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

Built for the Cloud

Embedded SOAR

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

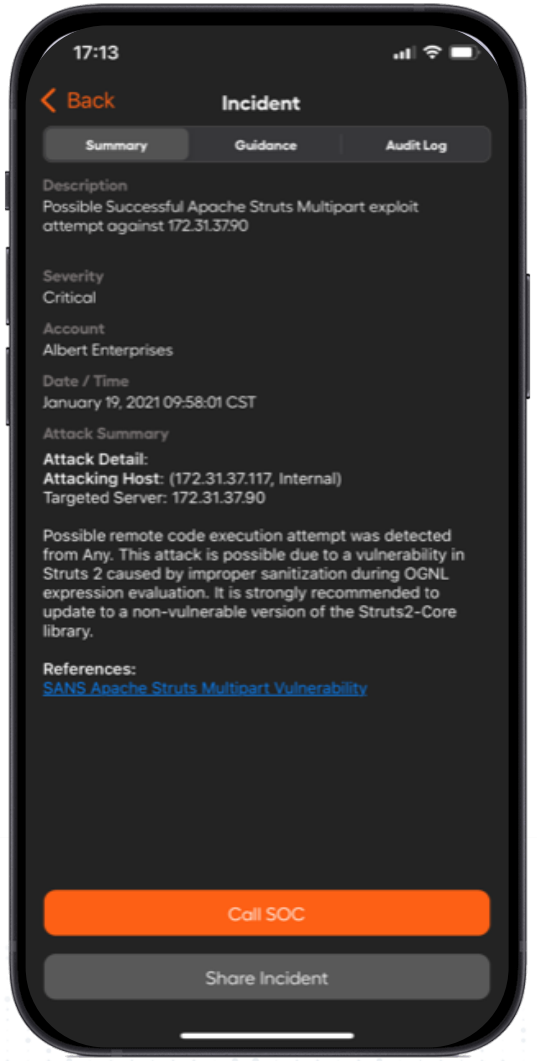
Bring work in balance with resources

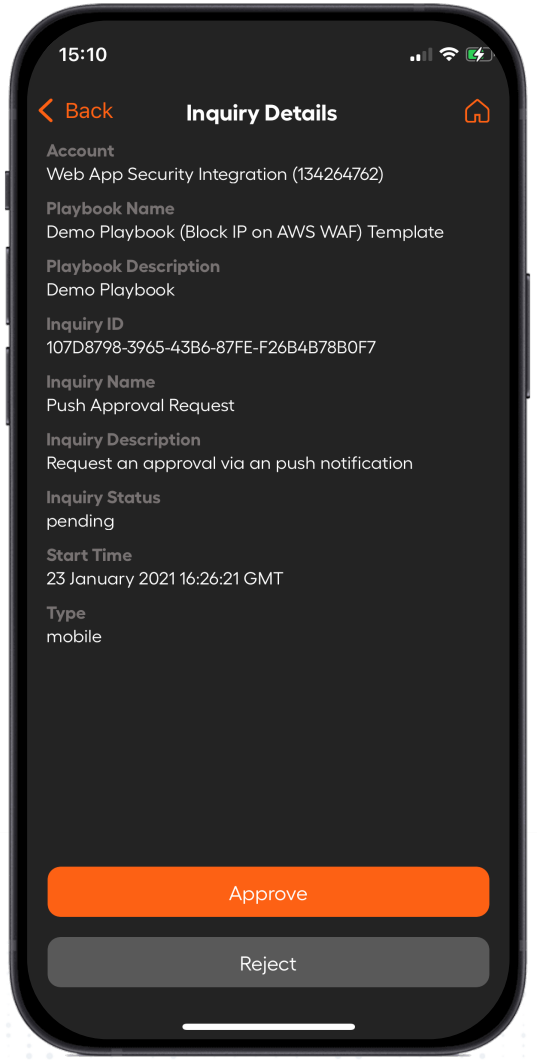
Trustable Automation

Stage 1: Human Approval	Stage 2: Automation with Guardrails	Stage 3: Automation Auditing
• Review before automation acts	• Whitelist key assets to avoid automation gone awry	• Trust but verify

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

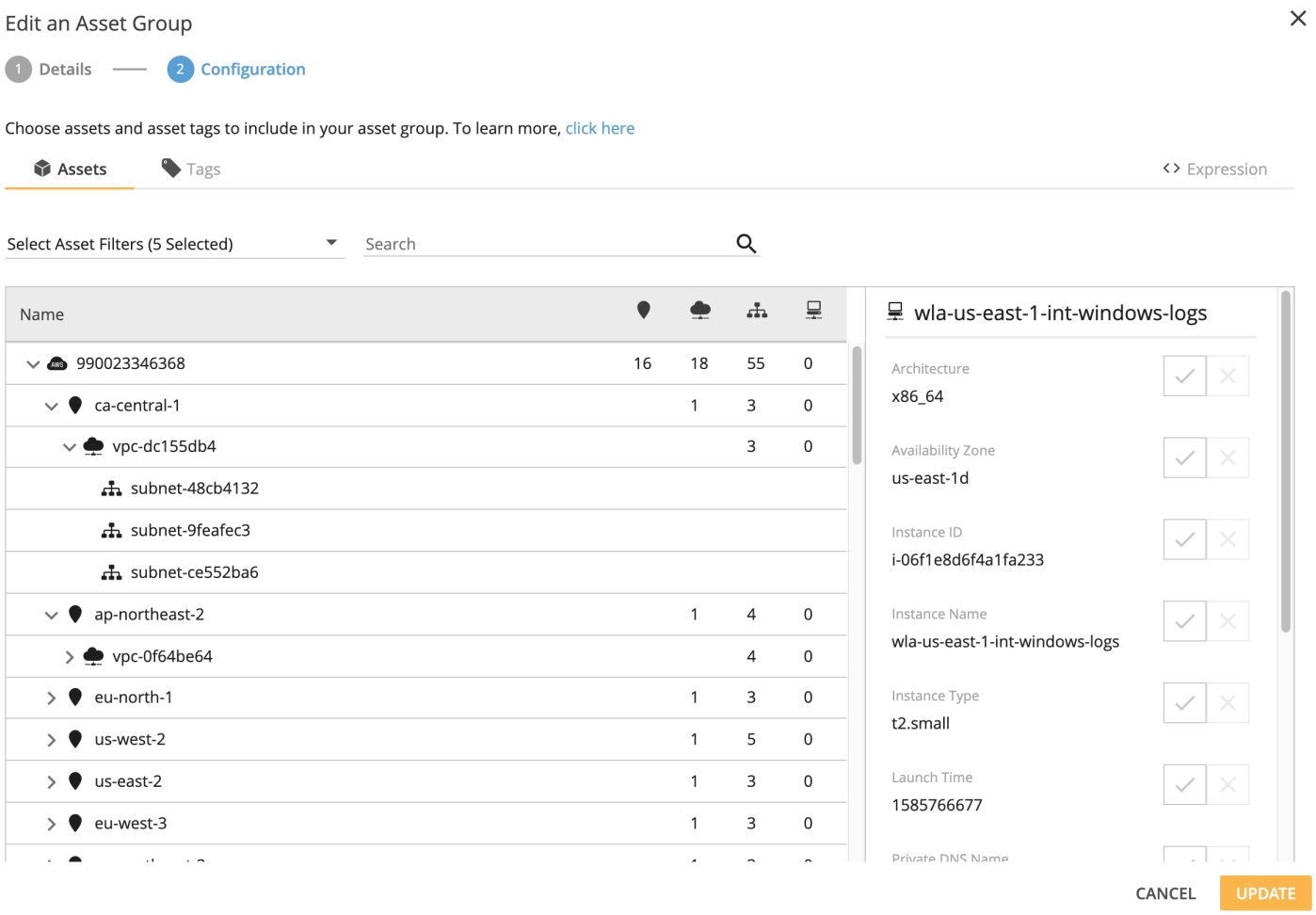
- Review before automation acts

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

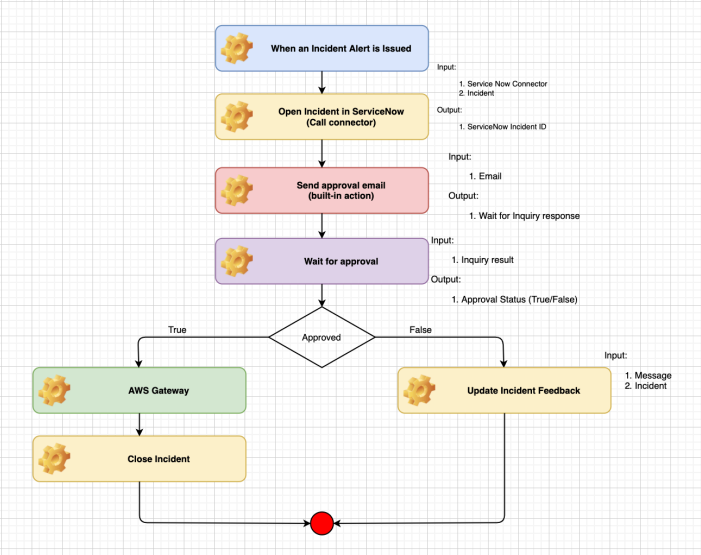


Demo

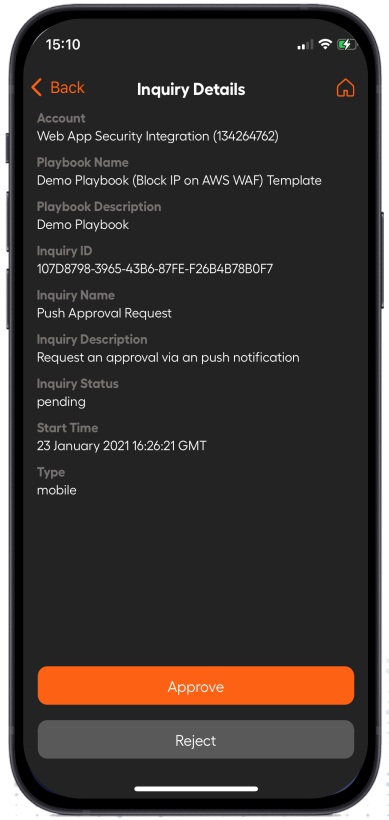
About the Beta Environment

Platform

Playbook



Approval



Outcomes

Block Attacker

Disable User Account

ALERT LOGIC™

Threat Intel Center

Threat Intel Center (Getting Started)

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

Dashboards

WHAT'S NEW

- Dashboards
- Respond
- Investigate
  - Search
  - Topology
  - Vulnerability Library
  - Threat Intel Center
- Validate
- Configure
- Manage
- Support

Data for the last: 7d 14d 30d

Custom range: 28 Dec 2020 - 27 Jan 2021

Count

Open CVE Count

0

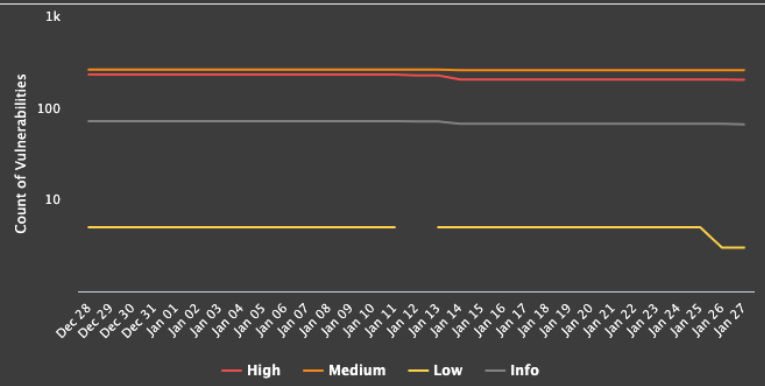
INVESTIGATE

Open Security Remediations

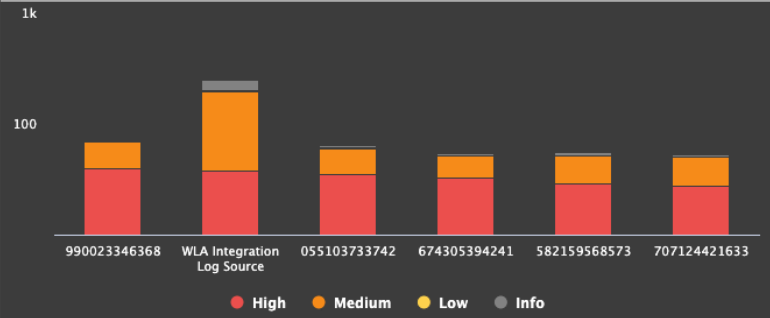
211

INVESTIGATE

Vulnerability Trend by Severity



Vulnerabilities by Deployment



INVESTIGATE

Top Security Remediations by Impacted Assets

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

EXPORT TO CSV

INVESTIGATE

Threat Intel Center Landing Page

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

Analytics

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_U
RNAME'] Granted Admin Privileges
y ['SOURCE_USERNAME']

Threat Level
Medium

Telemetry
logmsgs

Technology
AE

Visibility
Incident

Log Source
Microsoft Windows, Okta SSO

Logs
Okta User Granted Administrator P
vileges, Ossec Windows User Accou
t Changed, ProtoBase User Accour
nformation, ProtoBase User Accou
Modified, Windows Special Groups
ave Been Assigned To A New Logo
Windows System Security Access G
anted, Windows User Account Cha
ged

Signatures
None

Customize Table

Malcolm Palmer | Web App Security I... | 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

Analytics

Choose Columns (4 of 15 Shown)

- Logs
- Name
- Recommendations
- Response Actions

search

	Summary	Threat Level	Telemetry
a	Access to Anomalous Resource from %distinct%	Medium	None
a	Access to Unauthorized Resource from %distinct%	Medium	None
A	['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
app/eternalblue_success	ETERNALBLUE srvnet.sys RCE possible success from 1.2.3.4	High	IDS

accessanomaly

Summary
Access to Anom
%distinct%

Threat Level
Medium

Telemetry
None

Technology
AE

Visibility
Incident

Log Source
None

Logs
Not Applicable

Signatures
None

Filter 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** 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_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

successful_sqli/apache_struts_sc n_success

Summary
Successful Apache Struts CVE-2013 251 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 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

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

Investigate | Threat Intelligence Center

Metasploit PowerShell backdoor installation detected on ['ip_addre...

