
aws
SUMMIT
ONLINE

SEC01

Cloud-enabled security evolution with Origin Energy

Christoph Strizik
Chief Information Security Officer
Origin Energy

Glenn Bolton
Security Lead for Cloud
Origin Energy

aws SUMMIT ONLINE

Agenda

Our journey

Your journey starts here

Origin's energy and purpose

Our security principles

Three focus areas for transformation

Your action plan

Goodies

Our Purpose

Getting energy right for our customers, communities and planet

Leading energy retailer

4.2 million gas, electricity and LPG customer accounts

Growing renewables and storage supply

From ~19% of Origin's owned and contracted generation capacity today to more than 25% by 2020

Significant generation portfolio

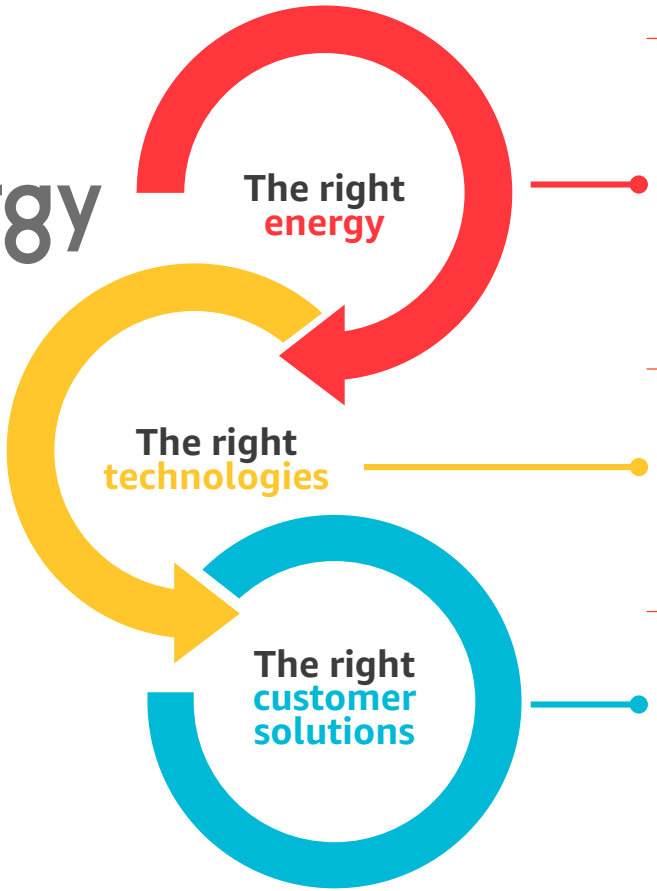
~7,500 MW with fuel and geographic diversity

Supplier to domestic and export markets

- Supplier of ~30% of domestic east coast gas demand in FY2019

Our business strategy: connecting customers to the energies and technologies of the future

good energy



Accelerate towards clean energy

Low cost operator developing and growing gas resources

- Business strategy required a reset of our technology and security strategies.
- Required level of cost, customer experience, security difficult to achieve in old school models.

Embracing decentralised and digital future

- We embraced public cloud.
- Moving to public cloud is a once in a generation opportunity to transform organisation and security

Leading customer experience and solutions

Our Security Mission

Continuously improve Origin's security resilience and safeguard our critical assets

How our strategy connects to Origin's purpose…

Getting energy right for our customers means safeguarding their data and the services we provide for them.

Getting energy right for our communities and planet means safeguarding our production assets to ensure reliable and safe energy supply.

Our Security Principles

1. We use every stakeholder interaction as an opportunity to help and create a **stronger security culture.**
2. We focus on providing **holistic, timely, risk-based** security solutions and advice.
3. **We use security metrics** to drive **continuous improvement** of security controls and culture.
4. We **give back** and work with partners, industry and regulators to achieve a broader security uplift.
5. We hold ourselves accountable through **regular independent assurance.**
6. We **leverage our network** to Government and peers as a force multiplier to Origin's security.
7. We use Open Source, cloud and automation to **scale and maximise security value at low cost.**

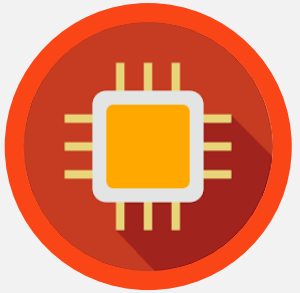
Identify the areas for transformation

Understand Business & IT Strategy

Define security principles

Identity capability gaps

#1 Security skills, competencies



#2 Reinvent security tech stack

#3 Improve security transparency

Transform - #1
Security skills and competencies

Why did we have to change?

