs, the 'Task Details' section includes:

- Name:** send_approval_email0
- Action:** send_approval_email
- Description:** Request an approval via an email
- Repeat this action

Buttons for 'CANCEL' and 'OK' are located in the top right corner of the task configuration window.

Defining the Playbook (cont)

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

Respond | Automated Response

incident
Beta Day (Informational Playbook)
Demo

VALIDATE TEST CANCEL SAVE

Playbook Context

Alert Logic
send_approval_email0

Creating a Condition

Defining the Playbook (cont)

Task **Request** Response

account_id * **VARIABLES** ▾
<% 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.

2
subject

3a **3b**
message
This IP <% ctx().payload.attacker_ip.set.select(\$ip)%> is bad

ttl
60

Condition
<% succeeded() %>

Playbook Context

Alert Logic
send_approval_email0

Respond | Playbooks

send_approval_email0

CANCEL OK

Defining the Playbook (cont)

The screenshot displays the Alert Logic Playbook Editor interface. On the left, a sidebar shows the 'Respond | Playbooks' menu and a list of tasks including 'Playbook Context' and 'Alert Logic send_approval_email'. The main workspace is titled 'send_approval_email0' and features a 'Response' task highlighted in blue. A red box labeled 'TBA' is positioned to the right of the task, with a red arrow pointing to the 'Response' label. The interface includes 'CANCEL' and 'OK' buttons in the top right corner.

Defining the Playbook (cont)

The screenshot displays the Alert Logic Playbook Editor interface. On the left, a sidebar shows the 'Respond | Playbooks' menu and a list of tasks including 'Playbook Context' and 'Alert Logic send_approval_email0'. The main workspace shows the configuration for the 'send_approval_email0' task. At the top right of the workspace are 'CANCEL' and 'OK' buttons. Below the task name, there are tabs for 'Task', 'Request', 'Response', and 'Publish', with 'Publish' highlighted in a red box. Under the 'Conditions' section, there is a 'Name' field, an 'If' field with a 'VARIABLES' dropdown, and a 'Do:' section containing a 'List of items to publish' field. Below this is a table with 'Key' and 'Value' columns, and a plus sign icon to add new items. A red arrow points from a red box containing the text 'TBA' to the 'Publish' tab.

Defining the Playbook (cont)

The screenshot displays the Alert Logic Playbook editor interface. On the left, a sidebar shows 'Respond | Playbooks' with a 'Playbook Context' and 'Alert Logic send_approval_email' section. A configuration window titled 'Condition <% succeeded() %>' is open, showing a 'Name' field with 'Rejected' and an 'If' field with '<% failed() %>'. A 'Do:' field is also present. A dropdown menu is open for the 'Do:' field, showing 'VARIABLES' and a list of variables including 'Task default status', 'Success', 'Fail', 'Playbook Inputs', and various payload attributes. Red boxes with numbers 1 and 2 highlight the 'Name' field, the 'If' field, and the 'Do:' field. A red box with the number 2 also highlights the 'VARIABLES' dropdown menu.

Defining the Playbook (cont)

The screenshot displays the Alert Logic Playbook editor interface. On the left, a sidebar shows the 'Respond | Playbooks' menu and a list of components including 'Playbook Context' and 'Alert Logic send_approval_email'. A 'Condition' dialog box is open, showing the configuration for a condition named '<% succeeded() %>'. The dialog has a title bar with a question mark icon and a close button. The main configuration area is titled 'Conditions' and contains the following fields:

- 1**: The 'Conditions' header.
- 2**: The 'Name' field, which contains the text 'Approved'.
- 3**: The 'Do:' field, which contains the text '<% succeeded() %>'.
- A 'VARIABLES' dropdown menu is visible next to the 'Name' field.
- Below the 'Do:' field, there is a section for 'List of items to publish' with a table structure showing 'Key' and 'Value' columns, and a plus sign icon to add items.

At the top right of the dialog, there are 'CANCEL' and 'OK' buttons. The background shows a partial view of the playbook editor with a 'Condition' block being added to a flow.

Defining the Playbook (cont)

The screenshot displays the Alert Logic Playbook Editor interface. The main window is titled 'incident_add_feedback1' and features a 'Task' tab highlighted in red. A red box with the number '1' is positioned above the 'Task' tab. The 'Task Details' section is visible, showing the following information:

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

In the background, a 'Condition Approved' dialog box is open, and a 'Playbook Context' panel is visible. The 'Alert Logic send_approval_email' task is also present in the workflow.

