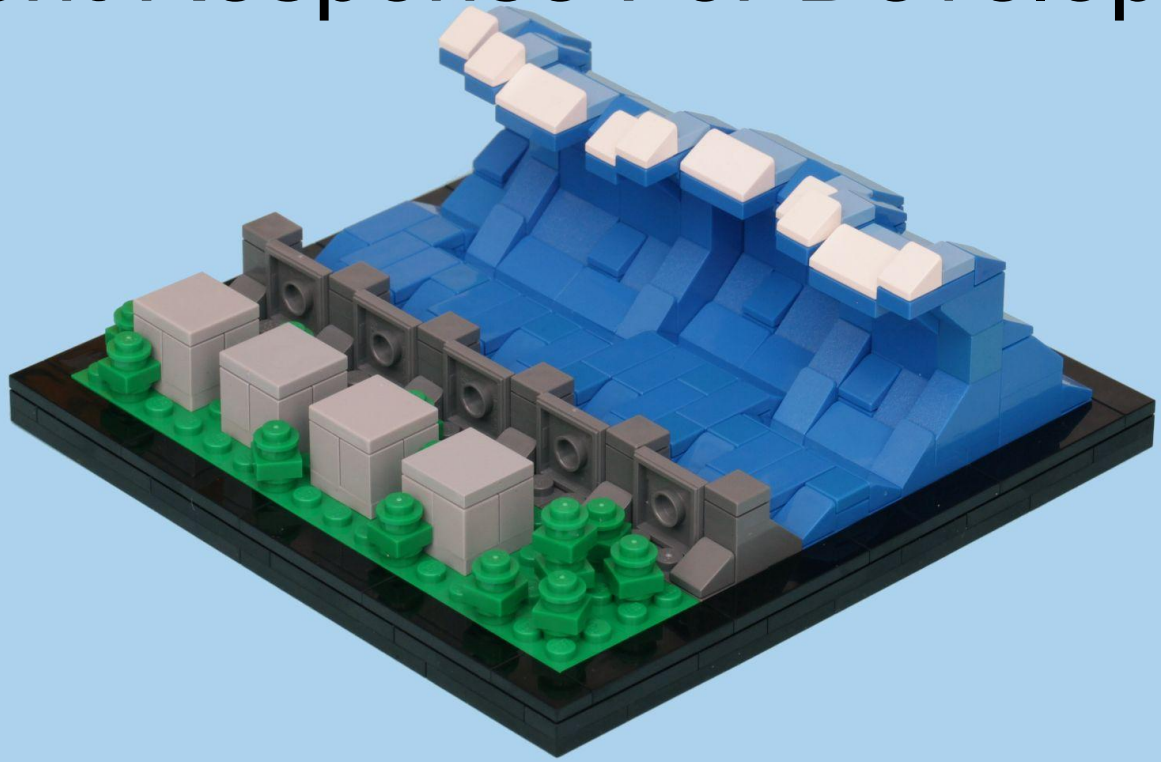
Incident Response For Developers



Joe Kuemerle - @jkuemerle@infosec.exchange

https://www.flickr.com/photos/pasukaru76/16295469666

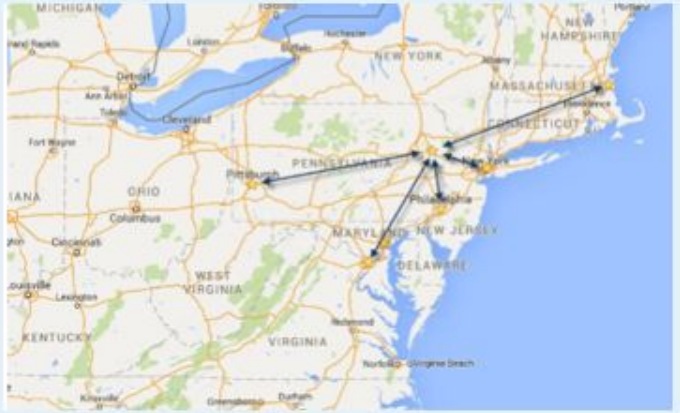
@jkuemerle@infosec.exchange

Disclaimer

https://brickset.com/article/40960/review-21043-san-francisco

techbash

October 13-16, 2026 | Pocono Manor, PA



- Great speakers with top content
- A fraction of the cost of the more crowded conferences
  - 3-day conference plus lodging for ~$1000
- Full-day deep dive preconference sessions available
- Easy travel from almost anywhere
- World-class keynotes
- In addition to the sessions, you get a great hallway Track, amazing food, attendee Welcome Reception, Game Night & more