Our competency was governing outsourced security services.

We had to learn how to build and run cloud security solutions at scale.

What we did:

Recognise barriers – talent, turnover, diversity.

Hired great people from different fields.

Training program & experimentation.

Promoted people with strong leadership but limited security skills.

Set up every role as flexible.

Transform - #1
Security skills and competencies

The outcome:

Diverse, skilled team that builds and runs Origin's security stack in the cloud.

Female participation:
30%
Average: 10%.

People turnover:
5%
Average: 20%.

Engagement score:
79%
Average: 61%.

Winning awards

Origin's IAM team, led by Vanessa Gale, won the **Saviynt innovation award**

Sources of stats:
https://workplaceinfo.com.au/hr-management/hr-strategy/analysis/one-in-three-workers-disengaged-what-can-you-do
https://www.afr.com/technology/showing-girls-cyber-security-not-just-a-boys-club-20180808-h13ptt
https://go.demisto.com/hubfs/Resources/2018%20SOAR%20Report/SOAR%20Report%202018.pdf

Transform - #2
Reinvent security tech stack

Why did we have to change?

Scaling our existing security stack would have significantly increased our cost and not enabled our security principles (timely, holistic, metrics-driven stack etc).

What we did:

Cancelled our managed security services contract and gave us a deadline to transform!

Created a completely new security stack in the cloud.

Leveraged native cloud security controls and open source where possible.

Transform - #2
Reinvent security tech stack

The outcome

Security monitoring costs dropped by 81%.

New monitoring use cases take minutes to set up instead of weeks.

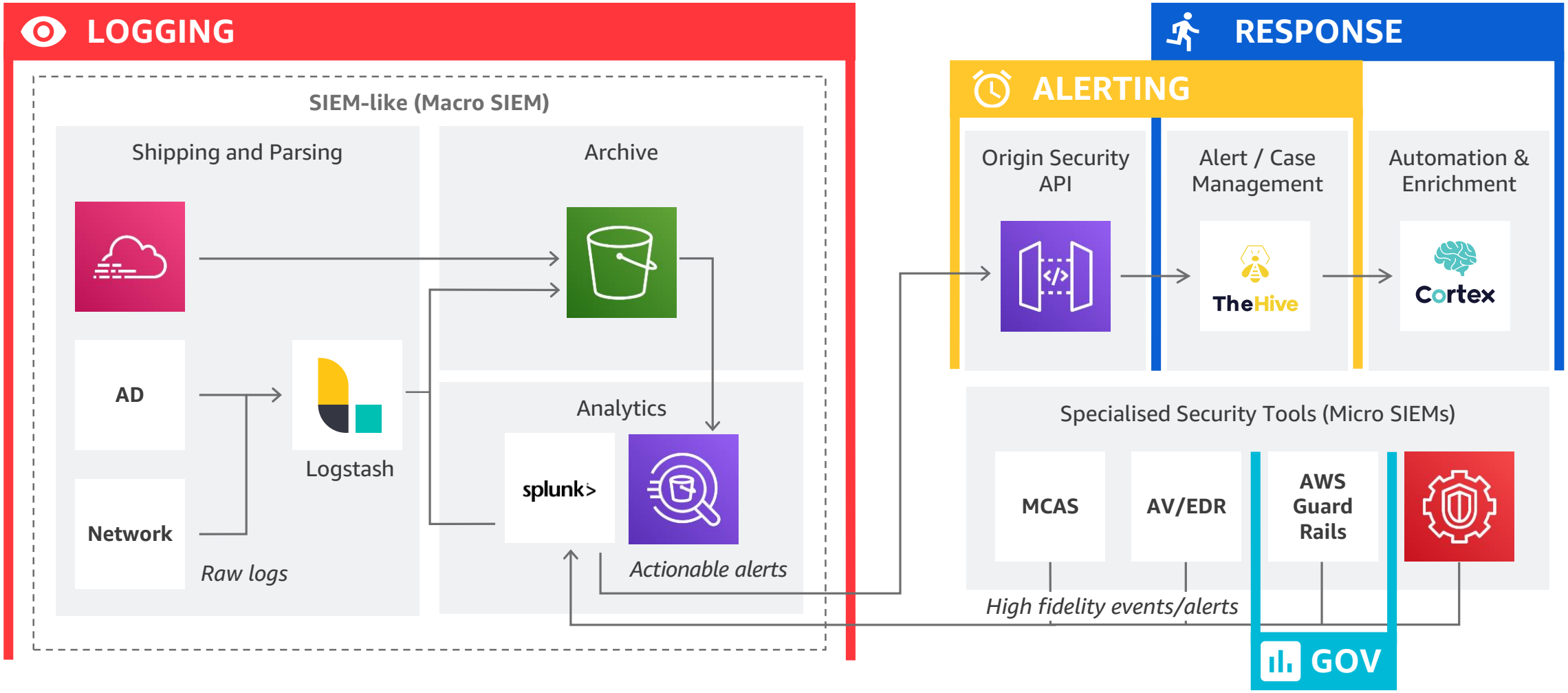
From quarterly security posture assessments to automated daily ones.