Defining the Playbook (cont)

The screenshot displays the Alert Logic Playbook Editor interface. On the left, the 'Respond | Playbooks' menu is visible, along with a 'Playbook Context' and 'Alert Logic' section. A 'Condition Approved' block is shown in the workflow. The main editor area is titled 'incident_add_feedback1' and contains a 'Request' task configuration. The configuration is annotated with four red boxes and numbers:

- 1**: The 'Request' task name.
- 2**: The 'VARIABLES' dropdown menu for the 'account_id' field.
- 3**: The 'VARIABLES' dropdown menu for the 'customer_feedback' field.
- 4**: The 'customer_feedback_reason' dropdown menu.

The task configuration details are as follows:

- Task:** Request
- Response:** Publish
- 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:** (Dropdown menu)
- further action:** (Dropdown menu with options: further action, acceptable risk, compensating control, threat not valid, not concluded, other)

Defining the Playbook (cont)

The screenshot displays the Alert Logic Playbook Editor. The main workspace shows a flowchart with a 'Condition Approved' step leading to an 'Alert Logic incident_complete2' step. A red box labeled '1' highlights the 'Task' tab in the right-hand configuration panel. The 'Task Details' section is visible, showing the following information:

- Name:** incident_complete2
- Action:** incident_complete
- Description:** Close incident and provide reason for closing an incident.
- Repeat this action

The configuration panel also includes tabs for 'Request', 'Response', and 'Publish', and buttons for 'CANCEL' and 'OK'.

Defining the Playbook (cont)

The screenshot displays the Alert Logic Playbook Editor interface. On the left, a workflow diagram shows a sequence of steps: 'Playbook Context', 'Alert Logic send_approval_email', 'Condition Approved', and 'Alert Logic incident_complete2'. The 'Alert Logic incident_complete2' step is selected, and its configuration is shown in a detailed view on the right.

The detailed view for the 'incident_complete2' task is titled 'Task Request' and includes the following configuration:

- Task:** Request
- account_id *:** <% ctx().account_id %>
- incident_id *:** <% ctx().payload.incidentId %>
- notes *:** The following IP <% ctx().payload.attacker_ip.select(\$.ip)%> is malicious and needs to be blocked
- reason_code:** acceptable risk

Four red boxes with numbers 1 through 4 highlight specific elements in the configuration: 1 points to the 'Request' task name, 2 points to the 'account_id' variable, 3 points to the 'notes' text containing a variable, and 4 points to the 'reason_code' dropdown menu.

Validating a Playbook

The screenshot displays the Alert Logic interface for validating a playbook. At the top, the user is identified as John Pirc, and the environment is Web App Security I... in US-EAST-1 (US). The page title is "Respond | Playbooks". The specific playbook being edited is "Beta Day (Informational Playbook)", which is a demo.

The main area shows a flowchart of the playbook logic:

- Playbook Context** (Start)
- Alert Logic send_approval_email0** (Action)
- Condition Approved** (Condition)
- Condition Rejected** (Condition)
- Alert Logic incident_complete2** (Action, triggered from Condition Approved)
- Alert Logic incident_add_feedback1** (Action, triggered from Condition Rejected)

At the bottom of the interface, a dark grey notification bar displays 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",
```