- Family Day Friday - full day of kids' sessions, free for attendees' families
- Discounted Kalahari Resort rooms with water park access: stay, learn & play all week

https://techbash.com or **@techbash**

@jkuemerle@infosec.exchange

Agenda

- What
- Why
- How

https://flickr.com/photos/brian-fitzgerald/370223118/

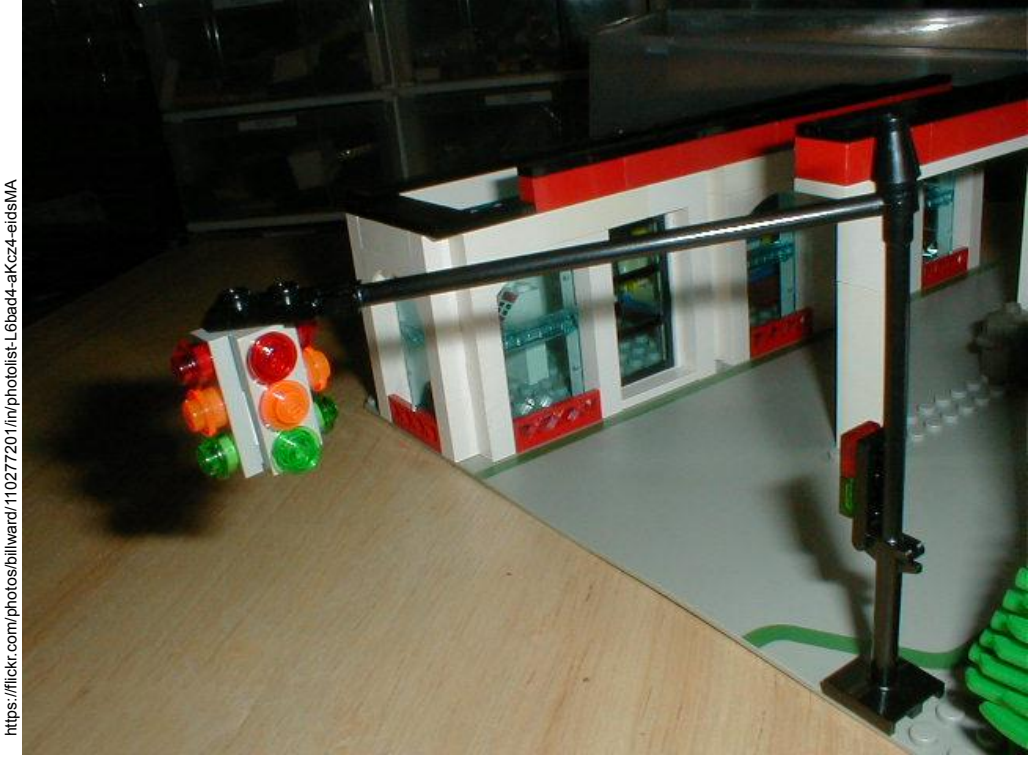
https://flickr.com/photos/masked-builder/5504022347/

https://flickr.com/photos/pasukaru76/5788095518/

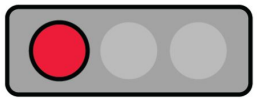
- Incident Commander
- Security Representative(s)
- Technical Lead (**not team**)
- Marketing/Comms
- Legal
- Executive

https://flickr.com/photos/the-magic-tuba-pixie/3543361685/

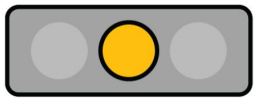
https://flickr.com/photos/billward/1102772201/in/photolist-L6bad4-aKcz4-eidsMA