Security guardrails enabled our risk based approach.

Transform - #2
Reinvent security tech stack

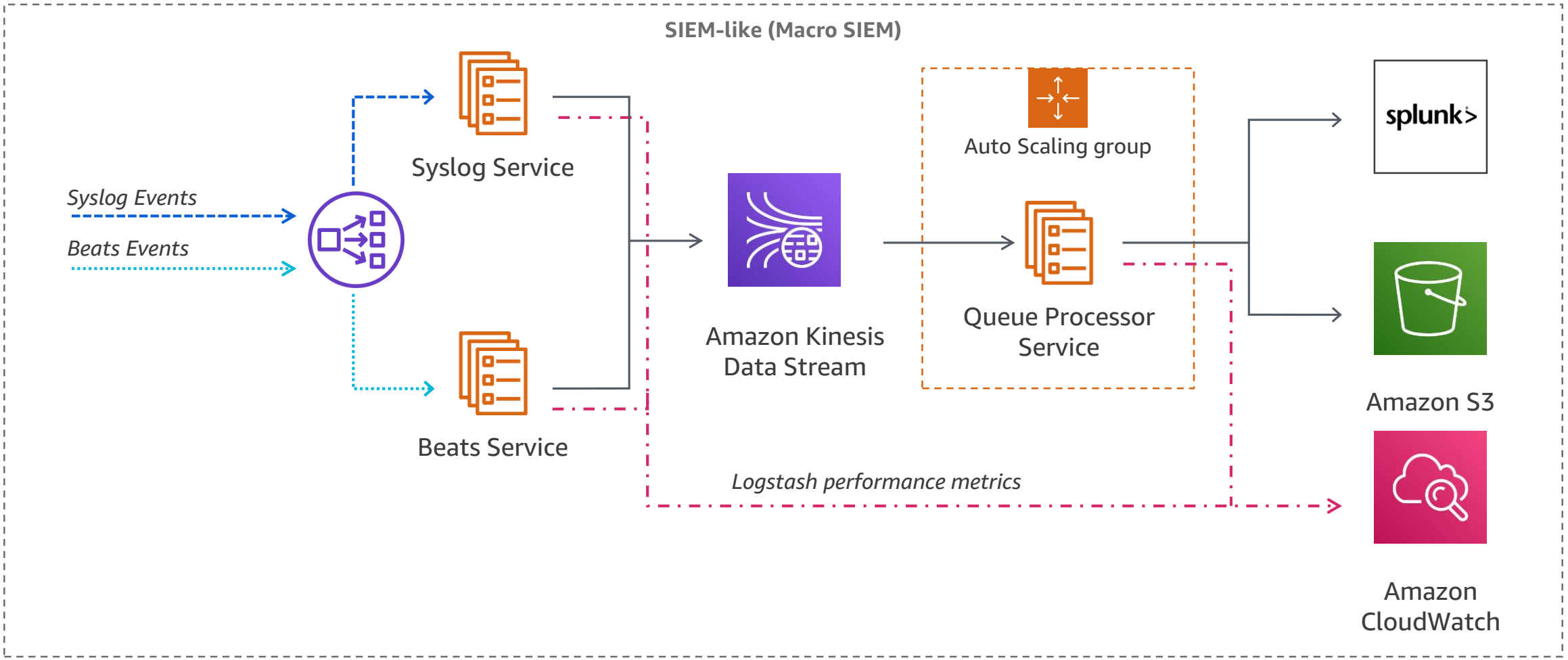
Architecture for Security Operations

#2 Reinvent security stack
Architecture for Security Operations



#2 Reinvent security stack

LOGGING – ARCHITECURE



#2 Reinvent security stack

LOGGING – OUTCOME

Zero servers

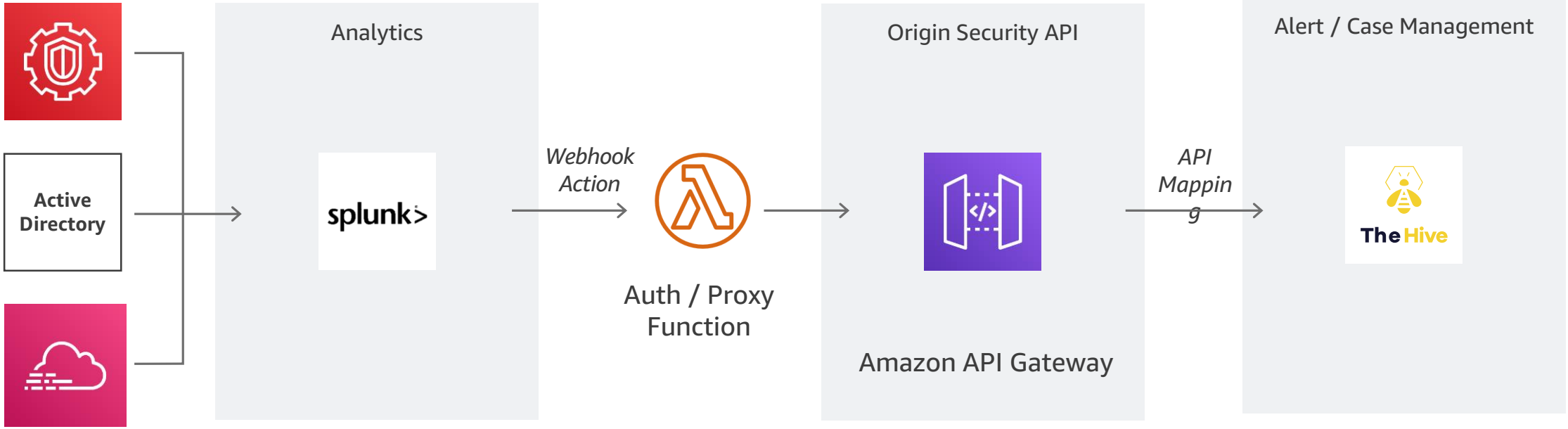
8000 events / second

$800 / month

We collect everything we *might* need without the stress of license limits or high costs.