```
2020-08-10T11:24:27.765796+00:00
{"accountId": 2, "asset_deployment_type": "aws", "asset_host_name": "10.1.2.3", "asset_native_account_id": "2", "assets": {}, "attacker": {"account": "2", "instanceId": "i-0a159b2a553285ebb", "ip": "10.10.10.12", "port": 40814, "region": "us-east-2"}, "attacker_country_code": "BR", "attacker_country_name": "Brazil", "attacker_lset": [{"ip": "86.34.222.99"}, {"value": "SomeAttacker"}], "closed_time": "2020-08-10T11:24:27.765796+00:00"}
```

Setting a Playbook in Motion

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

Manage | Notifications

- Dashboards
- Respond
- Investigate
- Validate
- Configure
- Manage
 - Integrations
 - Users
 - Notifications**
 - Service Status
 - Escalation Preferences
- Support

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

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.		View
Non-ada test	1 Recipients	View

<https://console.account.product.dev.alertlogic.com/#/manage-notifications/134264762/alerts?aid=134264762&locid=defender-us-ashburn>

Setting a Playbook in Motion (cont)

The screenshot shows the Alert Logic 'Manage | Notifications' page. On the left, there are filters for 'Active' (0/6) and 'Inactive' (0/7) notifications, search filters, and account details. The main area is titled 'Alert Notifications' and contains a 'Create a Notification' dropdown menu. The 'Incident' option is highlighted with a red box, and a red arrow points to it from a box labeled 'Select Incident'. Below the dropdown, a list of notifications is displayed, including 'High Incident Alert', 'Info Dev Test Incident Notification', 'Nancy's High Incident Alert', and 'Nancy's test'.

Notification Title	Most recent notification sent	Recipients	View
Info level notifications	Most recent notification sent: Jan 26 2021 17:00:46 GMT-6	2	View
High Incident Alert	Most recent notification sent: Jan 26 2021 11:54:37 GMT-6	2	View
Info Dev Test Incident Notification	Most recent notification sent: No notifications sent.	1	View
Nancy's High Incident Alert	Most recent notification sent: No notifications sent.	1	View
Nancy's test		1	View

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) ×

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.

Recipients

Notification Delivery

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

Select User(s)

Subscribe User(s) (1)

Select All

Subscribe Connector (none)

John Pirc john.pirc@alertlogic.com (creator)

Subscribe Playbook (none)

Email Subject

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

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

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) >

3

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
 - Channel 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)

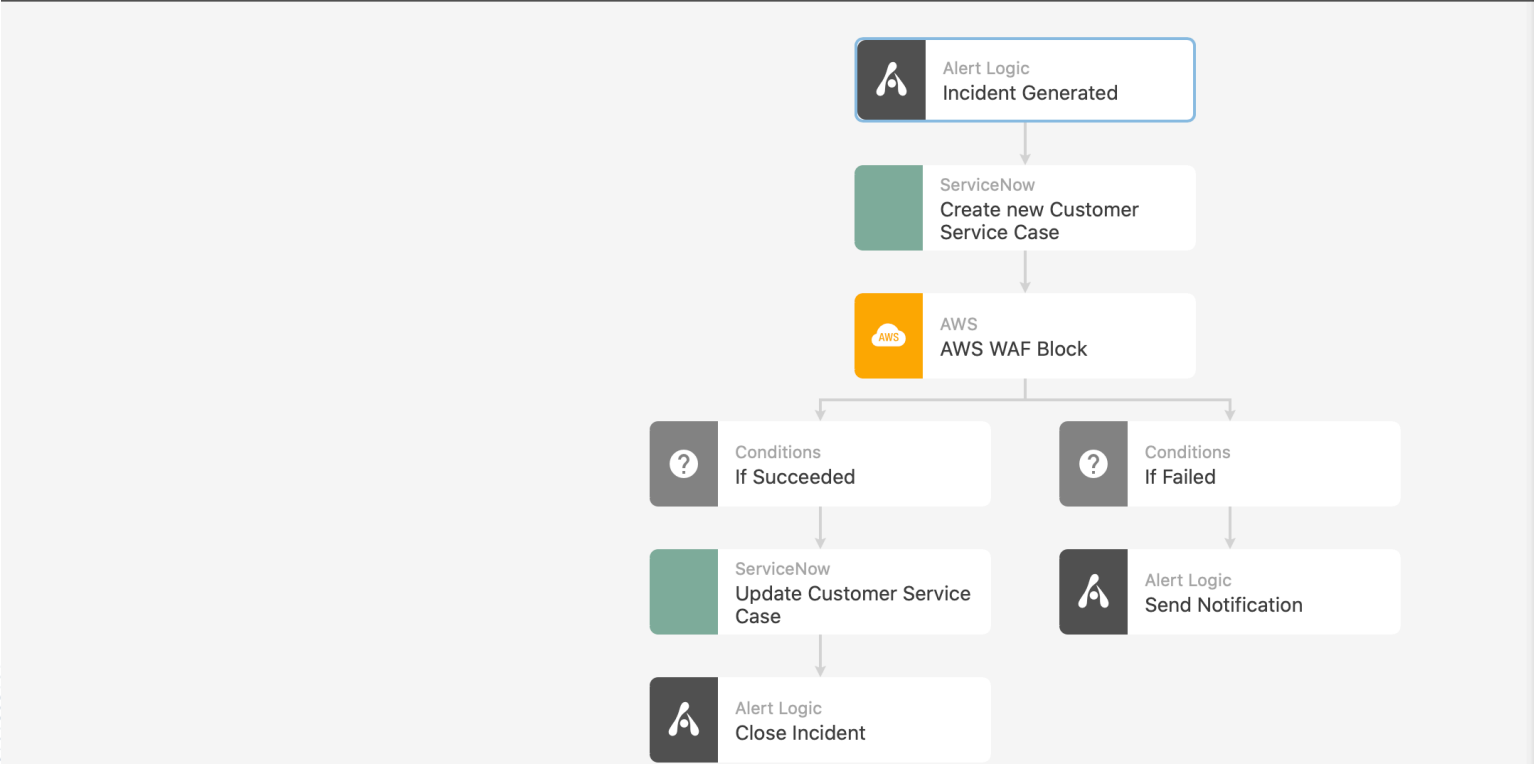
ALERT LOGIC

Configuration | Automated Response

Incident Response

ServiceNow and AWS WAF Block

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



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:

ADD FILTER ▾

search

Threat Rating

Escalation

Classification

Detection Source

Asset Groups



Setting a Playbook in Motion (cont)


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

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	
 Darwin Test for info level notifications Most recent notification sent: Jan 26 2021 17:00:46 GMT-6	2 Recipients	
 High Incident Alert Most recent notification sent: Jan 26 2021 11:54:37 GMT-6	2 Recipients	
 Info Dev Test Incident Notification Most recent notification sent: No notifications sent.	1 Recipients	

Running an on-demand Playbook

The screenshot displays a security dashboard with the following components:

- Header:** User 'John Pirc', 'Web App Security I...', and region 'US-EAST-1 (US)'. A 'WHAT'S NEW' notification icon is present.