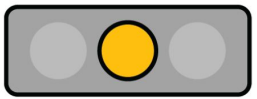
TLP:RED



TLP:AMBER+STRICT



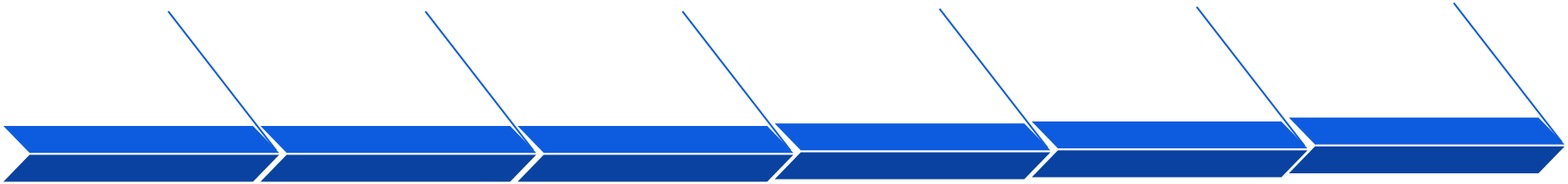
TLP:AMBER



TLP:GREEN

https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage

@jkuemerle@infosec.exchange



Preparation

Response Planning
IOC Documentation
Runbooks/Checklists
Threat Model
Disaster Recovery
Business Continuity
Tabletop Exercises

Identification

Log Analysis
Metrics
Behavioral Patterns
Data Queries

Containment

Emergency Fixes
Session Invalidation
Data Operations Limits

Eradication

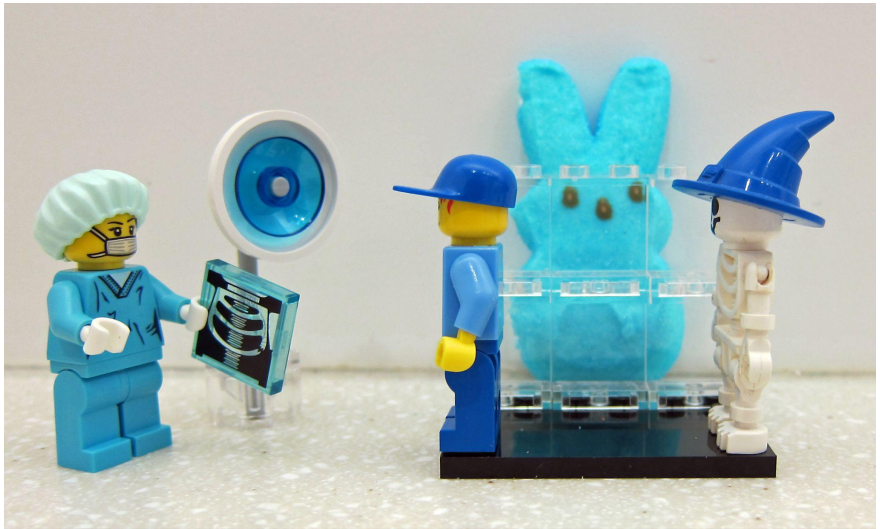
Persistence Analysis
Activity Log
Pivot Mapping

