

Open Source

OpenCDR/

Event-driven Cloud Detection & Response for AWS

OpenCDR is an open-source system that turns AWS security events into actionable detections and automated responses.



DETECT

Process AWS events
in real time.



RESPOND

Automate response
actions.



OPEN SOURCE

Transparent and
community driven.

Key capabilities



Real-time detection
Process AWS events as they happen.



Configurable rules
Create and customize detection
and correlation rules.



Automated response
Take action with built-in responders
or custom playbooks.



Native AWS integration
Built with AWS services and
security best practices.

Use cases



Identity and access
User, role and key abuse.



Data protection
Public S3/RDS, sensitive data access.



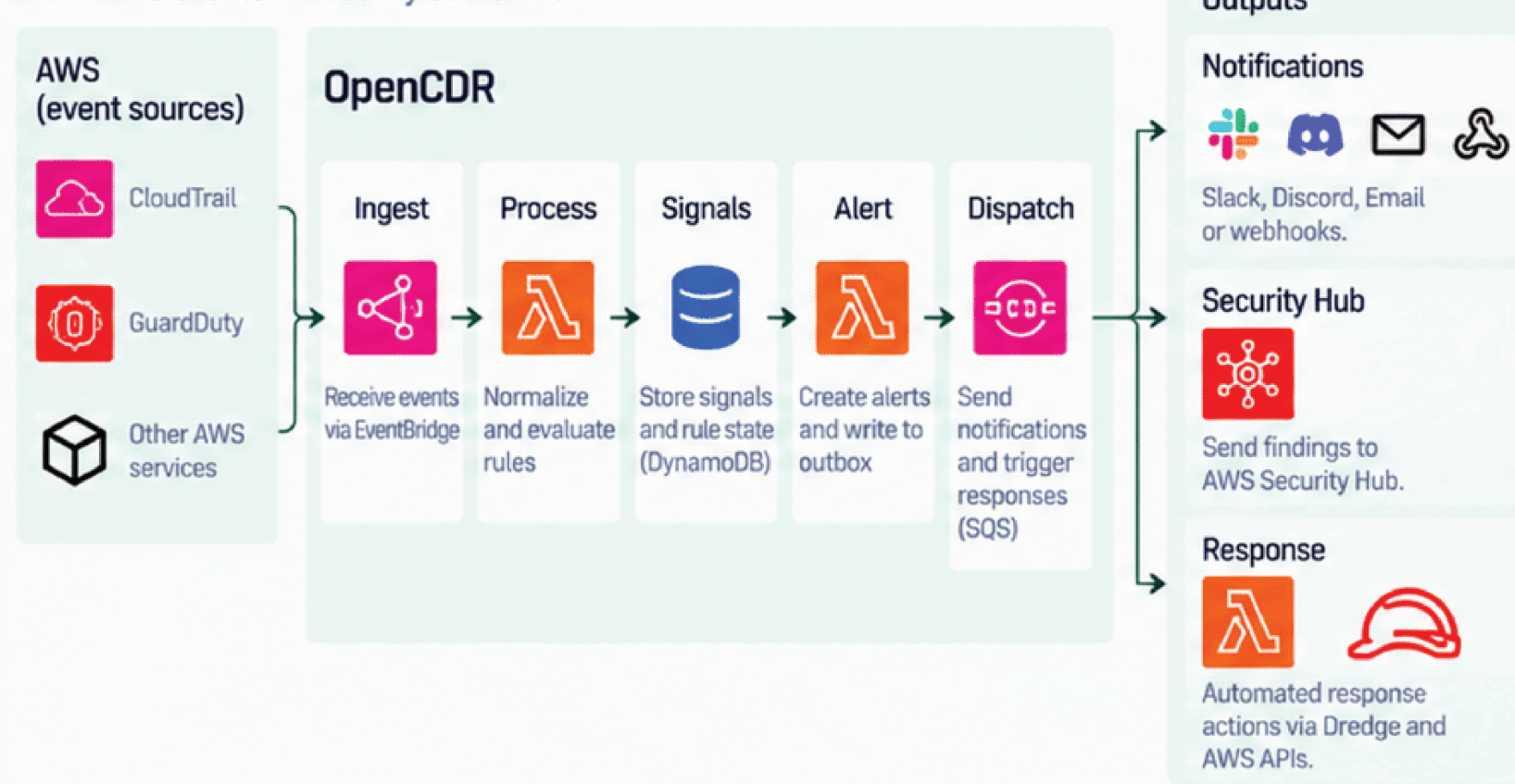
Threat activity
Defense evasion, persistence, discovery.



Infrastructure
Risky configuration changes.

Architecture

From AWS events to security outcomes.



Detection examples



CreateAccessKey
Detect and respond to
new access keys.



Disable or delete logging
StopLogging, DeleteTrail,
GuardDuty changes.



Public data exposure
S3 bucket made public,
RDS public access.



Privilege escalation
AssumeRole, PassRole,
new admin users.



Suspicious activity
Unusual API patterns,
defense evasion techniques.

API

Query and respond, even beyond detections.



- Query signals, alerts and logs
- Manage rules and configuration
- Trigger response actions (on-demand)
- Integrate with custom tooling and workflows

```
curl -X POST https://api.opencdr.local \
-H "Authorization: Bearer <token>" \
-H "Content-Type: application/json" \
-d '{
  "action": "disable-access-key",
  "key_id": "AKIA..."
}'
```

Open source



github.com/dbnz-io/opencdr



Code, rules and
contributions
are welcome.