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

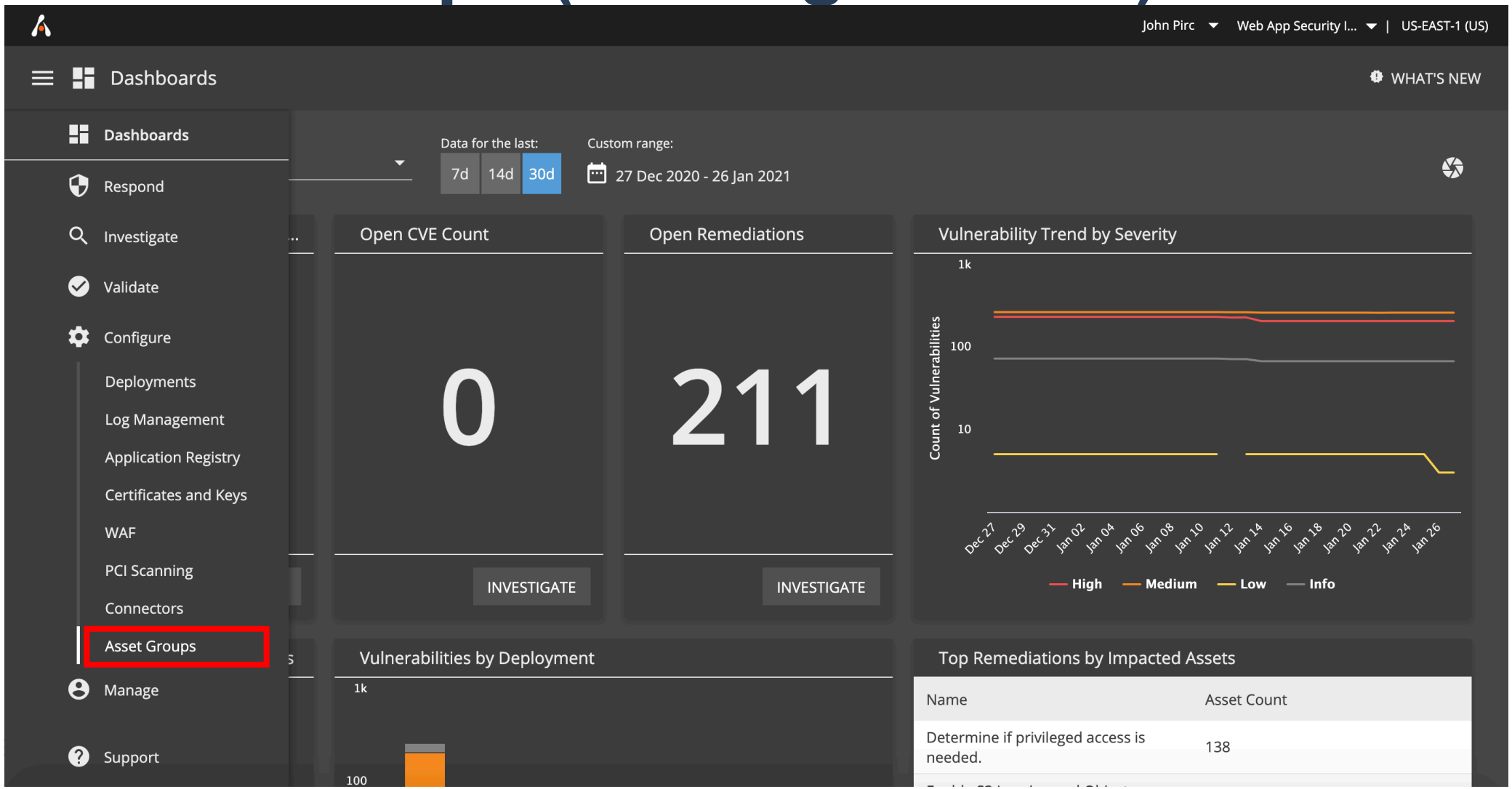
Technology	Telemetry	Log Source	Log Message Types
NGX	Log	Log	Windows PowerShell Engine State Changed

Signatures	CVE	CWE	Threat Classification
None			None

Response Actions	Response Action Parameters
Quarantine	victim

Asset Groups

Asset Groups (Getting Started)



Asset Groups Landing Page

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

Configure | Asset Groups

Add an Asset Group

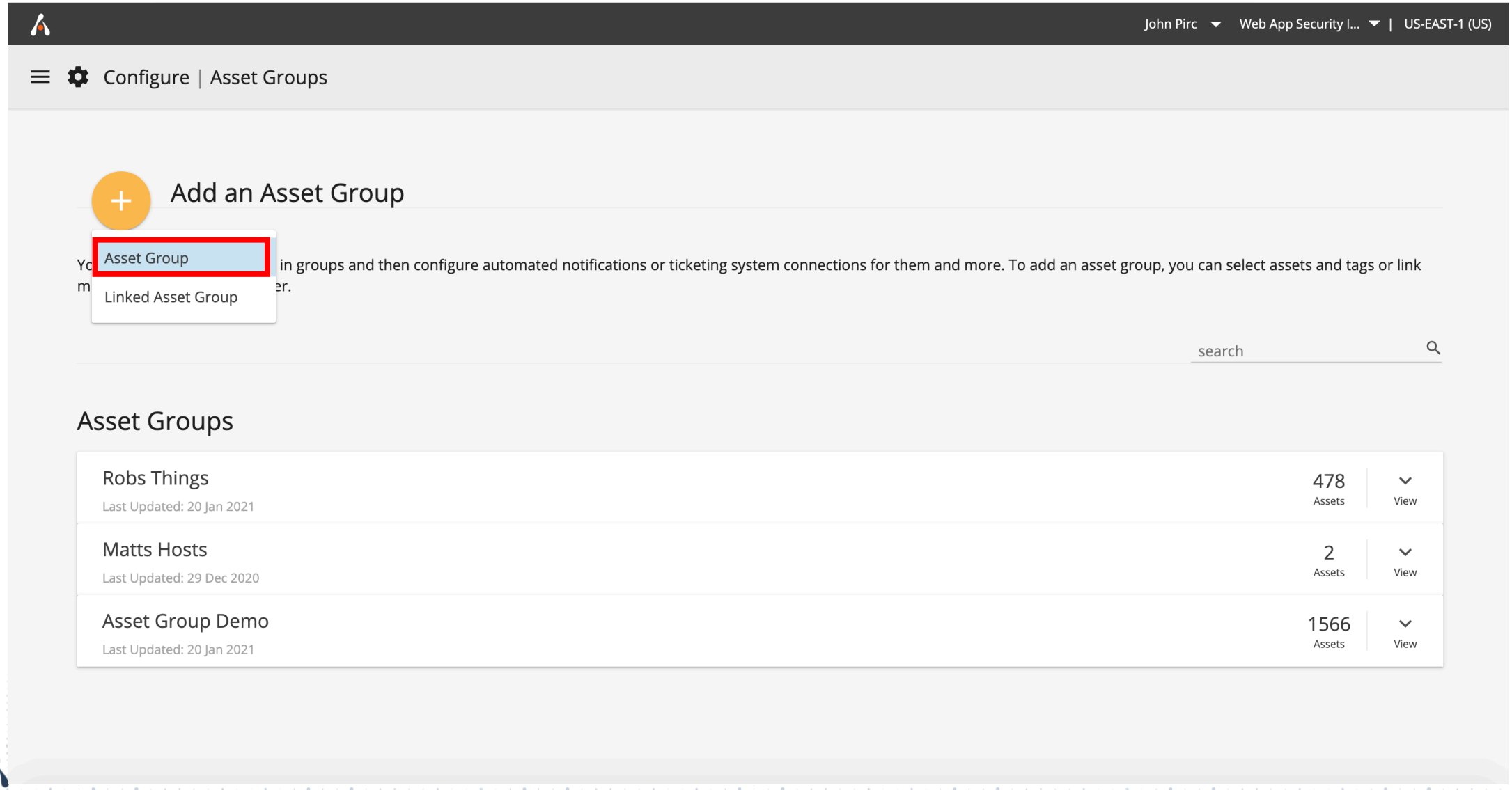
You can organize your assets in groups and then configure automated notifications or ticketing system connections for them and more. To add an asset group, you can select assets and tags or link multiple asset groups together.

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



Adding an Asset Group (Step 1)

Add an Asset Group

1 Details — 2 Configuration

Provide details about your new asset group

1

Name *
PCI

2

Description *
Assets in Scope

3

Criticality Rating
3

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

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
us-east-1		2	7	2
cas-dev-wla-us-east-1-int			1	1
vpc-be8c16d9			6	1
subnet-86a2118a				
subnet-0f1df346				1

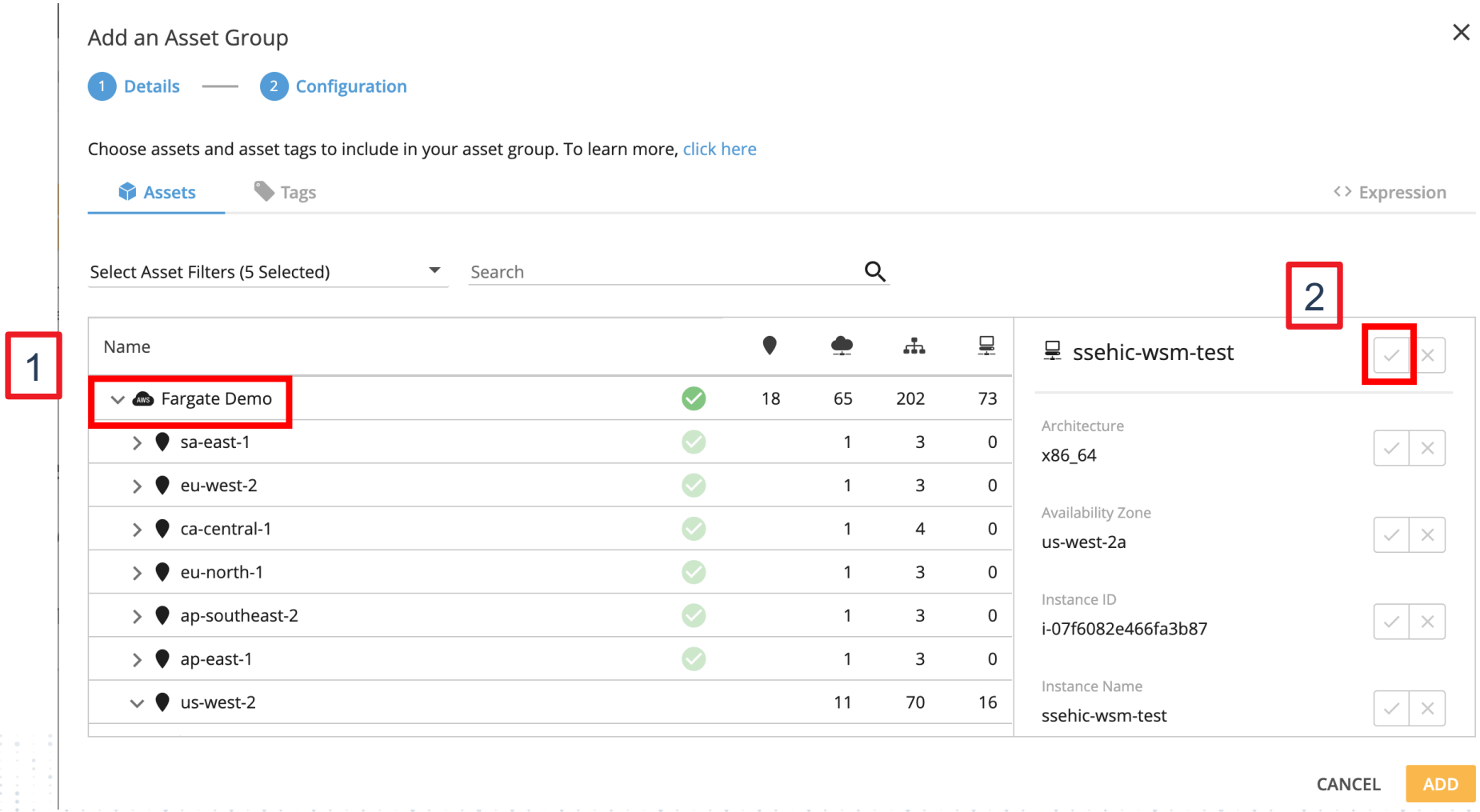
1

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)



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

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

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

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

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-

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.

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 1 Expression

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

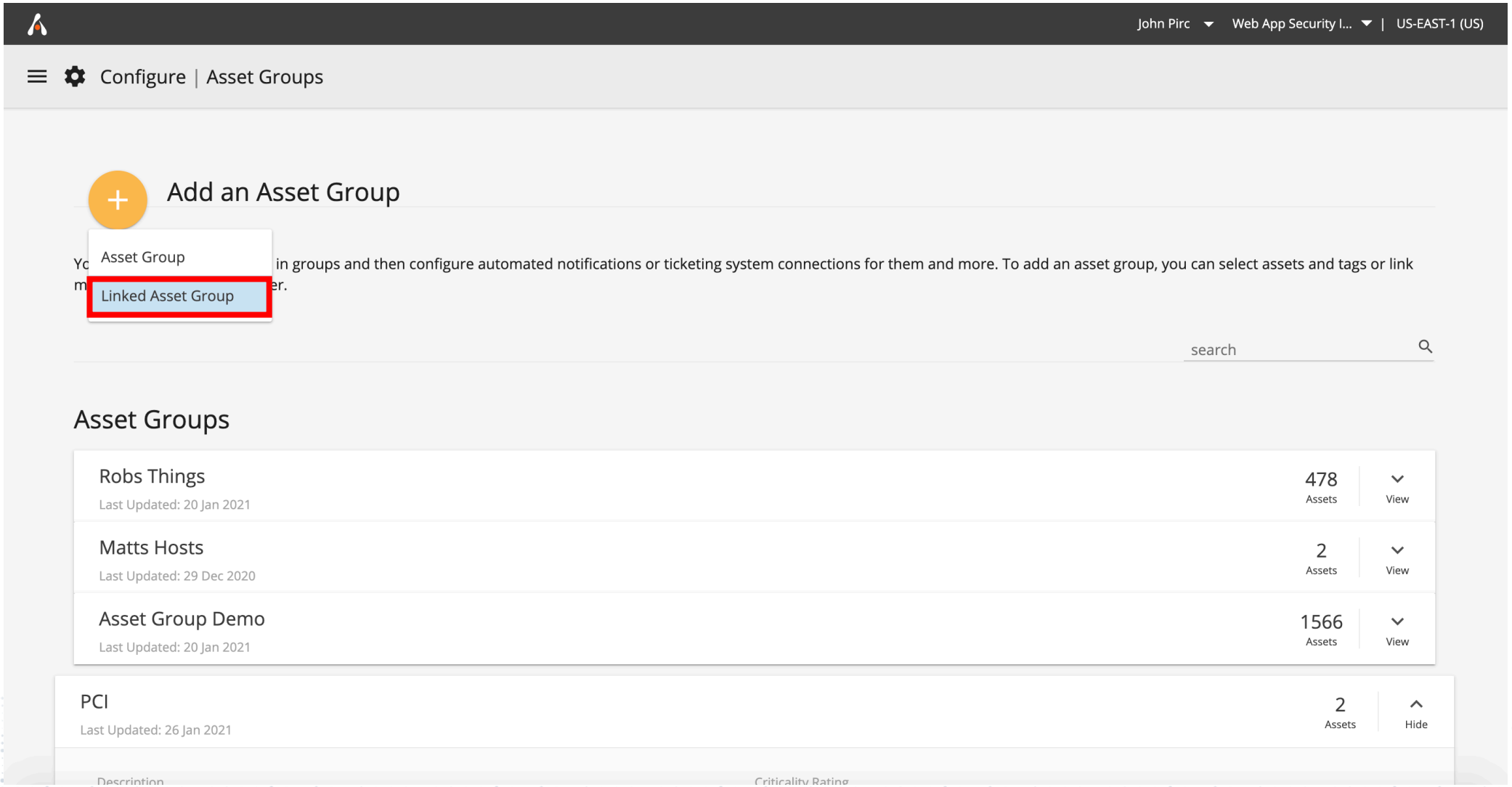
View the schema and learn more

Expression Editor EDIT 2

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

CANCEL UPDATE

Creating Linked Asset Groups



Creating Linked Asset Groups (cont)

Add a Linked Asset Group

1 Details — 2 Configuration

Provide details about your new asset group

1

Name *
Compliance

2

Description *
Critical Assets in Scope

3

Criticality Rating
3

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

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

1 Robs Things

Matts Hosts

2 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)

Asset Groups and Exposures

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

Respond | Exposures

HELP

Category
- Security 2.5k
- IAM Access Analyzer 94
- External 41

Deployment
- AWS Production Deployment 1.4k
- Fargate Demo 430
- Ozone 409
- Development Azure Environment 299
- Production Data Center 12
- Training-Lab-Test 7

Platform
- AWS 2.2k
- Azure 299
- Data Center 19

Asset Group
- JP Test 398
- AWS Production Web Servers 75

Select a deployment to view additional asset filters.