Recovery

Transactional Analysis
Configuration Recovery
Data Recovery

Lessons Learned

RCA
Update Materials
New Work Planning
Patching



https://flickr.com/photos/wiredforsound23/7009309089

@jkuemerle@infosec.exchange

https://flickr.com/photos/pasukaru76/52456412874/

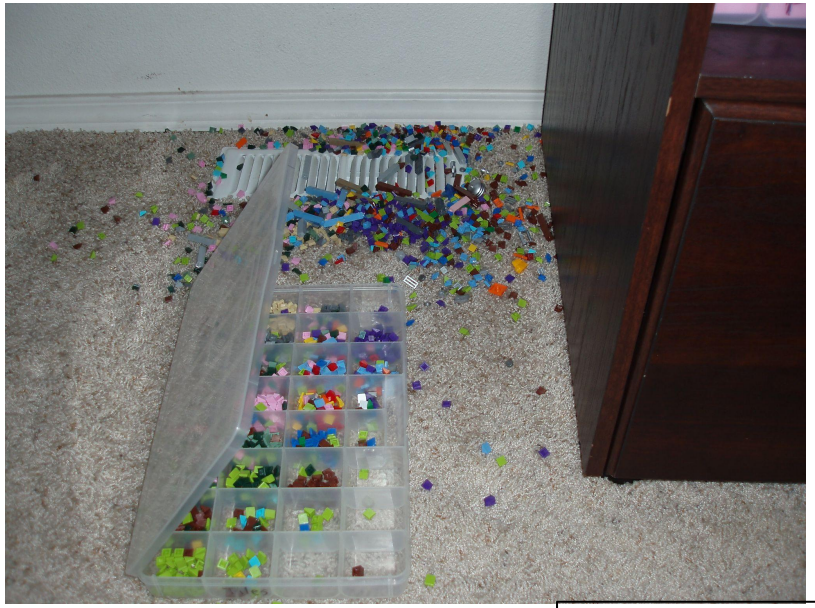
@jkuemerle@infosec.exchange

https://flickr.com/photos/journalismfestival/25822764473/

https://flickr.com/photos/bosta/6020400291/

@jkuemerle@infosec.exchange

Preparation

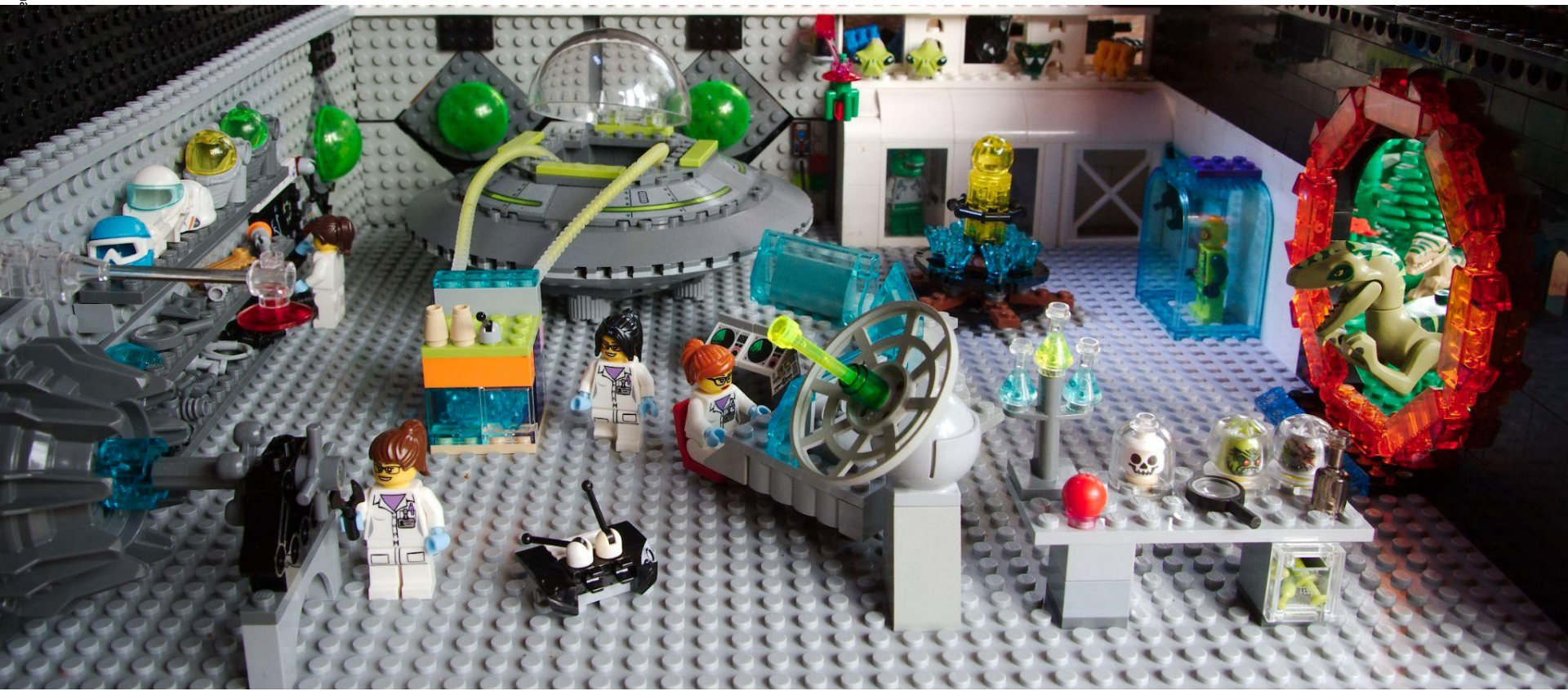


https://flickr.com/photos/eilonwy77/8262632833/

https://flickr.com/photos/irrational_cat/2354166726/

- ❏ Response Planning
- ❏ IOC Documentation
- ❏ Runbooks/Checklists
- ❏ Threat Model
- ❏ Disaster Recovery
- ❏ Business Continuity
- ❏ Tabletop Exercises

Identification



https://flickr.com/photos/paulspace/10388748355/

@jkuemerle@infosec.exchange

Containment

https://flickr.com/photos/eilonwy77/8524707011/

Eradication

https://flickr.com/photos/brickninja/32587837648/

@jkuemerle@infosec.exchange

Recovery

https://flickr.com/photos/wwarby/11682625885/

@jkuemerle@infosec.exchange

Lessons Learned

https://flickr.com/photos/billward/3399197394/

Root-Cause Analysis Template

A root-cause analysis should be completed after each Tier 1 or 2 incident. Additionally, it should be completed after each penetration test.

Purpose

Use this section to explain briefly why this report is being filled out (i.e. What incident is it addressing? Data breach, penetration test, etc.)

General Information

Incident Number	Root-Cause Analysis Number	Location of Incident	People Who Worked on Incident
Text	Text	Text	Text
Start Date/Time	**End Date/Time**	**Duration**	Text
Text	Text	Text	Text

Summary of Incident