#2 Reinvent security stack

ALERTING – ARCHITECTURE



#2 Reinvent security stack

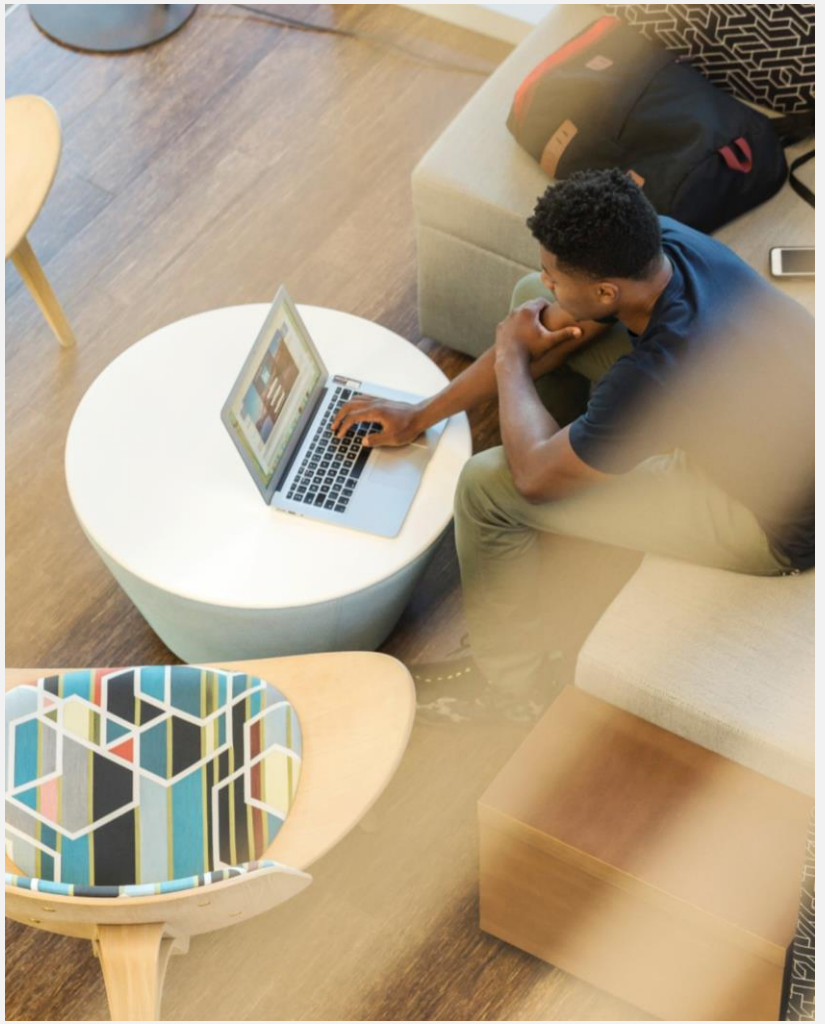
ALERTING – OUTCOME

Abstracts systems