	Affected Assets	Exposure Instances		
Determine if privileged access is needed. (114 | 0 | 0 | 0 | TRI 400.35)	42	114	Open	View
IAM Access Analyzer,Security — Review the IAM Access Analyzer findings for this account. (94 | 0 | 0 | 0 | TRI 343.57)	94	94	Open	View
Security — Restrict access to/from non-required IP addresses (40 | 6 | 0 | 3 | TRI 332.58)	38	49	Open	View
Security — Upgrade OpenBSD OpenSSH to version 8.3.0 (29 | 155 | 21 | 0 | TRI 318.99)	22	205	Open	View
Security — Upgrade Apache Http_server to version 2.4.44 (7 | 170 | 11 | 0 | TRI 281.03)	7	188	Open	View
Security — Enable log metric filters and alarms. (0 | 84 | 0 | 0 | TRI 211.30)	3	84	Open	View
Security — Apply non-default NACLs to all VPC subnets (15 | 0 | 0 | 0 | TRI 120.00)	15	15	Open	View
Security — [illegible]	73	73		

Asset Groups and Exposures

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

Respond | Exposures

HELP

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.

	94 / 0 / 0 / 0	TRI 343.57				
Security	Determine if privileged access is needed.	34 / 0 / 0 / 0	TRI 119.40	10 Affected Assets	34 Exposure Instances	Open / View
Security	Enable log metric filters and alarms.	0 / 28 / 0 / 0	TRI 70.43	1 Affected Assets	28 Exposure Instances	Open / View
Security	Restrict access to/from non-required IP addresses	8 / 3 / 0 / 1	TRI 70.29	8 Affected Assets	12 Exposure Instances	Open / View
Security	Add traffic restrictions to default security group	0 / 20 / 0 / 0	TRI 40.01	10 Affected Assets	20 Exposure Instances	Open / View
Security	Upgrade OpenBSD OpenSSH to version 8.3.0	6 / 9 / 1 / 0	TRI 35.75	1 Affected Assets	16 Exposure Instances	Open / View
Security	Upgrade Php to version 7.3.21	4 / 14 / 0 / 0	TRI 35.03	1 Affected Assets	18 Exposure Instances	Open / View
Security	Use AWS SSL security policy for ELB	4 / 0 / 0 / 0	TRI 32.00	4 Affected Assets	4 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.

Healthy

View Networks | Sort by Name | search

Configuration
alb-ent-backup
Development Azure Environment | 10.2.0.0/16
View

Configuration
AlbertEnterprises-vnet
Development Azure Environment | 10.0.0.0/16
View

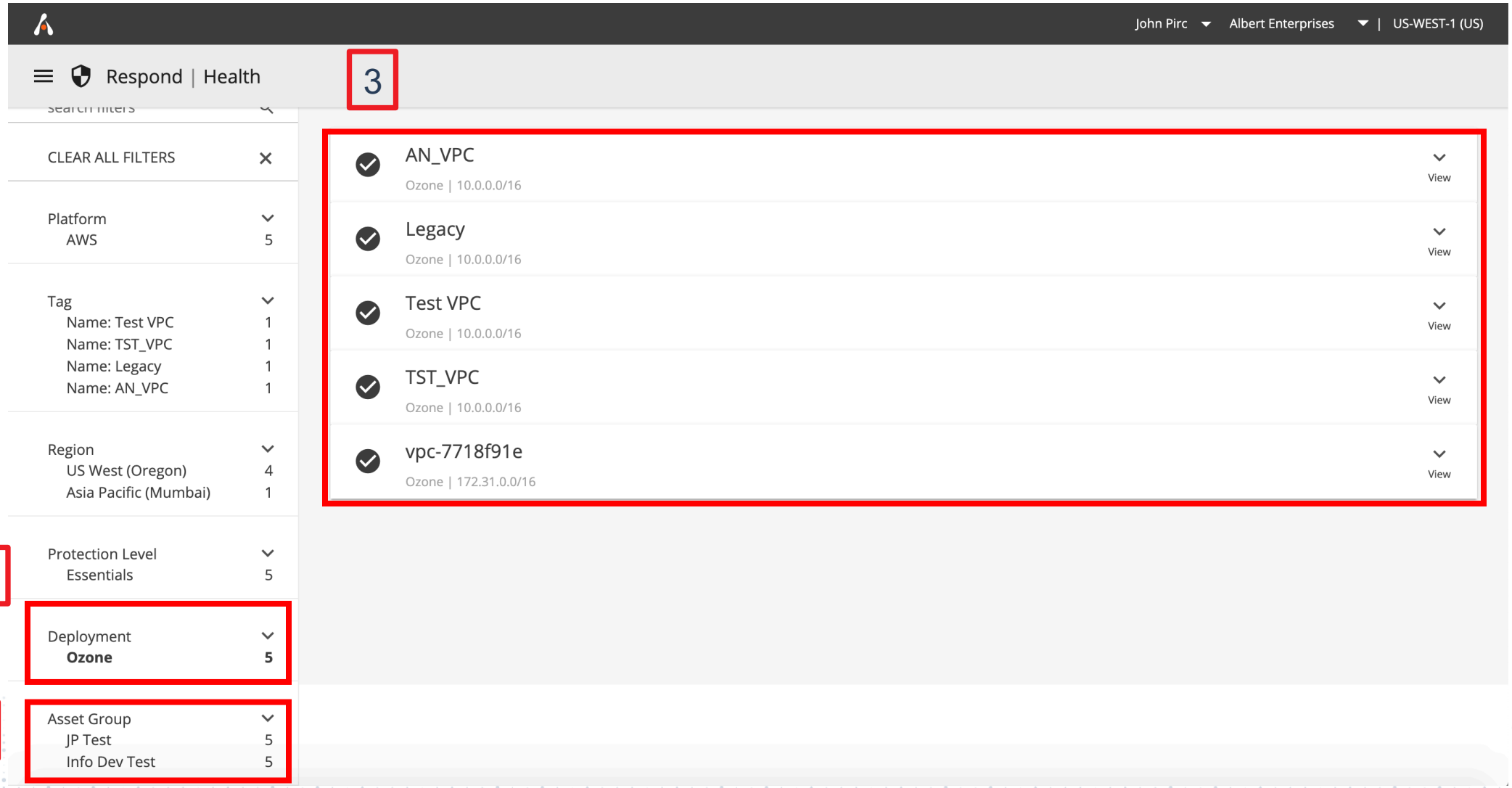
AN_VPC
Ozone | 10.0.0.0/16
View

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



Getting Started from the Dashboard (Playbook)

