On the Importance of Visibility

Allan Shone
Systems Engineering Lead @ Deputy
Visibility

01  The Basics

02  The Situation

03  The Incidents
Is...?

- A buzzword
- Not *that* one
- The bare minimum
- Often pre-provided
“The fact, state, or degree of being visible.”
Is Not!

- Observability
- Monitoring
- Tooling
The Situation

Visibility is like an onion...

https://i.ytimg.com/vi/c9b5L3ivPDo/maxresdefault.jpg
Problem

- Observability into existing systems was missing
- Available tooling was prohibitively expensive
- Specific scenarios were known
Solution

- Build our own tool
- Use composable components
- Integrate with existing workflows
17:43 security-alerts APP

Monitor Alert! usage from unknown IP detected!

IP

Investigate  Whitelist IP Address?
Thoughts

- Worked for our needs
- Manage our own rules
- Only what we needed
- Full integrated
- How do we know it’s working?
22:03 **security-alerts** APP

Security Lambda Monitoring

**Alarm**

Monitor_No_Invocation_Alarm

**State**

ALARM

**Desc**

Monitor for lack of invocations of the _Monitor lambda function_

Security Lambda Monitoring

Monitor_No_Invocation_Alarm has recovered
More Thoughts

- When the function doesn’t execute
- Minimal setup and overhead
- Same visibility
- Worked fine

@CerealBoy
It Works!

FUNCTION NOT RUNNING IS ALL WE NEED

WE CAN STILL SEND MESSAGES RIGHT?

WE CAN STILL SEND MESSAGES RIGHT?!
Hey, why hasn't the [redacted] fired off any alerts for a while? Was something tied to [redacted] account?
Problem!

- Function invocations had been happening
- Metrics were being generated
- Configuration had not drifted
- Messages were not coming through
Alert! Anomalous activity detected!

Account Address

User ARN: arn:aws:iam::[redacted]:root

Investigate Whitelist IP Address?
Solution!

- Create a new Slack webhook
- Update the function configuration
- Re-test
The Incidents

You don’t know what you don’t look for

https://s0.geograph.org.uk/geophotos/01/48/01/1480195_aac60ff.jpg
Incidents

- Interruptions were chaotic
- Often in private discussions
- Typically involved the same handful of people
- Typically didn’t have actions
Outcomes

- Created our Incident Management Framework
- Streamline handling interruptions
- Distribute the workload
- Make situations more visible
- Visible internally and externally
The Framework

- Roles and responsibilities
- Gives structure
- Facilitates communication
- Involve the right people
- Ensures we don’t make the same mistakes
Effects

- Mayhem
- Confusion
- Interruptions galore
- Drop in confidence
- Visibility
Technical Things

- The basics should be basic
- Contemplate failure conditions
- Redundancy in visibility
- Cost isn’t always in currency
- Standards can sometimes be good
Visibility Things

- Making something visible might be horrifying
- With data change can come
- Understand your community
- Visibility is a great pathway to building trust
On the Importance of Visibility

Allan Shone
Systems Engineering Lead @ Deputy