One security API

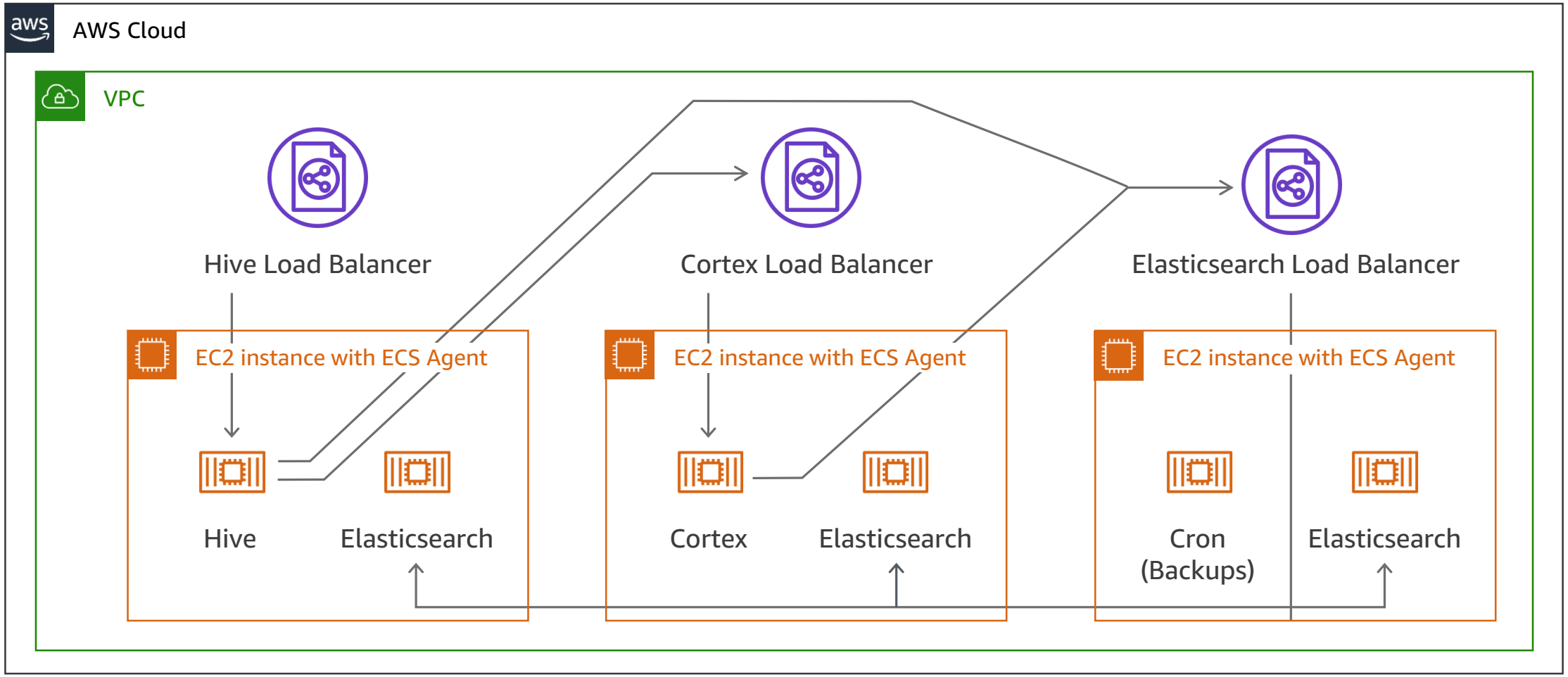
$30 / month

Coding against our own API lets us make future tooling changes without re-writing everything.



