Supercharging Alerts Using Dassana

Alert contextualization and risk prioritization open source solution.

Gaurav Kumar (GK)

Founder & CEO, Dassana

Current approach and challenges

Prioritization based on vendor assigned severity

Challenges

Still too many alerts
No Business context

Let’s change default severity

...based on context

Try expressing these:

“For the dev environment, crypto and visibility related alerts have low severity“

Resources with tag “pci” must have high severity for firewall related issues

Which approach is better?

Vendor X - CSPM/CWPP
Vendor Y - Threat Detection
Vendor Z- Vuln Scanner

1

VendorX	VendorY	Vendor Z
Make Changes	Make Changes	Make Changes

2

VendorX
VendorY
VendorZ

Aggregate/Normalize

Vendor X
`tags.key==env and tag.val=pci, sev=high,policy=Foo`

Vendor Y
`tagsSet.name==env and tagsSet.val=pci, sev=high,policy=Bar`

Vendor Z
Doesn't support tags :(

Next, let’s talk about..

Resource Context

For resource A, tell me X, Y and Z.

given ec2 instance, tell me its internet exposure

Policy Context.

open s3 buckets are bad, but not so bad when they have a website associated with them.

Security groups open to the internet are bad, but not so bad when they are connected to Load Balancers etc

The need for an open source alert *normalization*, *contextualization* and *prioritization* framework

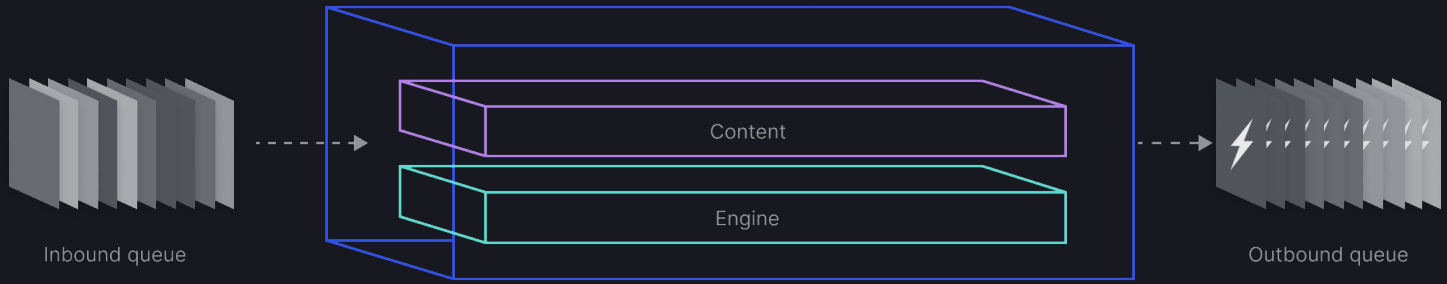
Introducing...

Dassana

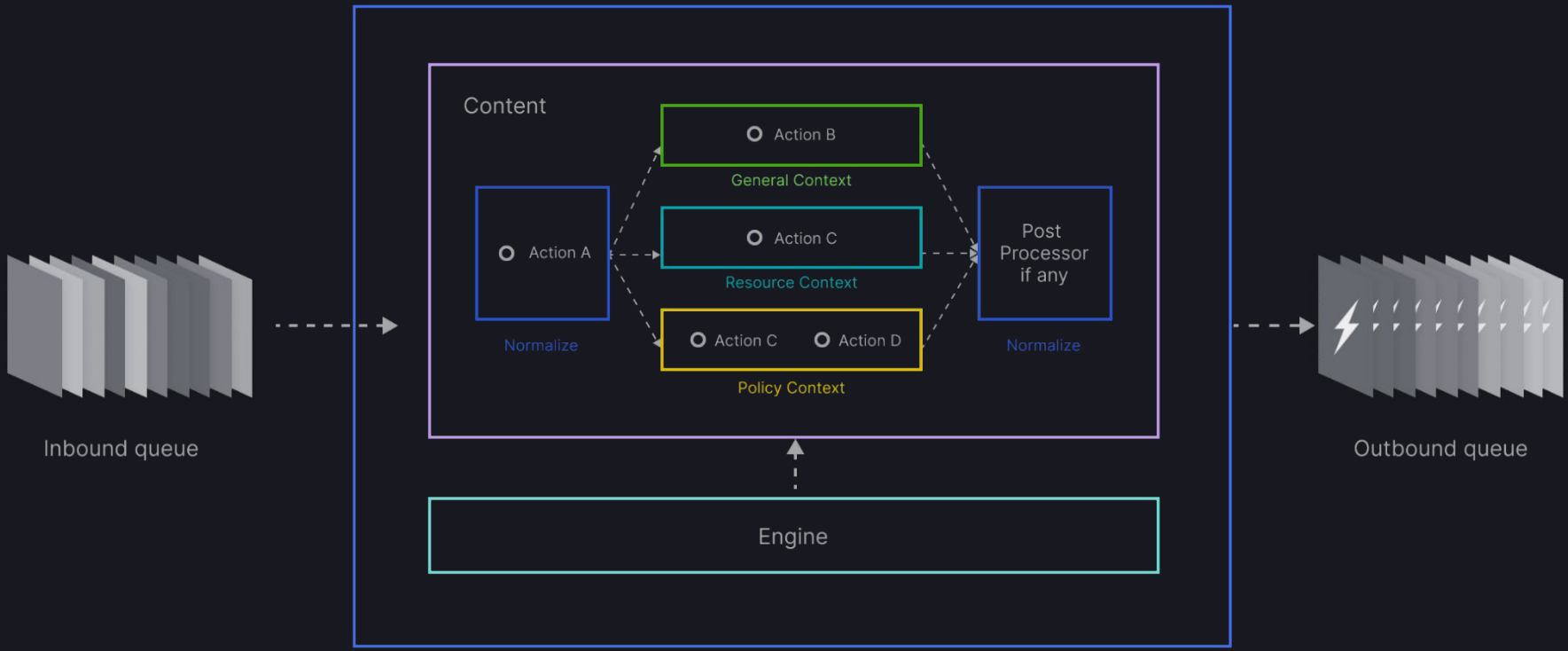
Deployment

- CloudFormation Template
- Multi Account Support
- Serverless
- Declarative
- Alert Vendor Support
  - Risk
    - CSPM
      - AWS Config → Security Hub
      - Prisma Cloud (Due Sep 20, 2021)
    - Vulnerability Scanners
      - TBD
  - Incident
    - Guard Duty → Security Hub
- CSP Support
  - Azure (Due Q4 2021)

Dassana Implementation



What does the Engine do?



Summary

- Alert prioritization tool
- Prioritization is done by adding context
  - General Context
  - Resource Context
  - Policy Context
- Dassana Actions (serverless functions) bring context

Upcoming features

- IAM context
  - Using CloudSplaining, Access Analyzer etc
  - How exposed the resource is?

- IAC context
  - Which PR created this resource?
    - Add a comment to the PR

Try it out!

https://github.com/dassana-io/dassana