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

Dashboards

WHAT'S NEW

- Dashboards
- Respond
  - 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

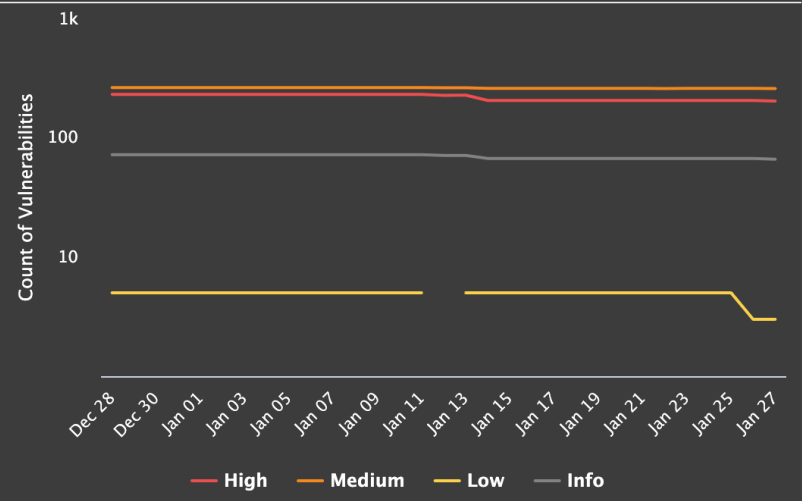
INVESTIGATE

Open Remediations

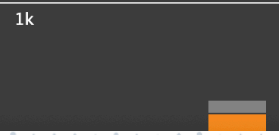
211

INVESTIGATE

Vulnerability Trend by Severity



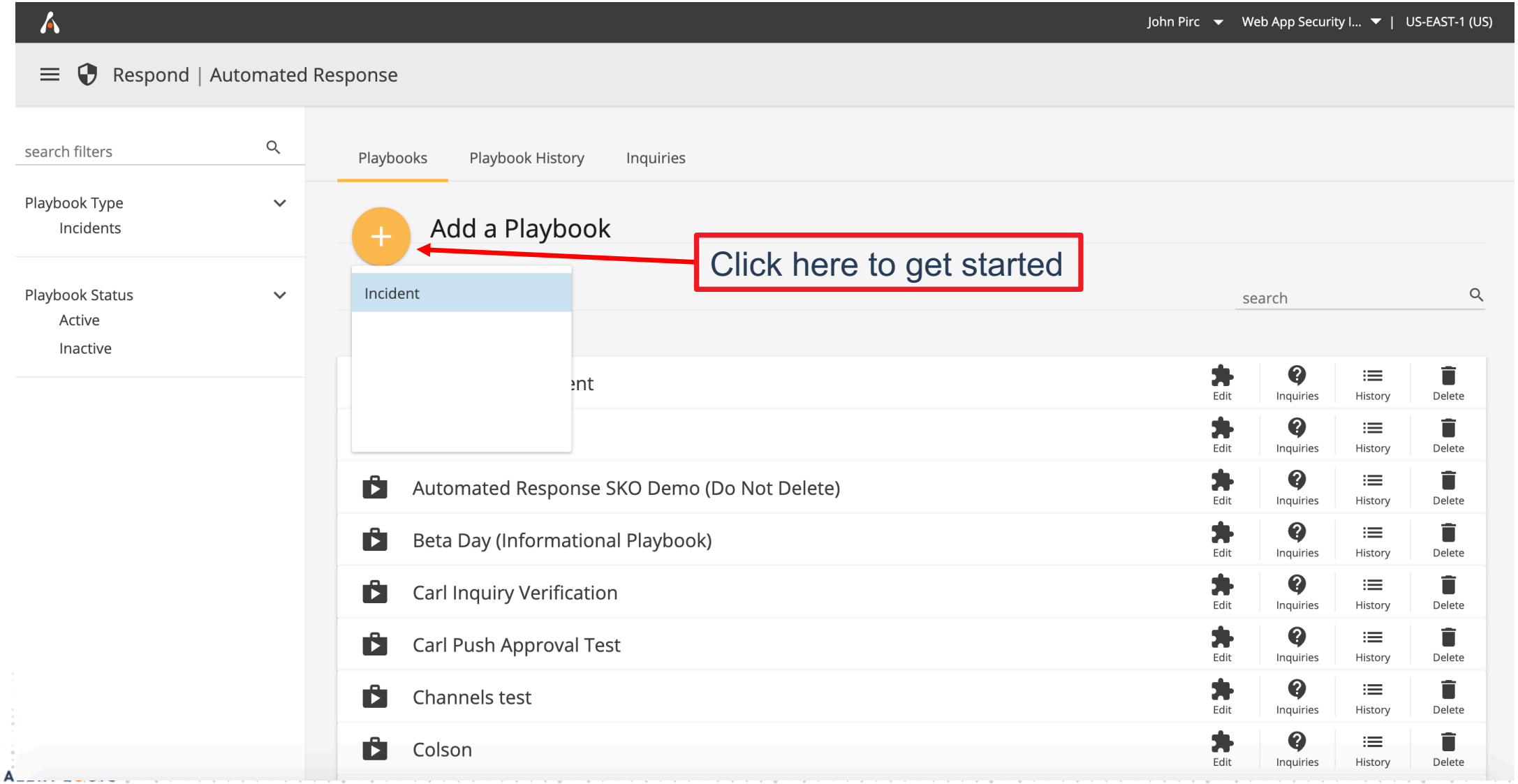
Vulnerabilities by Deployment



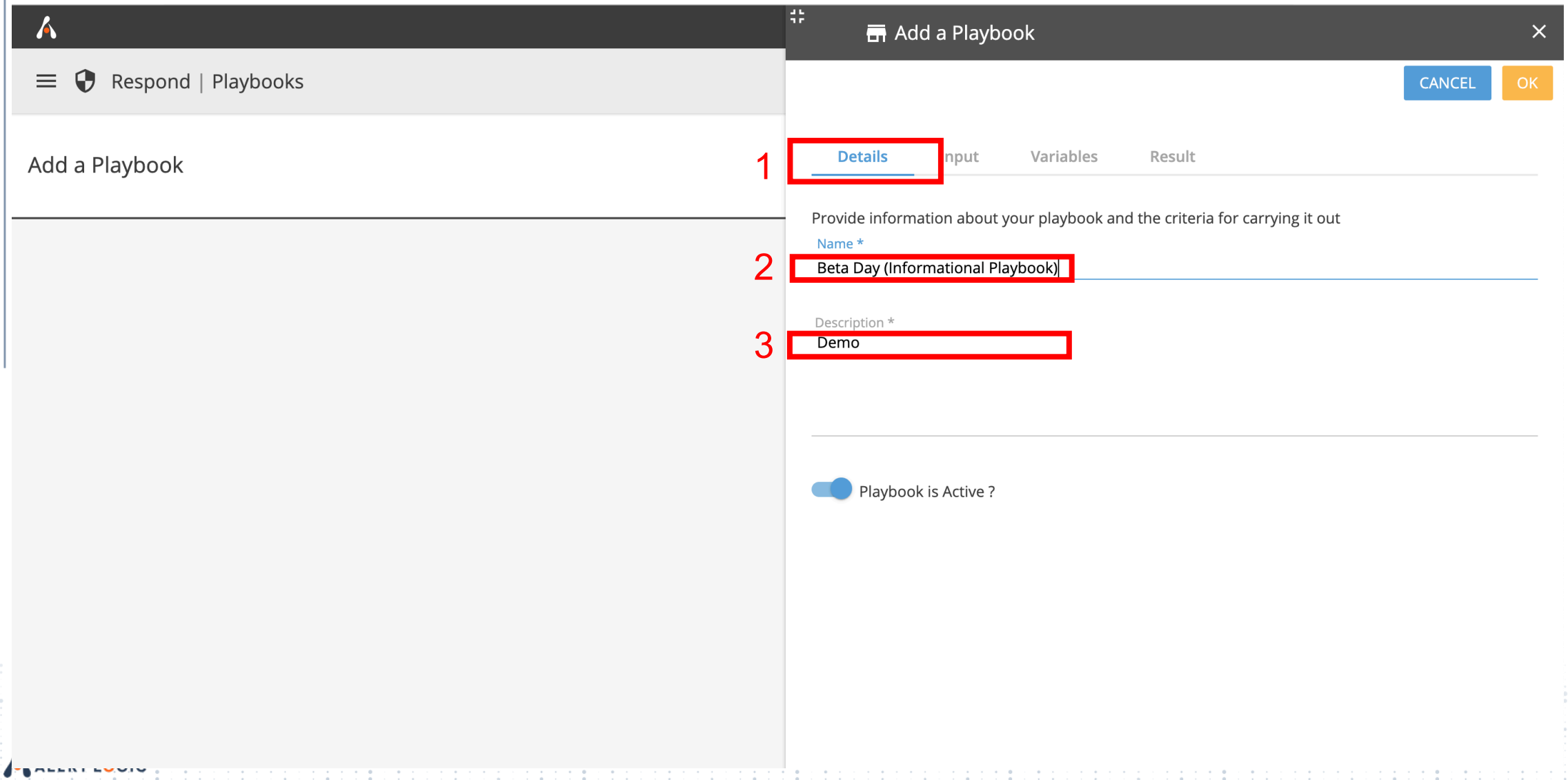
Top Remediations by Impacted Assets

Name	Asset Count
Determine if privileged access is needed.	138

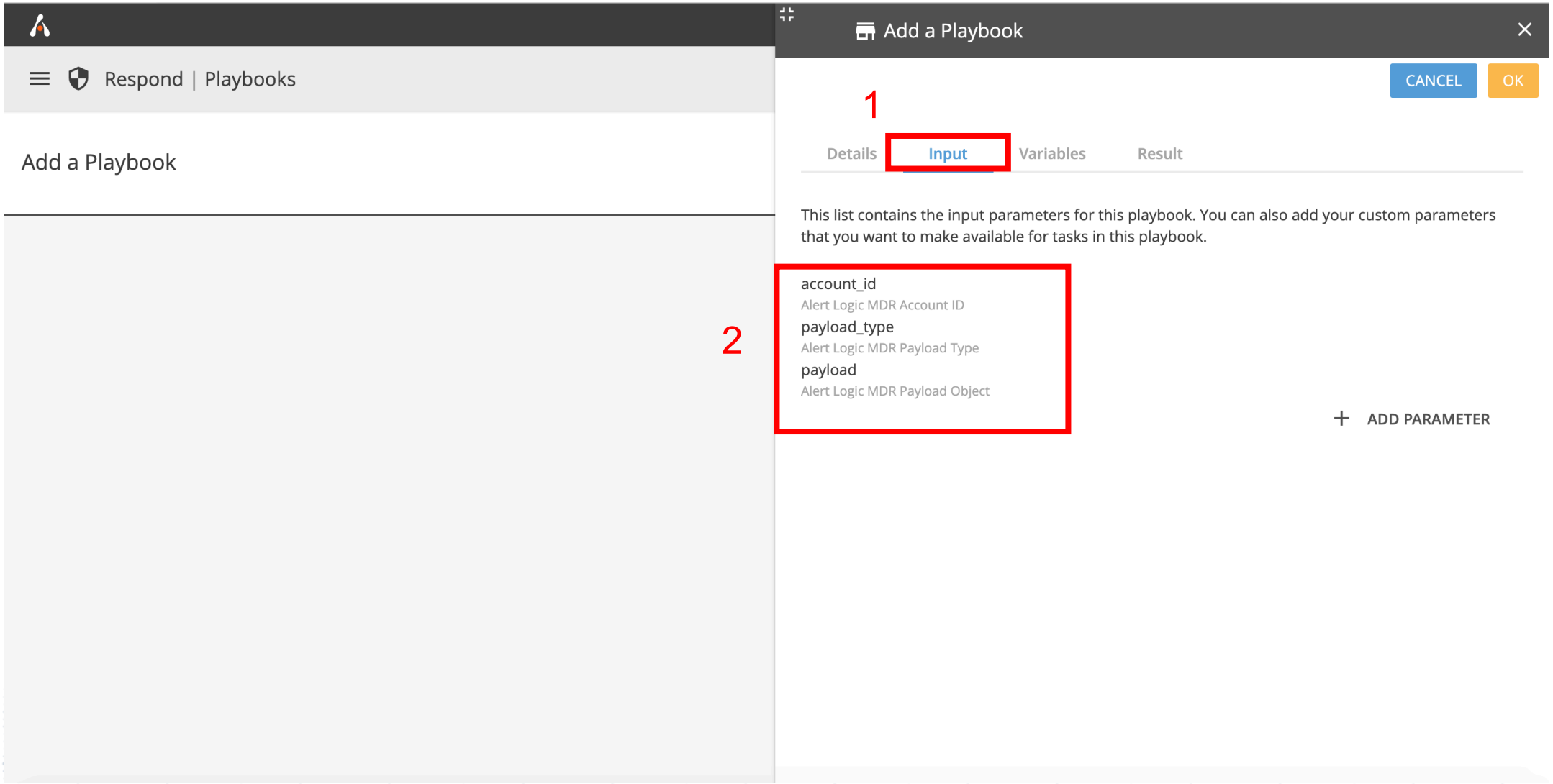
Defining the Playbook



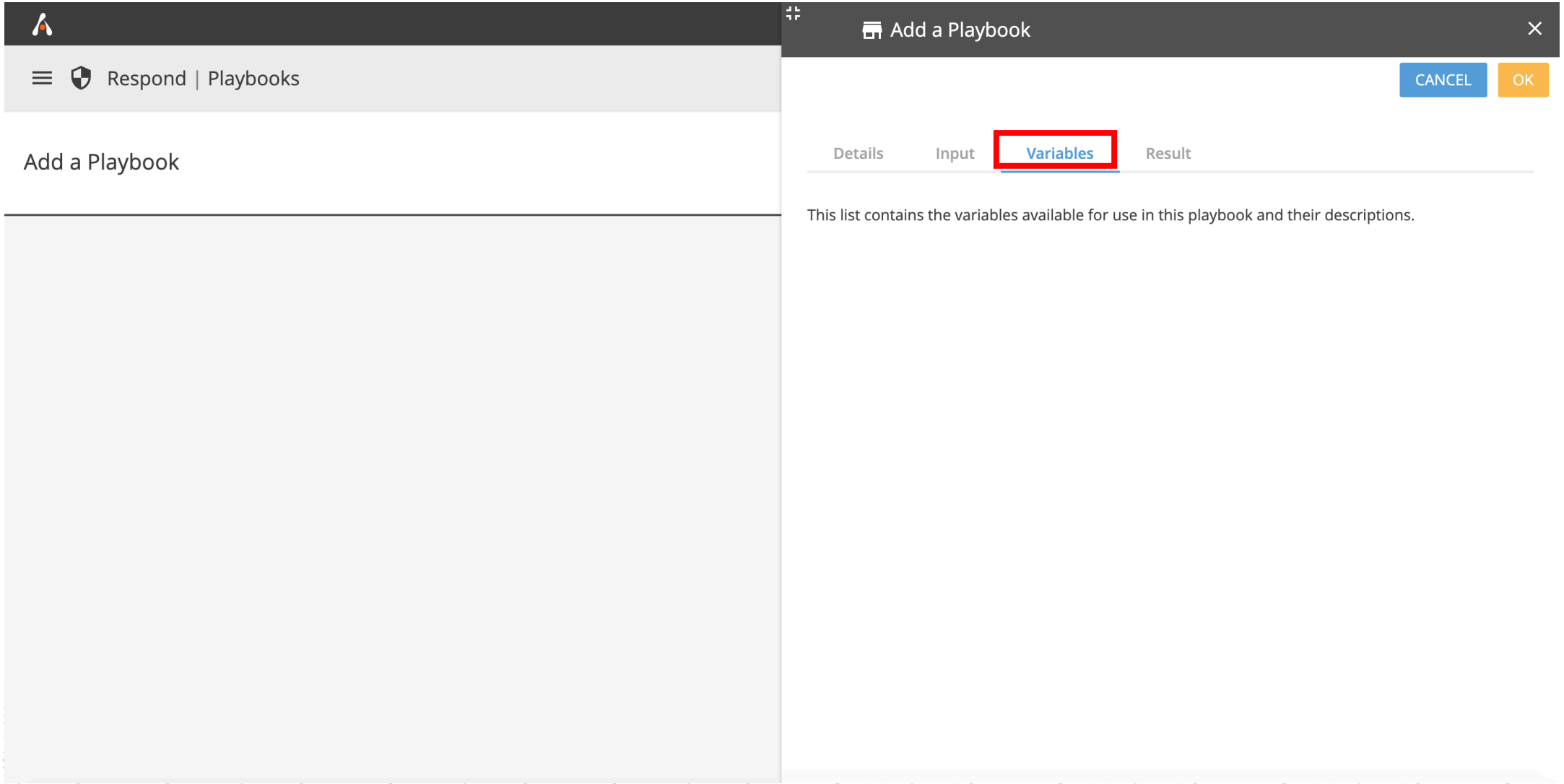
Defining the Playbook (cont)



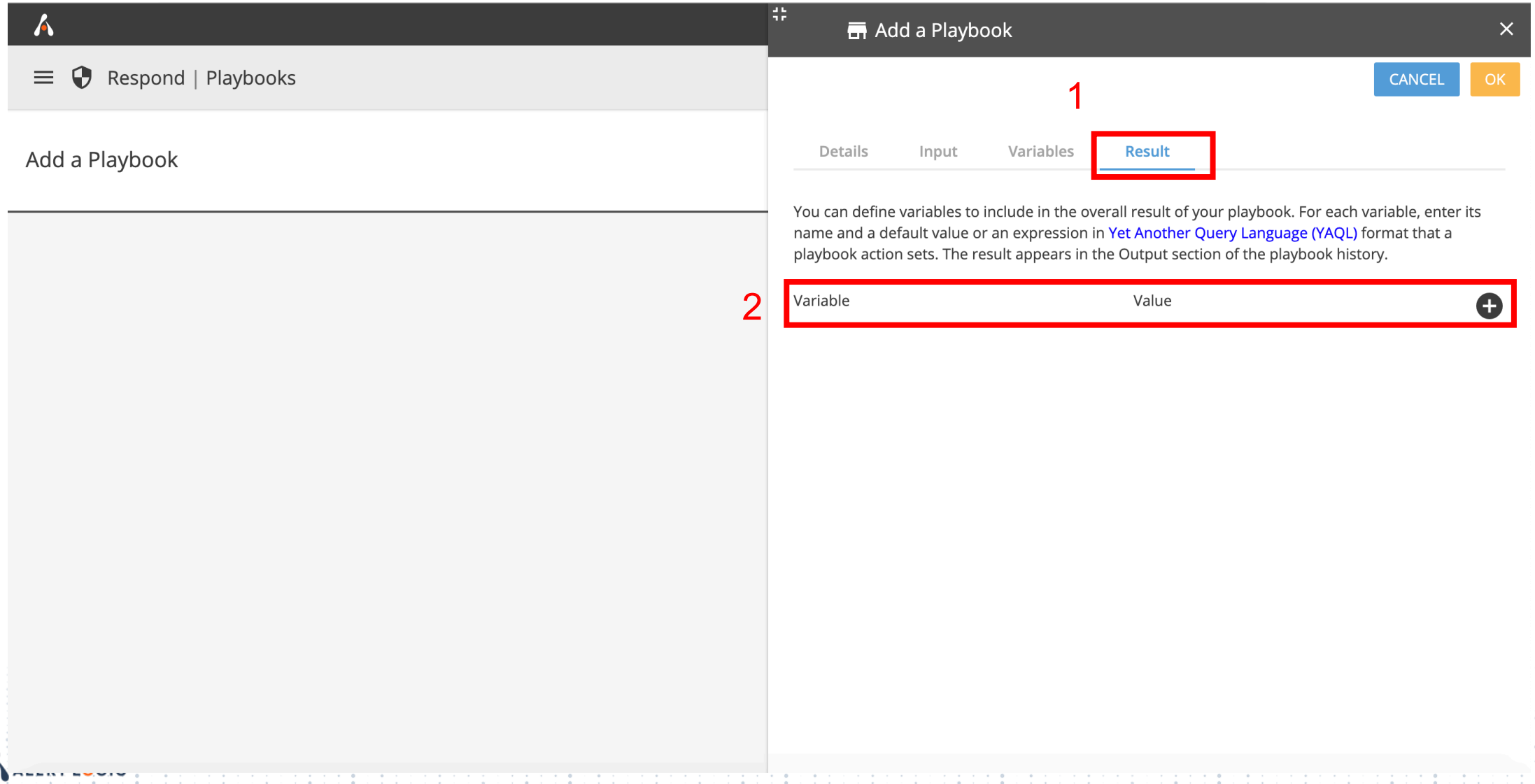
Defining the Playbook (cont)



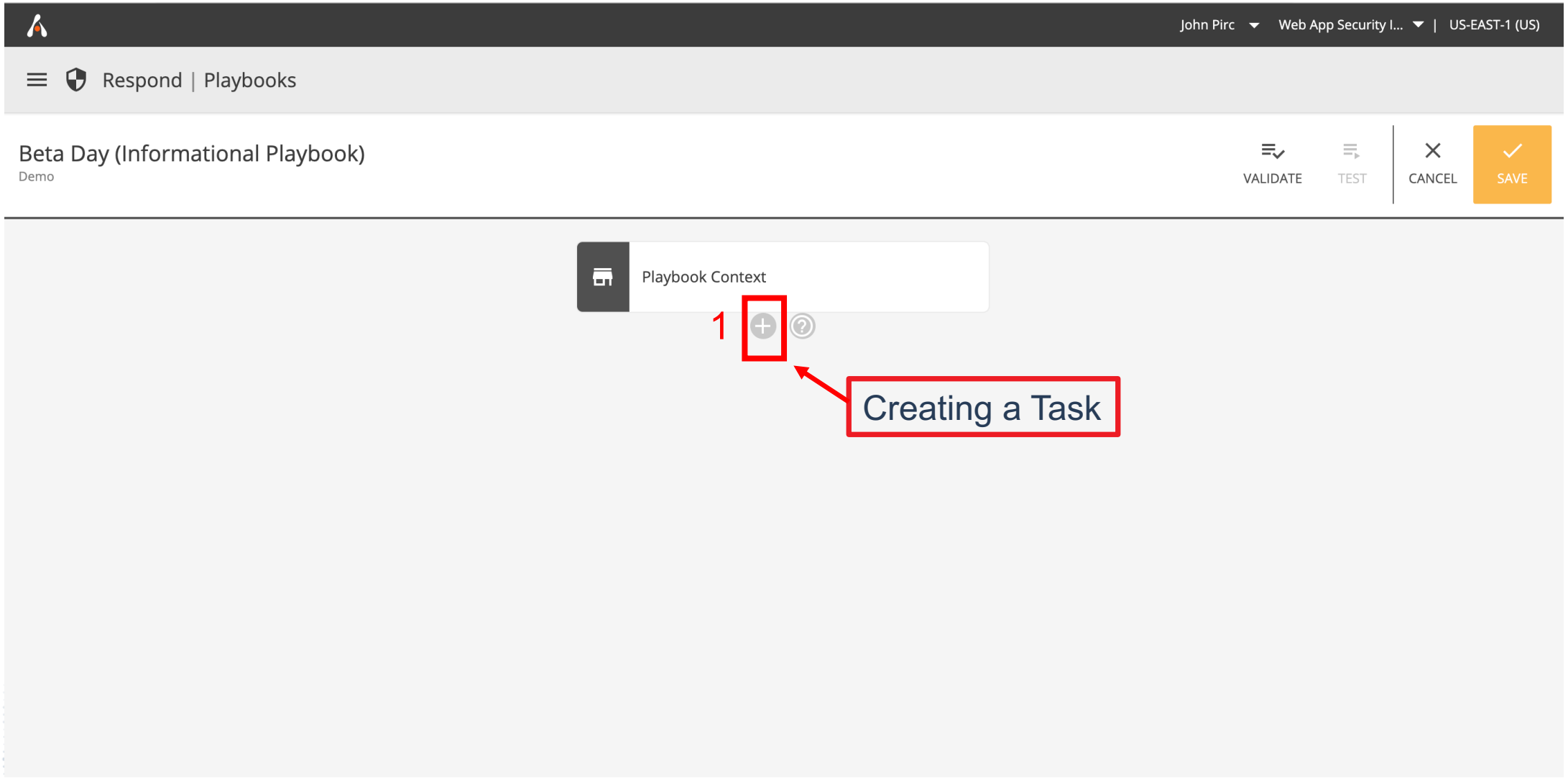
Defining the Playbook (cont)