#2 Reinvent security stack

RESPONSE – ARCHITECTURE



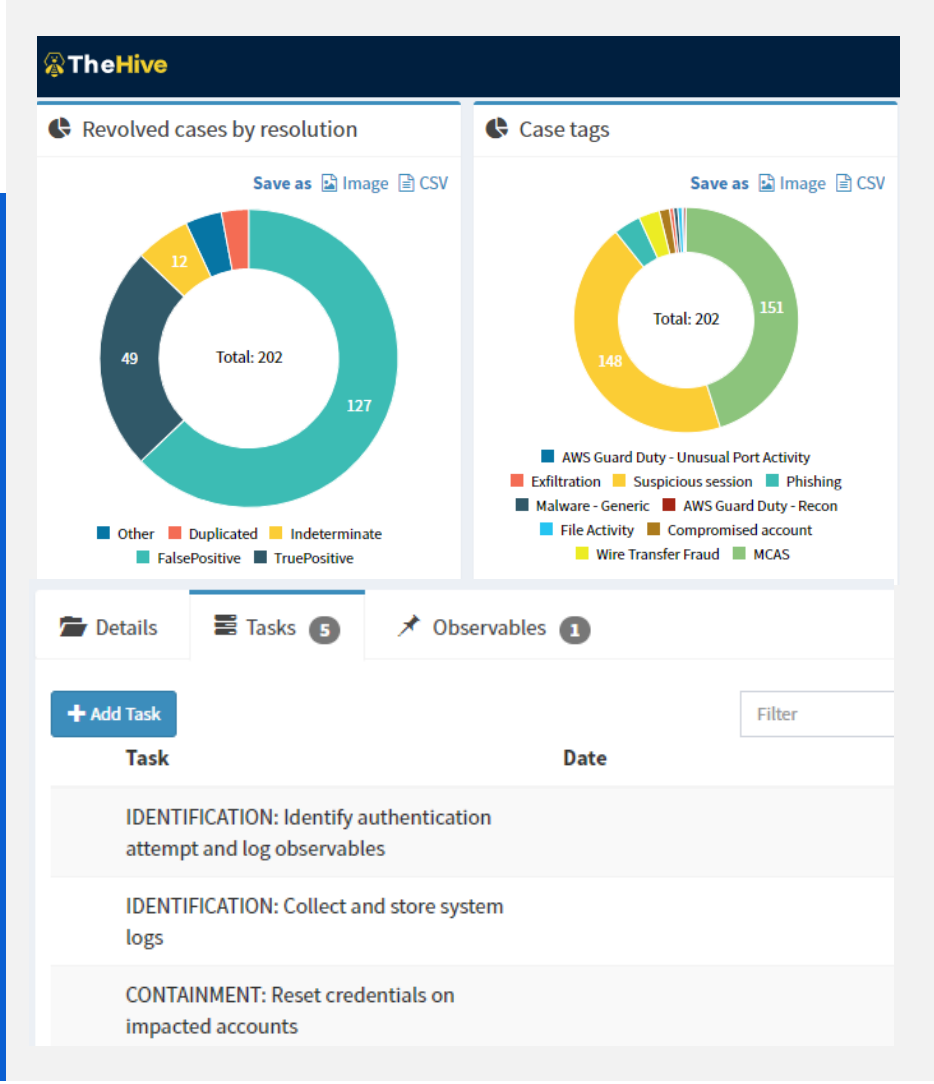
#2 Reinvent security stack

RESPONSE – OUTCOME

Playbooks