- Navigation:** A sidebar menu includes 'Dashboards', 'Respond', 'Incidents' (highlighted with a red box), 'Exposures', 'Health', 'Automated Response', 'Investigate', 'Validate', 'Configure', 'Manage', and 'Support'.
- Filters:** 'Data for the last:' with options '7d', '14d', and '30d' (selected). 'Custom range:' with a date range '28 Dec 2020 - 27 Jan 2021'.
- Open CVE Count:** A large card showing '0' with an 'INVESTIGATE' button.
- Open Remediations:** A large card showing '211' with an 'INVESTIGATE' button.
- Vulnerability Trend by Severity:** A line chart showing the count of vulnerabilities over time for High, Medium, Low, and Info severities. The Y-axis is logarithmic (10, 100, 1k). High and Medium severity counts are relatively stable around 200-300. Low severity counts are around 5-10. Info severity counts are around 80.
- Vulnerabilities by Deployment:** A bar chart showing the distribution of vulnerabilities across different deployment environments.
- Top Remediations by Impacted Assets:** A table listing remediation actions and the number of assets impacted.

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

Running an on-demand Playbook

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

Respond | Incidents

UPDATED INCIDENTS EXPERIENCE | NOTIFICATIONS | HELP

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

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) search

<input type="checkbox"/>	↓	↓ Date	↓ ID	Summa	↓ Thre.	↓ Class	↓ Dete	↓ Corri	↓ Incid	↓	↓ Depli	↓ Acco	↓ Attac	↓ Target
<input type="checkbox"/>	1	26th Jan 2021	9sysx5	SQL Injection, Null Byte, Path Traversal Attempts from 7.33.6.77	Medium	application-attack	Web Log Analytics	0			WLA Integration Log Source	Web App Security Integration	7.33.6.77	suitablek id.com
<input type="checkbox"/>	>	26th Jan 2021	38jr5b	SQL Injection, Null Byte, Path Traversal	Medium	application-attack	Web Log Analytics	0			WLA Integration Log Source	Web App Security Integration	35.6.0.4	suitablek id.com

Setting a Playbook in Motion (cont)

Alert Logic logo | 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...
26th Jan 2021 11:54:29 GMT-6

OPEN IN IRIS | UPDATE | SNOOZE | CLOSE | **PLAYBOOK**

2

Investigation and Recommendation

Evidence

Search

Investigation Report

Audit Log | Notification History

Topology

Grid icon | Tag icon | Shield icon | Fork icon | Window icon



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

Setting a Playbook in Motion (cont)

The screenshot shows the Alert Logic interface for an incident. The incident title is "SQL Injection, Null Byte, Path Traversal Attempts from 7...". A modal window titled "Run playbook" is open, showing a list of playbooks. The "Beta Day (Informational Playbook)" is highlighted. The "RUN" button is also highlighted.

Incident 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

Run playbook

playbook_id

Add Note to Incident

- Select --
- Add Note to Incident
- Austin Texas
- Automated Response SKO Demo (Do Not Delete)
- Beta Day (Informational Playbook)**
- Carl Inquiry Verification

CANCEL RUN

Setting a Playbook in Motion (cont)

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

Respond | Incidents | UPDATED INCIDENTS EXPERIENCE | NOTIFICATIONS | HELP

Execution record created successfully. Go to Playbook History



Medium

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

Topology



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



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



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
- UPDATED
- SNOOZE
- CLOSE
- PLAYBOOK

Investigation and Recommendation

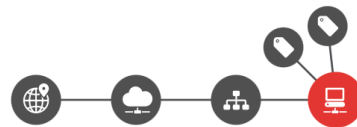
Evidence

Search

Investigation Report

Audit Log | Notification History

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

search filters

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

Playbooks **Playbook History** Inquiries

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

3