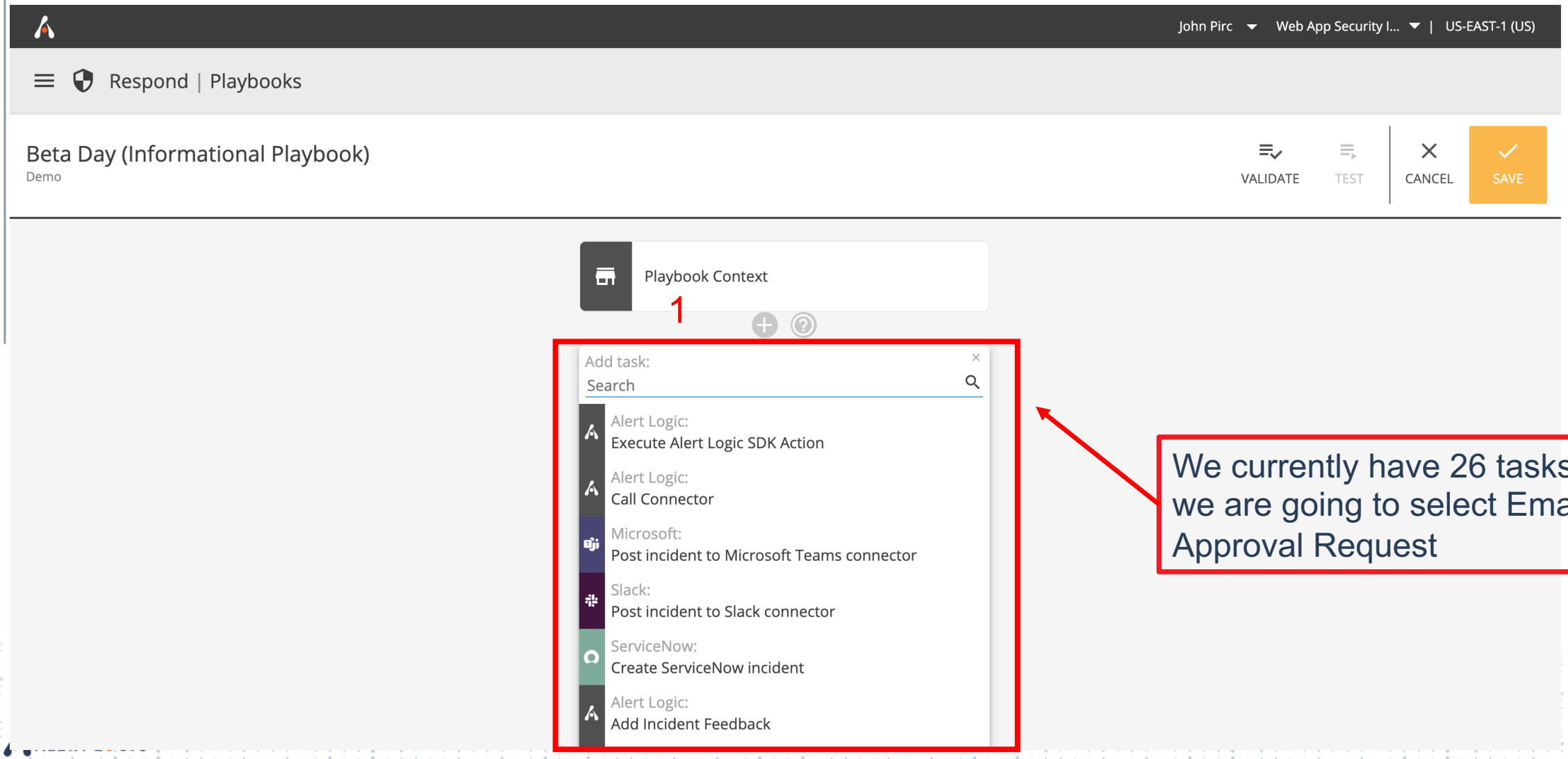
Defining the Playbook (cont)



Defining the Playbook (cont)

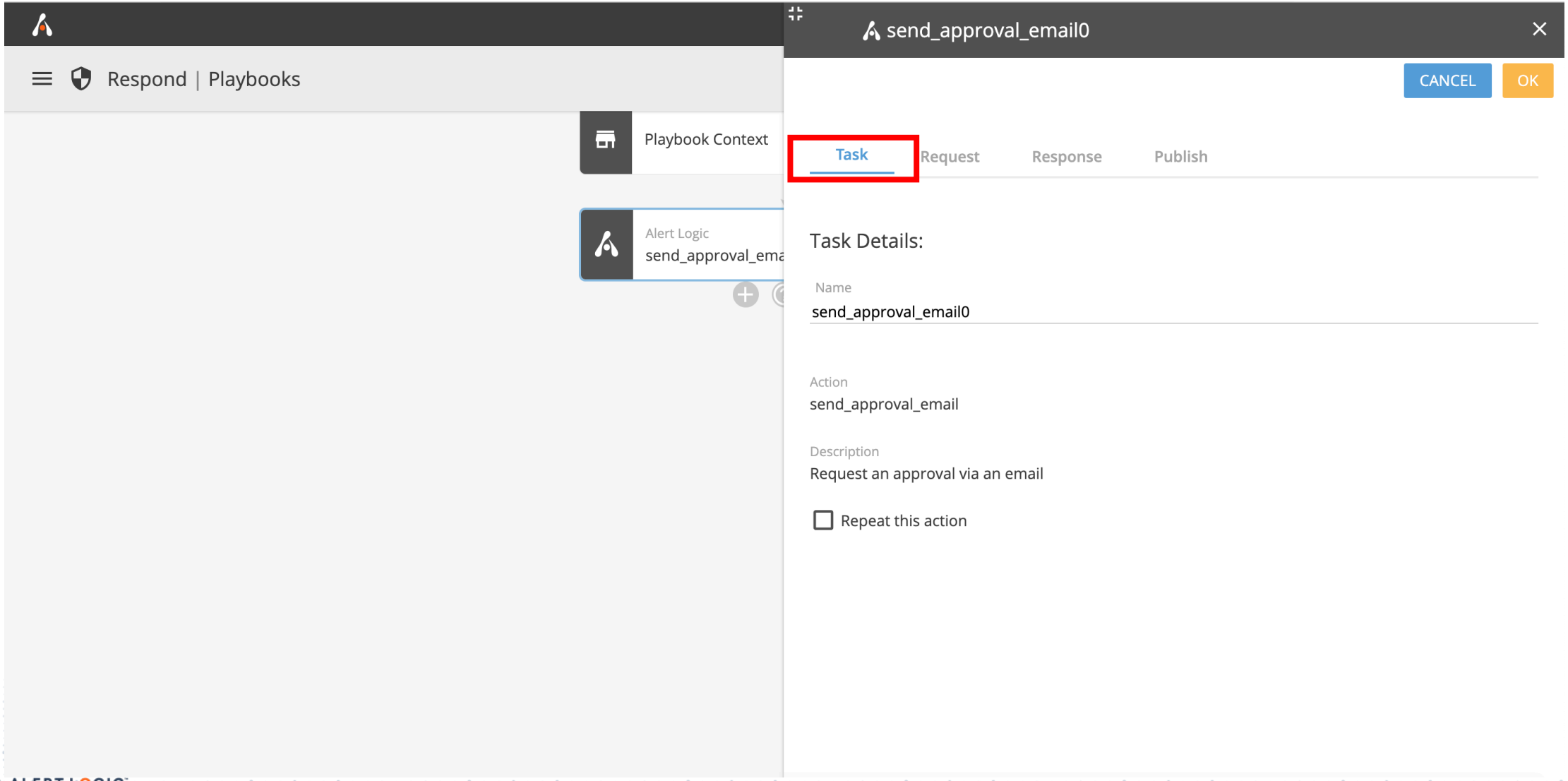


Defining the Playbook (cont)

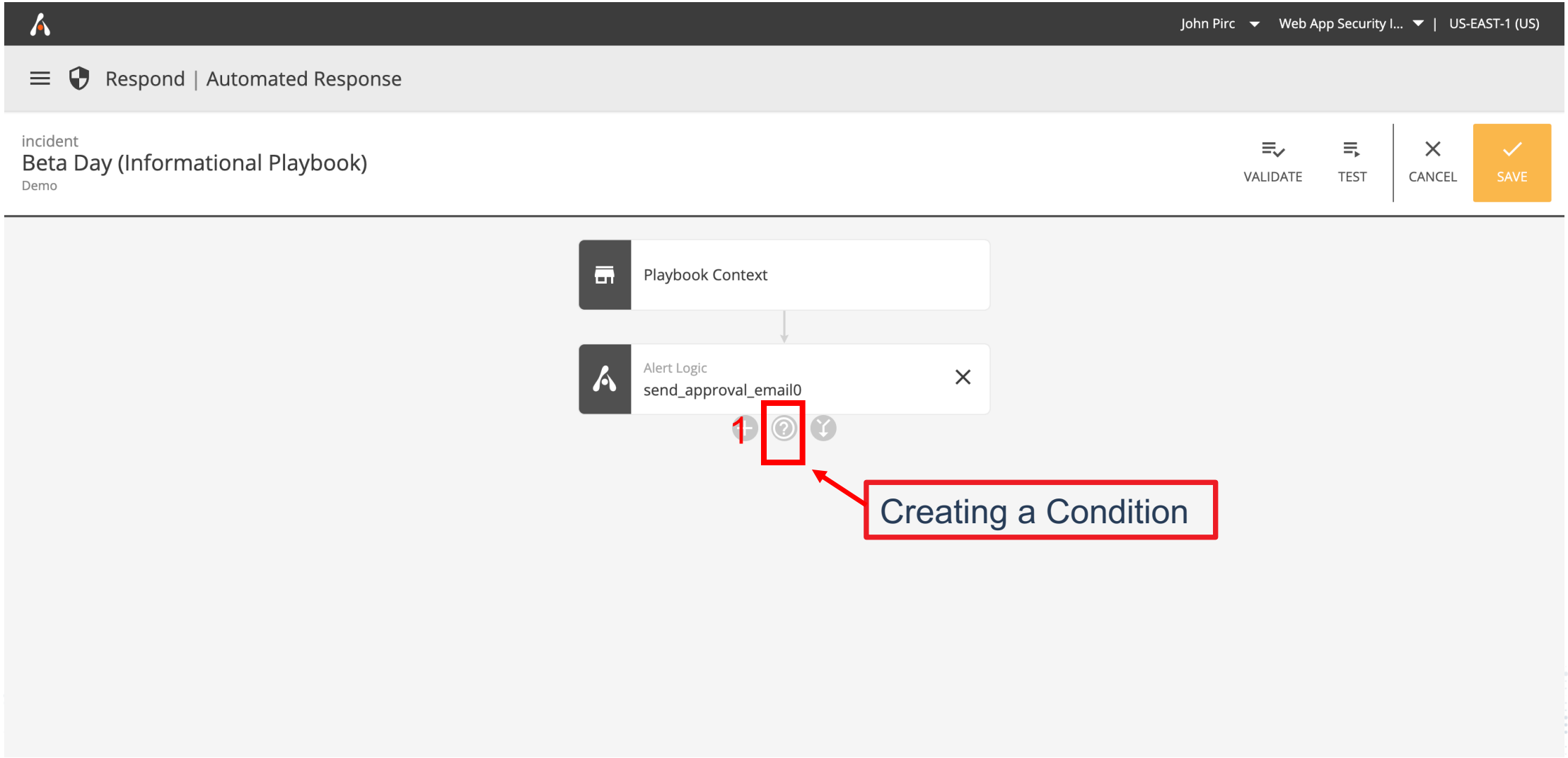


We currently have 26 tasks and we are going to select Email Approval Request

Defining the Playbook (cont)



Defining the Playbook (cont)



Defining the Playbook (cont)

Respond | Playbooks

Playbook Context

Alert Logic
send_approval_ema

Condition
<% succeeded() %>

send_approval_email0

CANCEL OK

Task Request Response

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.