Case metrics
$200 / month

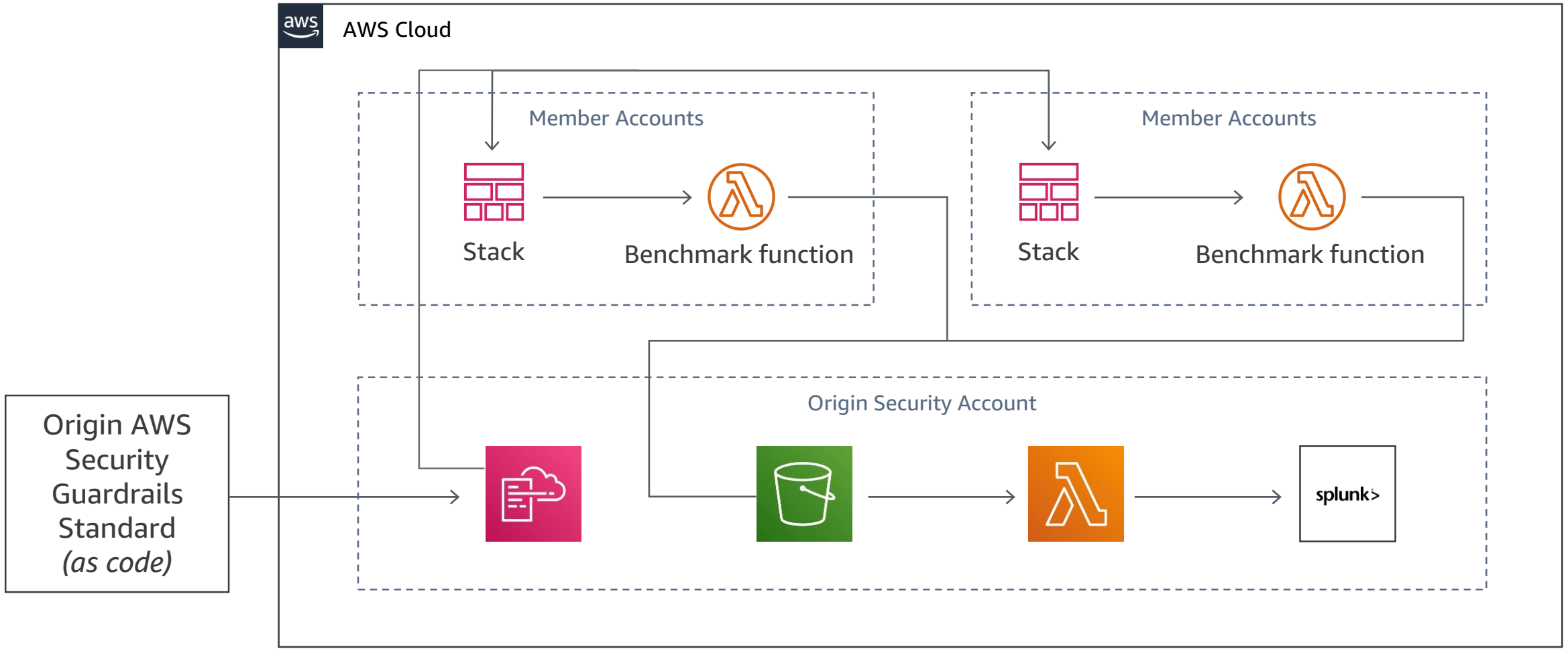
Standard playbooks provide consistency.

Metrics help tune alerts and prove effectiveness.