```
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": {
```

4

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

2

Jan 26 2021 18:03:49 GMT-6

ID
70C757FE-B7EC-4E5E-8E91-148AFB04340
2

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




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"
    }
  ]
}
```

Inquires (Pending Playbooks)

search filters

Display name

- Email Approval Request 10
- Channels Approval Request 3
- Push Approval Request 3

Status

- pending 9
- succeeded 7

Playbook

- 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

- email 10
- channels 3

Playbooks | Playbook History | **Inquiries**

Inquiries

25 Jan 2021 - 26 Jan 2021

Showing 4 columns of 4 | Sort by Start Time | Search

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-6C048311C543

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

Inquires (Pending Playbooks)

Alert Logic interface showing a list of pending playbooks and a detailed view of a specific one.

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

Navigation: Respond | Automated Response

Filters:

- 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

Playbook Details (Channels test - pending):

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

Actions: 1 (PLAYBOOK), 2 (RESPOND), 3 (EXECUTION)

Logs:

Task Name	Status	Start Time	End Time
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	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](#)



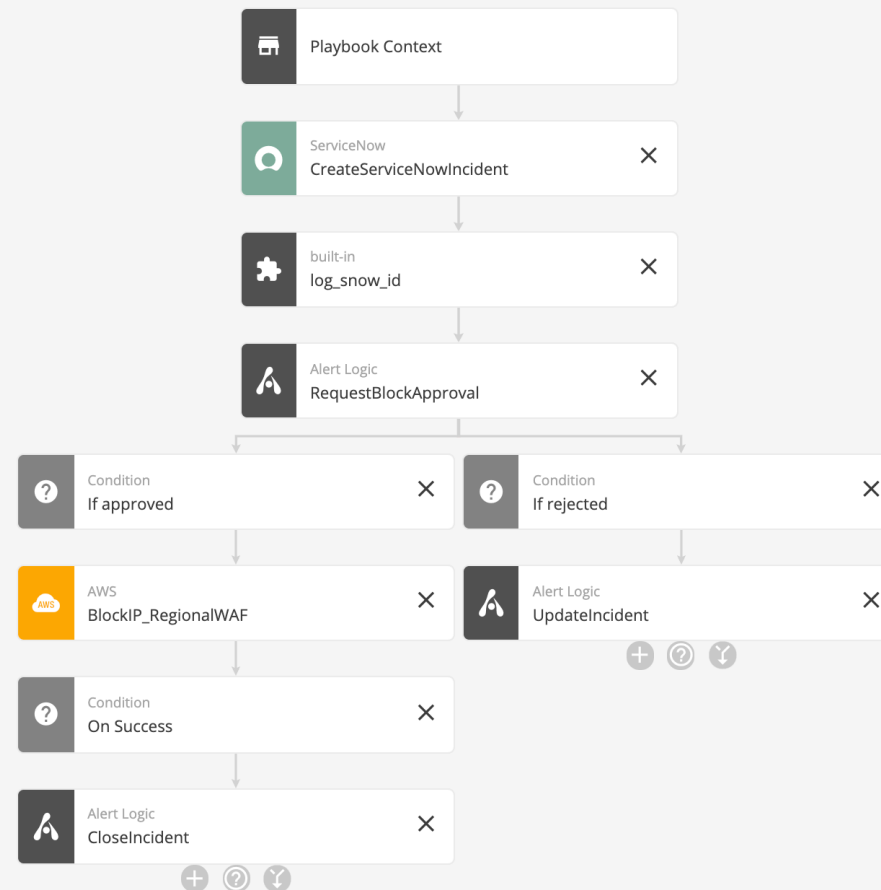
Thank You

Simple Workflow

Respond | Automated Response

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

VALIDATE TEST CANCEL SAVE



Complex Workflow

Incident
Automated Response SKO Demo (Do Not Delete)
This is a playbook that highlights full power of Automated Response to be presented at SKO

VALIDATE TEST CANCEL SAVE