2

VARIABLES

subject

3b

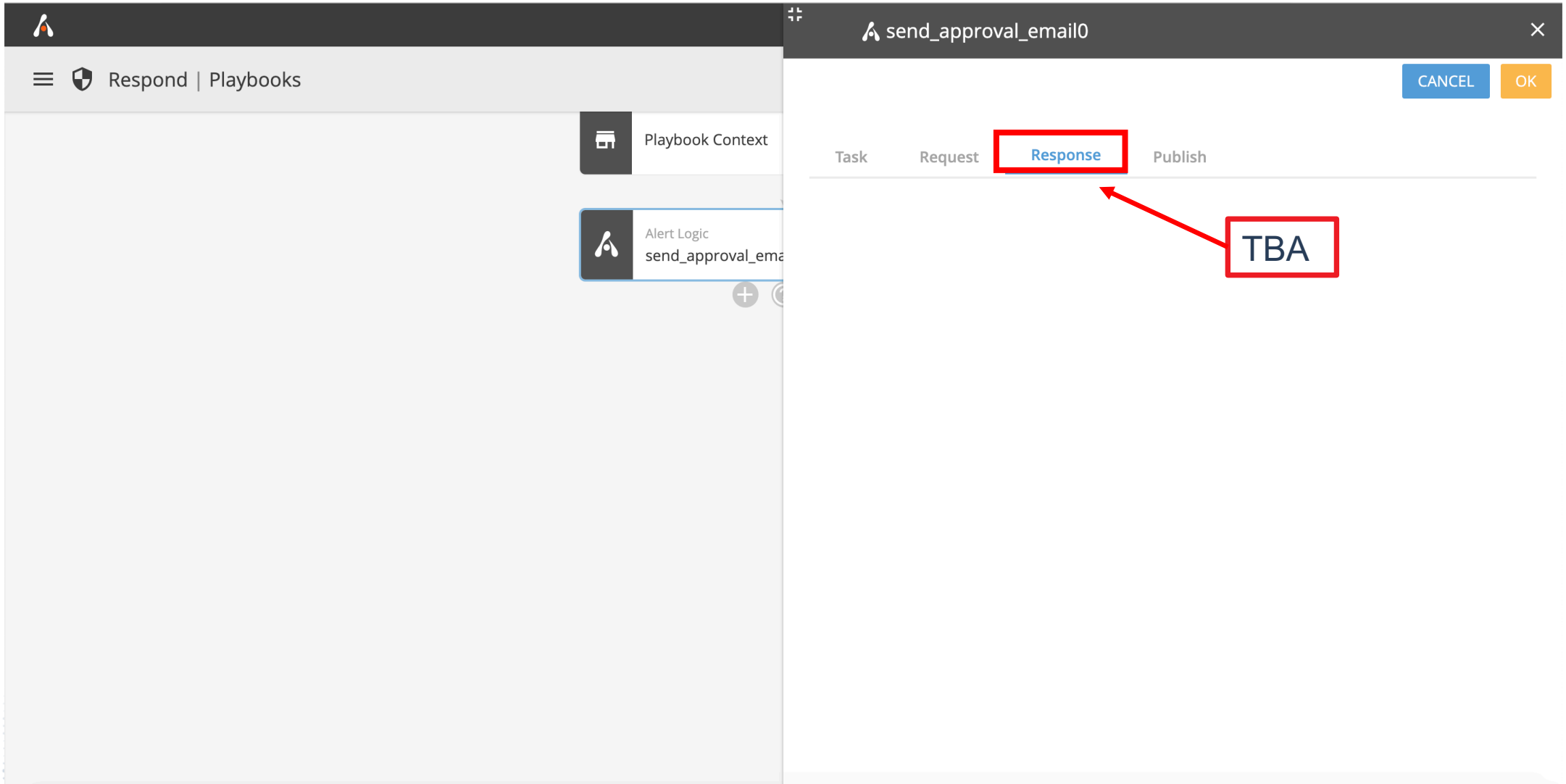
3a

VARIABLES

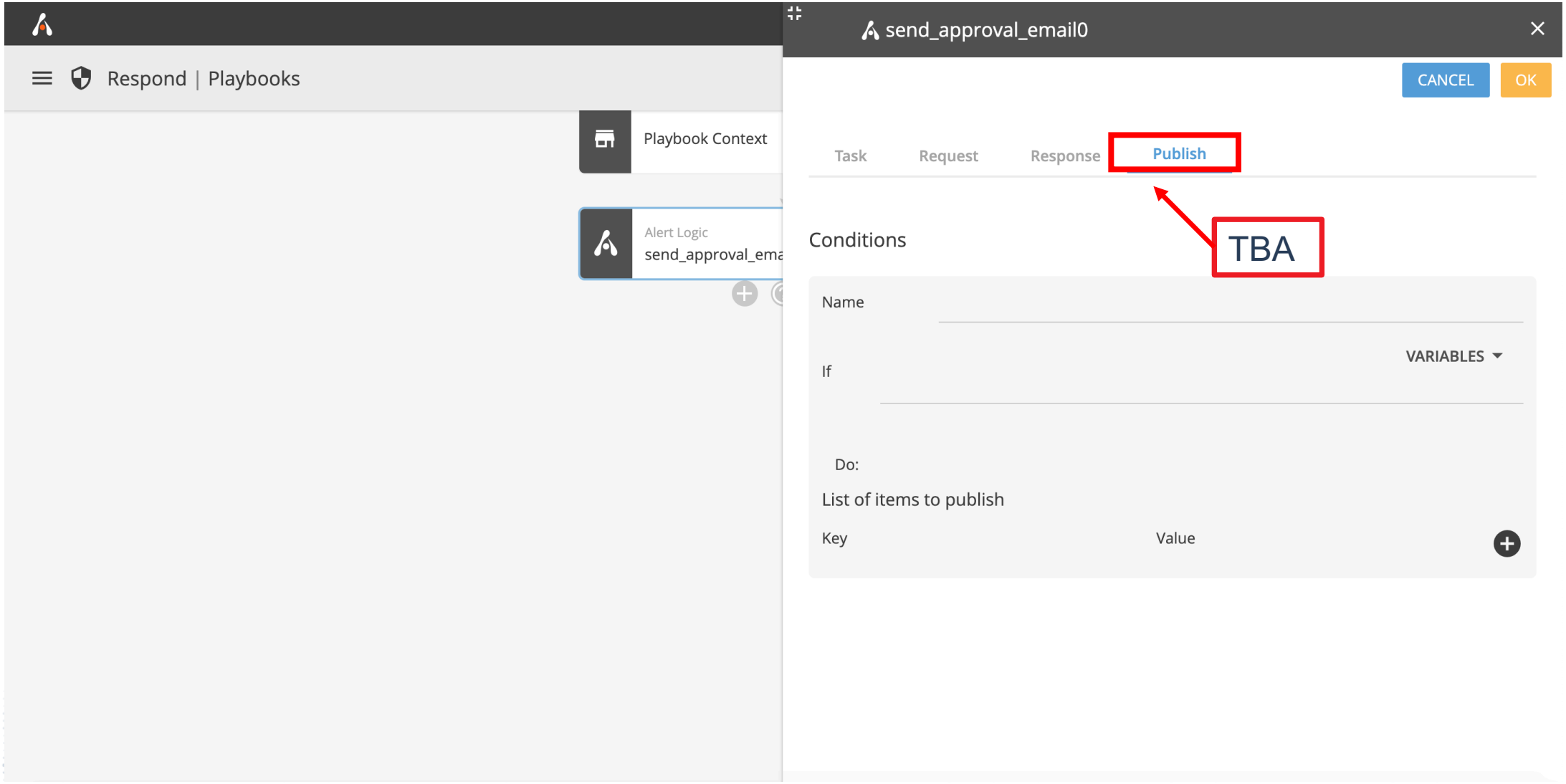
message
This IP <% ctx().payload.attacker_lset.select($.ip)%> is bad

ttl
60

Defining the Playbook (cont)



Defining the Playbook (cont)



Defining the Playbook (cont)

Respond | Playbooks

Playbook Context

Alert Logic
send_approval_ema

Condition
<% succeeded() %>

<% succeeded() %>

CANCEL OK

Conditions 1

Name Rejected 2

VARIABLES

If <% failed() %>

Search

Task default status
Success
Fail

Do: 2

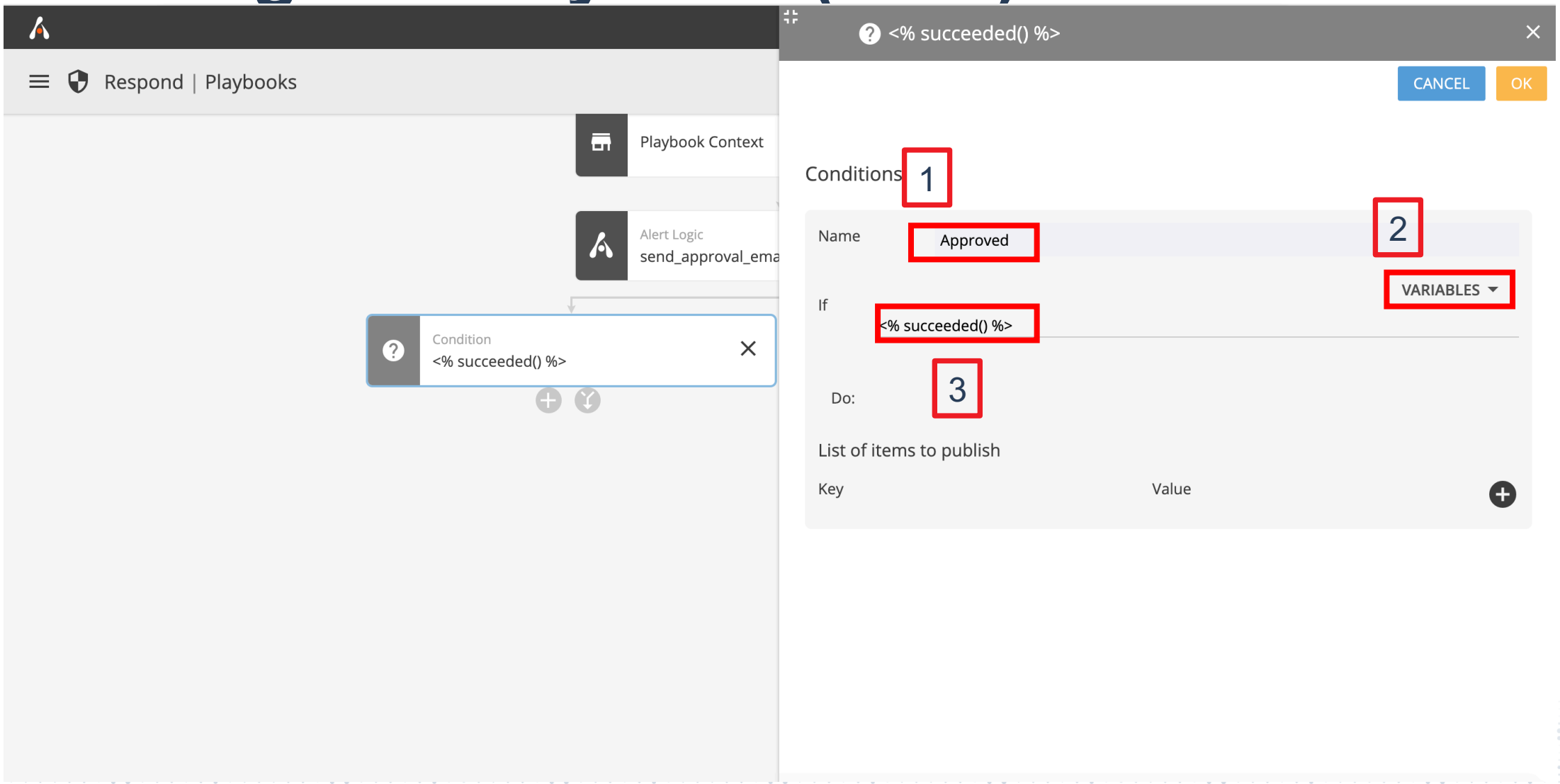
2

List of items to publish

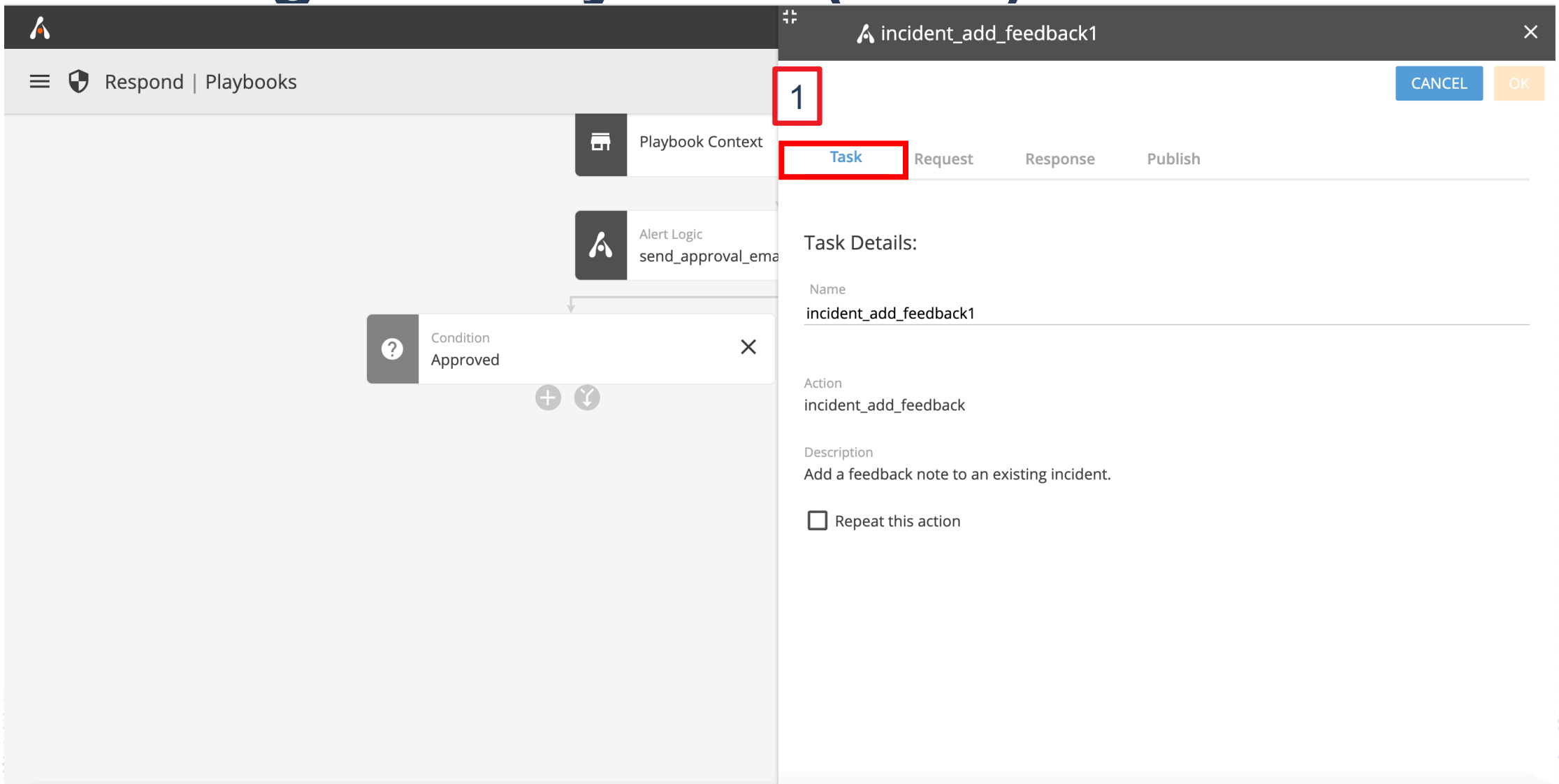
Key

Playbook Inputs
account_id
payload_type
payload
payload accountId
payload asset_deployment_type
payload asset_host_name
payload asset_native_account_id

Defining the Playbook (cont)



Defining the Playbook (cont)



Defining the Playbook (cont)

Respond | Playbooks

Playbook Context

Alert Logic
send_approval_ema

Condition
Approved

incident_add_feedback1

CANCEL OK

1

Task Request Response Publish

2

VARIABLES

account_id *
<% ctx().account_id %>

VARIABLES

incident_id *
<% ctx().payload.incidentId %>

3

3

VARIABLES

customer_feedback *
We need more information on IP <% ctx().payload.attacker_lset.select($.ip)%>

4

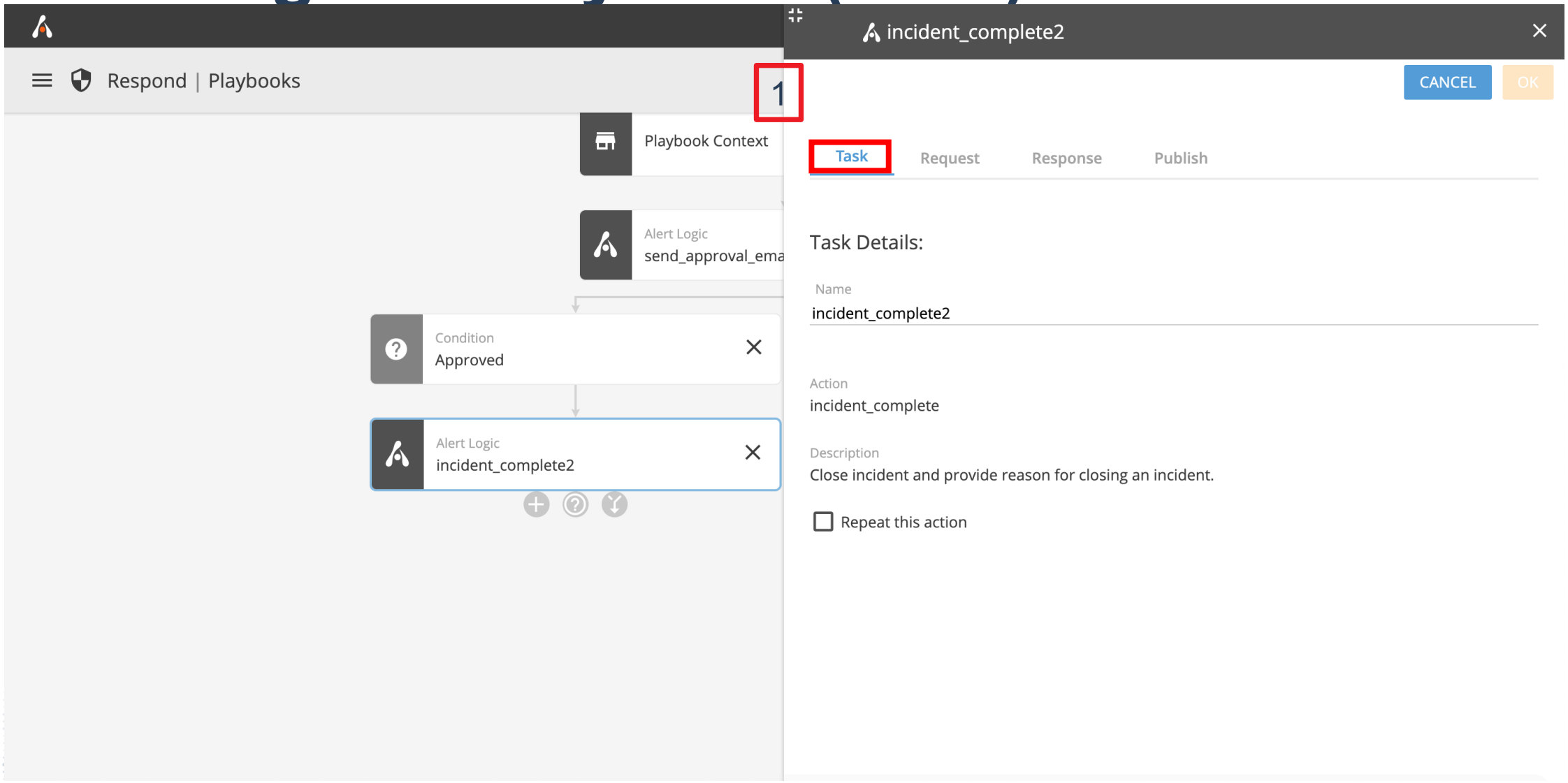
4

customer_feedback_reason

further action

further action
acceptable risk
compensating control
threat not valid
not concluded
other