#2 Reinvent security stack

GOVERNANCE – ARCHITECTURE



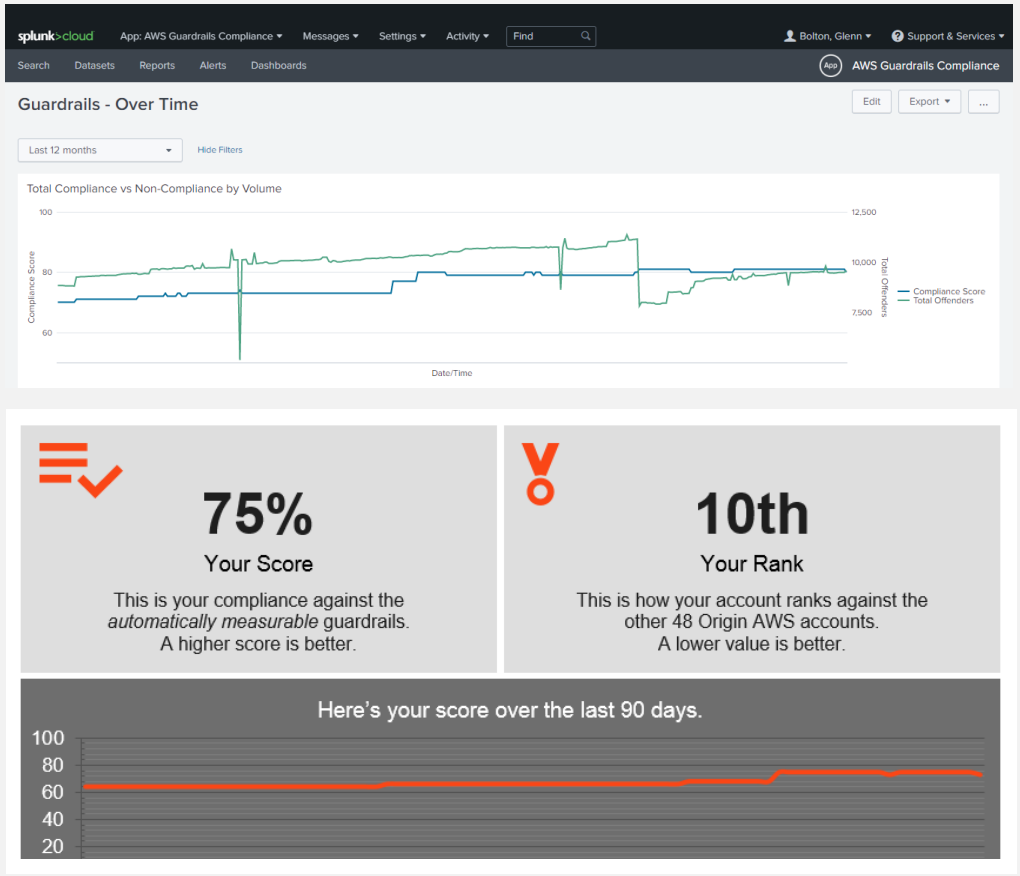
#2 Reinvent security stack

GOVERNANCE – ARCHITECTURE

Competitive compliance

<$2 / month

Continuous compliance monitoring and open reporting encourages improvement.



Transform - #3
Improving security transparency

Why did we have to change?

We want to continuously improve security culture.

We believe increased security transparency drives security culture.

What we did:

New tech stack enabled transparency of security information.

Developed a security metrics dashboard and league table.

Made it easy for the business to access information.

Transform - #3
Improving security transparency

The outcome

Business is asking “how do we compare?” and this creates a competitive spirit.

Compliance with security controls improved between 14-25% within a year.

Significant issues are resolved immediately instead of taking days.

Auditors can perform on-demand assurance.

Your action plan

Be bold and use your cloud journey as an opportunity to transform your security capability and culture.

Focus on transforming your skills and competencies, technology stack, and security transparency.

These actions get your journey started:

1. Leverage our **security principles** as a starting point for defining your own.

2. Take the **AWS Security Fundamentals training** to uplift your skills and capability and talk to **AWS professional services.**

   https://aws.amazon.com/training/course-descriptions/security-fundamentals/

3. Use the **AWS Security Benchmark on GitHub** or **AWS Security Hub** as a starting point.

   https://github.com/awslabs/aws-security-benchmark

   https://aws.amazon.com/security-hub/

4. Deploy our stack from GitHub to **fast-track your logging pipelines.**

Origin open source project

Remember that one of our security principles is about **working with partners, industry and regulators to achieve a broader security uplift**

To bring this principle to life, we are happy to announce that Origin Energy has open sourced the presented security monitoring pipeline

Go to [GitHub URL HERE]

good energy

Thank you!

aws SUMMIT ONLINE