Defining the Playbook (cont)



Defining the Playbook (cont)

Respond | Playbooks

Playbook Context

Alert Logic
send_approval_ema

Condition
Approved

Alert Logic
incident_complete2

incident_complete2

CANCEL OK

1

Task Request Response Publish

2

VARIABLES

account_id *
<% ctx().account_id %>

VARIABLES

incident_id *
<% ctx().payload.incidentId %>

3

3

VARIABLES

notes *
The following IP <% ctx().payload.attacker_lset.select($.ip)%> is malicious and needs to be blocked

4

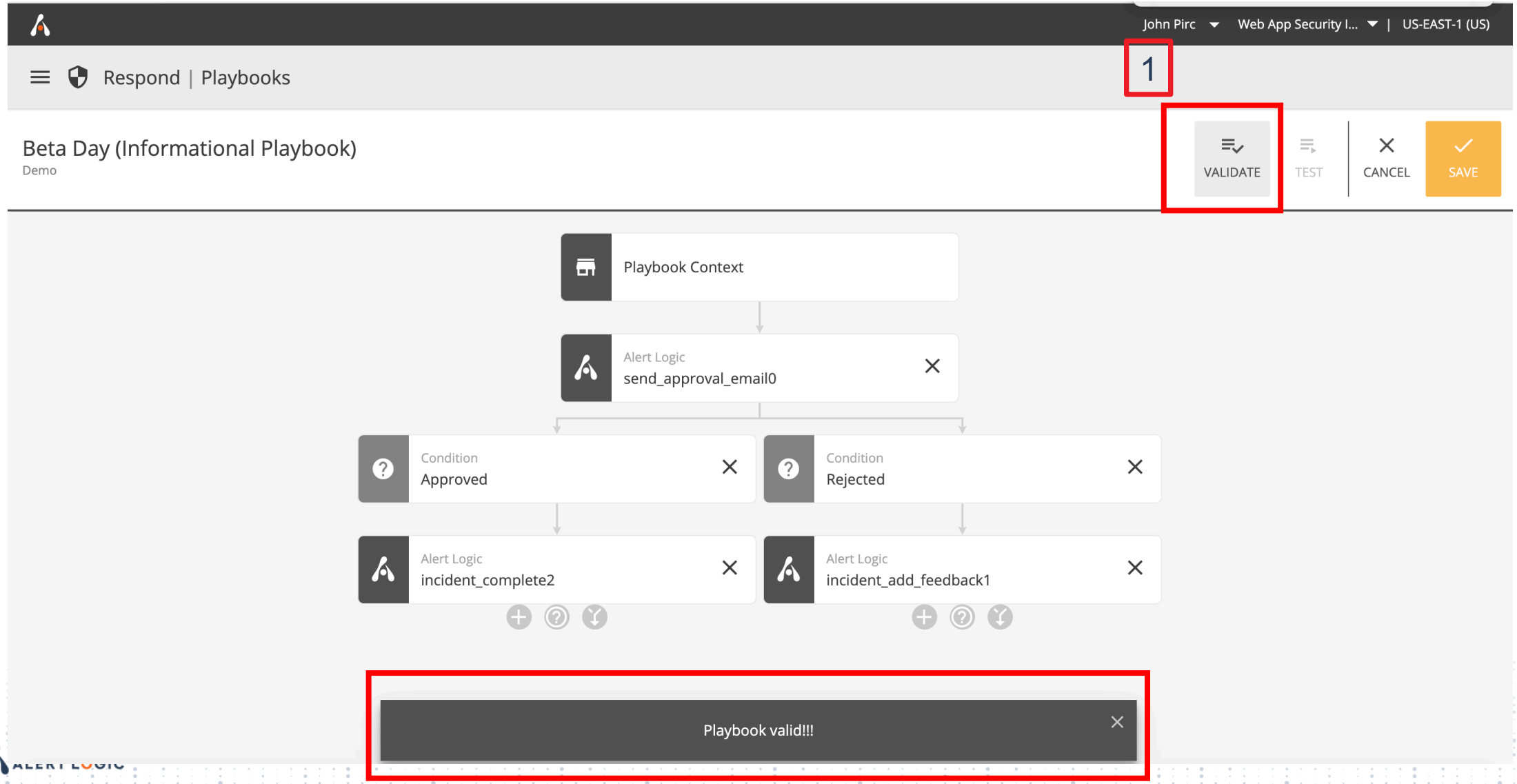
reason_code

4

acceptable risk

further action
acceptable risk
compensating control
threat not valid
not concluded
other

Validating a Playbook



Testing a Playbook

Test Playbook

CANCEL RUN

1. Payload — 2. Results

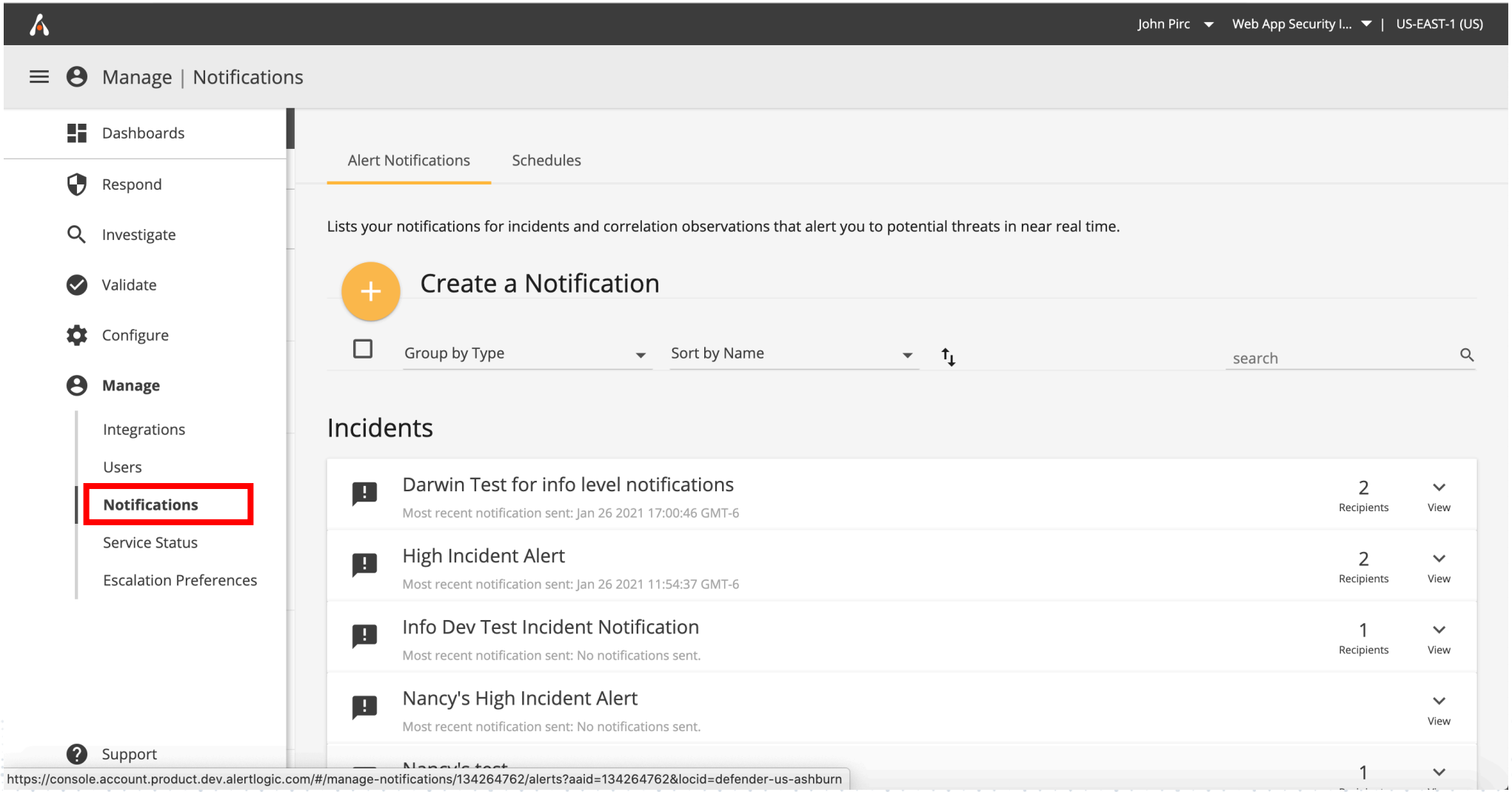
Incident Type

Incident

Incident Payload


```
{
  "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



Setting a Playbook in Motion (cont)

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

Manage | Notifications

Active 0/6

Inactive 0/7

search filters

Type
Incidents

Account
Web App Security Integration

Subscribed User
Darwin d Garcia m
Kimberly Heintschel
Nancy Wang
Nancy Wang

Subscribed Connector
ServiceNow Create Security Incident
Test webhook

Alert Notifications | Schedules

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

Create a Notification

+ Add Notification
Observation
Incident

Sort by Name

search

Select Incident

fo 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

Nancy's test
1

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.

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

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.

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)**

3

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

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

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.

Alert Logic
Incident Generated

ServiceNow
Create new Customer Service Case

AWS
AWS WAF Block

Conditions
If Succeeded

Conditions
If Failed

ServiceNow
Update Customer Service Case

Alert Logic
Send Notification

Alert Logic
Close Incident

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

search filters

Type
Incidents

Account
Web App Security Integration

Subscribed User
Darwin d Garcia m
John Pirc
Kimberly Heintschel
Nancy Wang
Nancy Wang

Subscribed Connector
ServiceNow Create Security Incident
Test webhook

Alert Notifications | Schedules

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

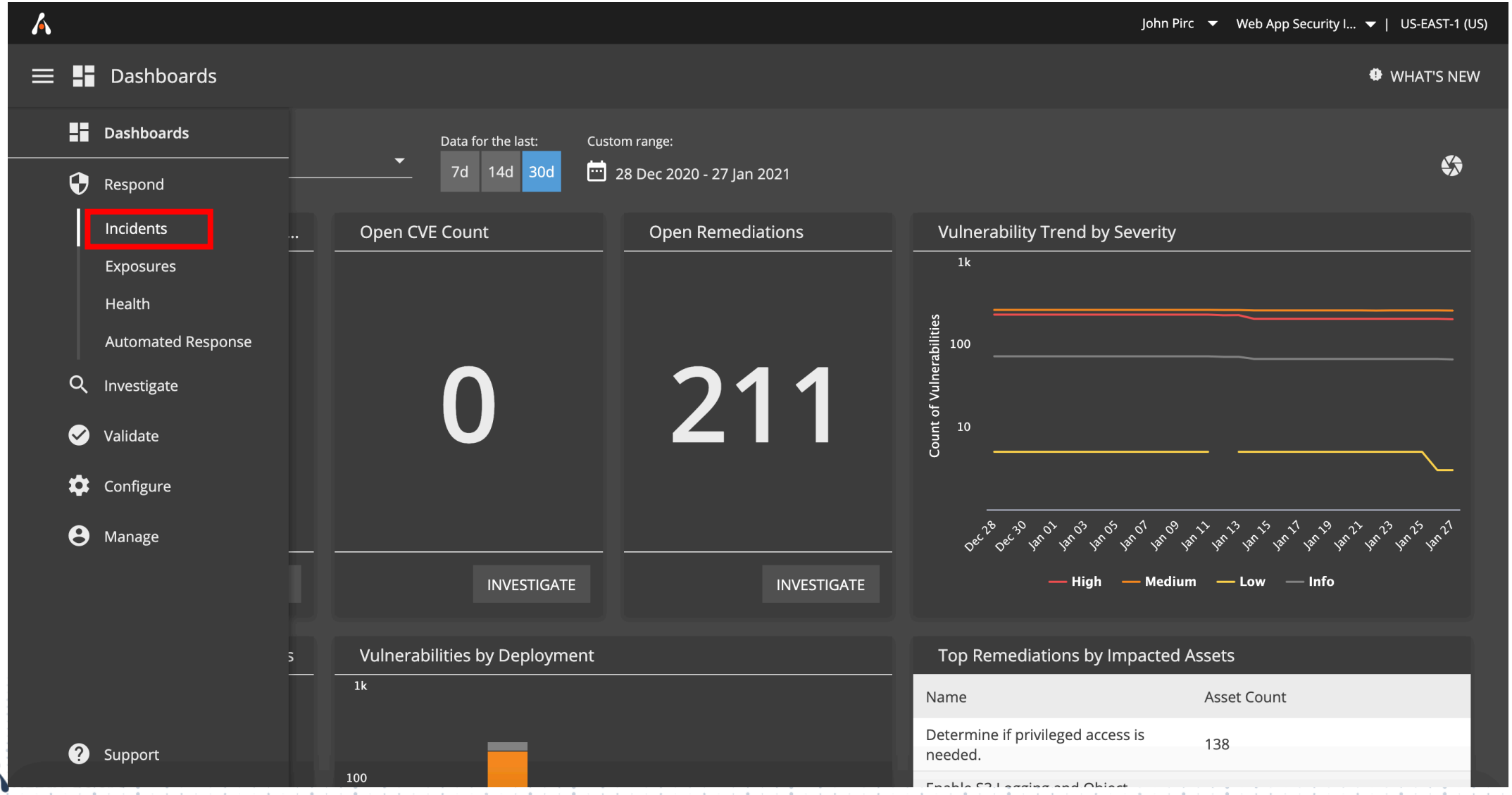
Create a Notification

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

Running an on-demand Playbook



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

1

Date	ID	Summa	Thre	Class	Dete	Corr	Incid	Depl	Acco	Attac	Target
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	WLA Integration Log Source	Web App Security Integration	7.33.6.77	suitablekid.com
26th Jan 2021 11:24	38jr5b	SQL Injection, Null Byte, Path Trave	Medi	application-	Web Log Analy		0	WLA Integration Log	Web App Security	35.6.0.4	suitablekid.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

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

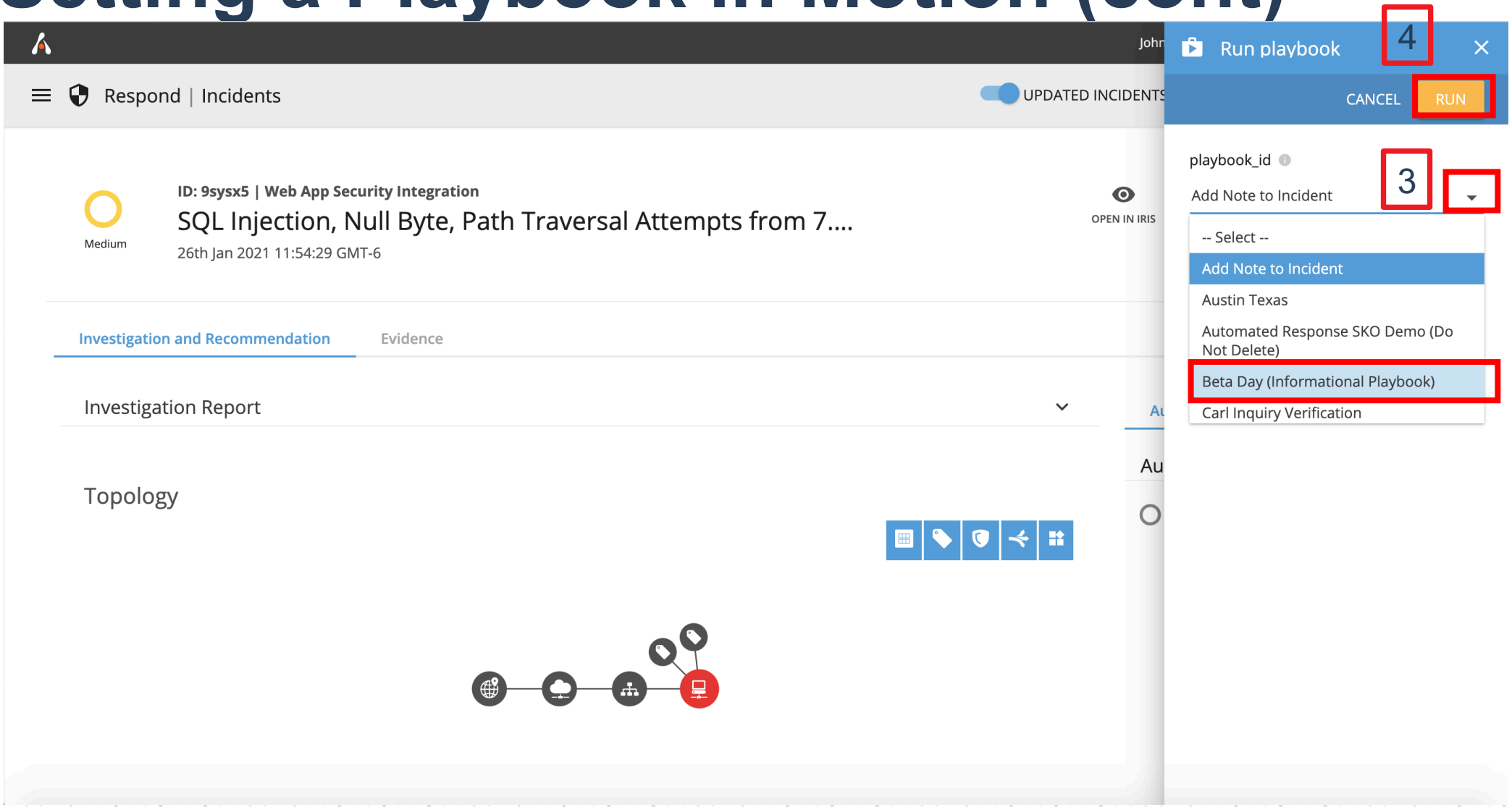
Topology

Audit Log | Notification History

Audit Log

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

Setting a Playbook in Motion (cont)



Setting a Playbook in Motion (cont)

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

Topology

Audit Log | Notification History

Audit Log

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

Executing the Response Action (Email)

Alert Logic MDR Approval Request

AL

Alert Logic Dev no-reply <no-reply@product.dev.alertlogic.com> Today at 6:04 PM

To: Pirc, John

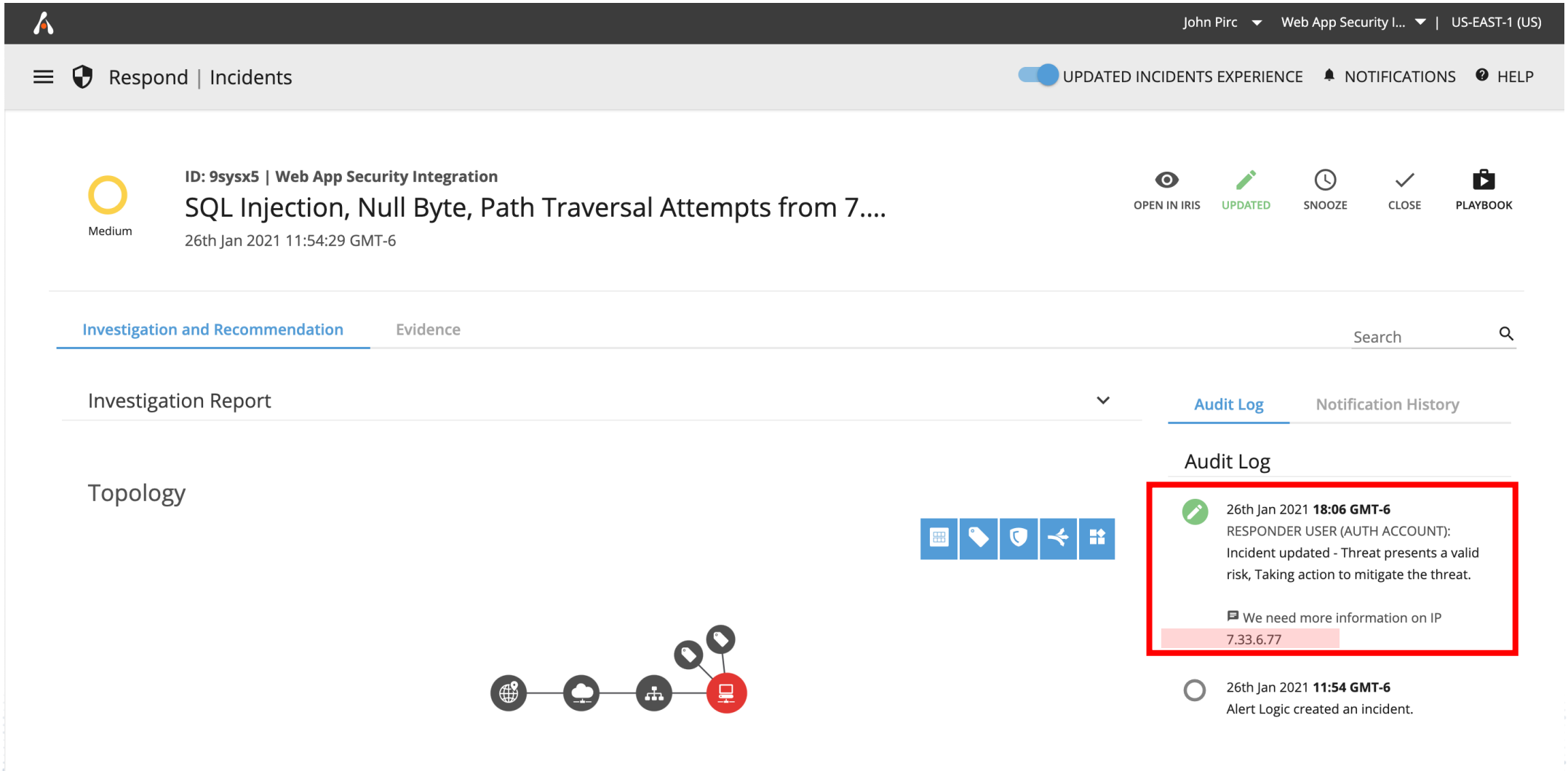
Hello Alert Logic MDR Customer,

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



Playbook History

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

Respond | Automated Response

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

- 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

Deployment
- WLA Integration Log Source 521

Playbook Execution History

25 Jan 2021 - 26 Jan 2021

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

1

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

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-8E91-148AFB043402

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

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"
```


Logs

Inquires (Pending Playbooks)

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

Respond | Automated Response

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

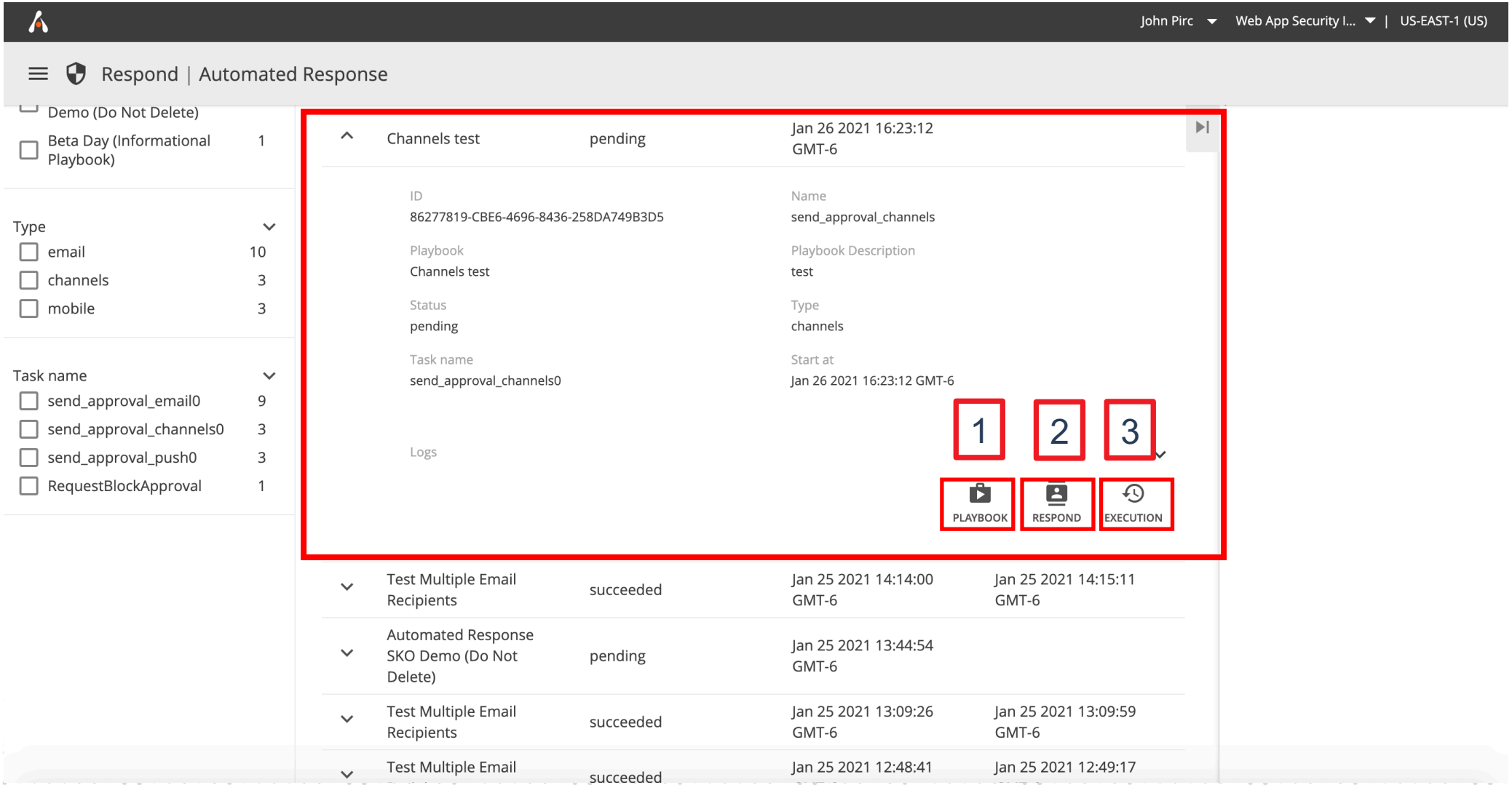
Task Name
send_approval_channels0

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)



Questions

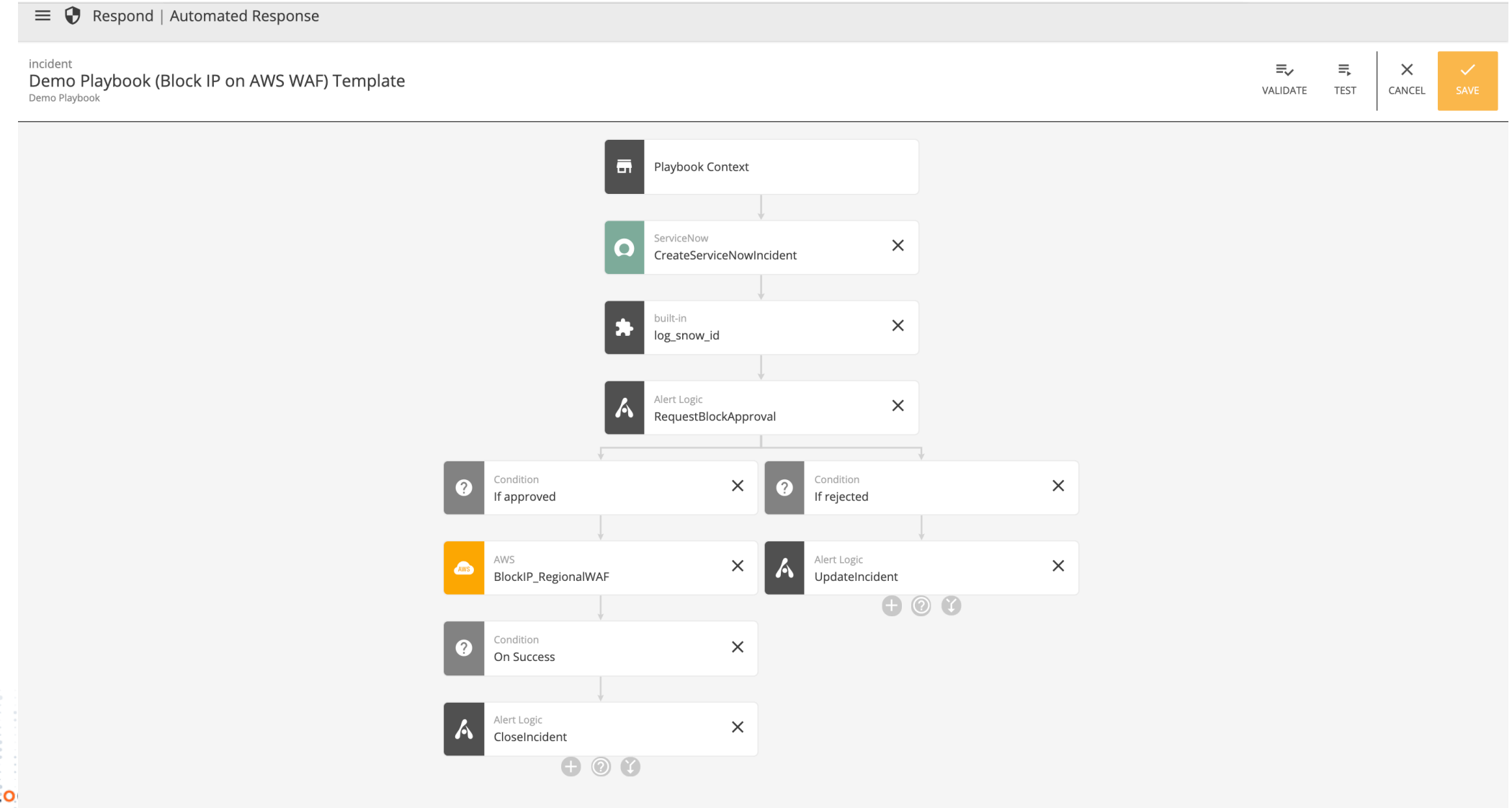
Resources

- 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

ALERT LOGIC™

Thank You

Simple Workflow



Complex Workflow