Give a brief recap of the incident in three to five sentences.
(This section provides a succinct description of the "5 whys" noted in the TIP below.)

Timeline of Activities

Date	Details	Contact for Activity

Specifics of Root Cause

Describe the following:

- Services impacted
- Duration of incident
- Type of incident
- Severity level of incident
- Incident details

TIP: Use this section to continue to ask "Why?" Why did this incident occur? After asking "Why?" five times, you will be at the root cause of the incident.

Corrective Measures

Highlight the specific technical components that need to be changed or adapted for this incident type.

Areas of Improvement

Use this section to highlight areas of improvement for the response team. Focus mainly on process elements rather than technical details.

Incident Response Contacts

Contact	Contact Information
End User	
Service Desk	
Third Party/Vendor	
Security	
SOC	
CISO	
IT Operations	
Legal/PR	
HR	

Incident 2413 – Summary of Our Investigation ›

The following is a summary, including known threat actor activity and our responses, of our investigation into unauthorized access to Heroku systems taking place between April 13, 2022, and May 30, 2022.

Incident Summary ›

On April 13, 2022, GitHub notified our security team of a potential security issue they identified on April 12, 2022, and we immediately launched an investigation. Within three hours, we took action and disabled the identified compromised user's OAuth token and GitHub account. We began investigating how the user's OAuth token was compromised and determined that, on April 7, 2022, a threat actor obtained access to a Heroku database and downloaded stored customer GitHub integration OAuth tokens.

According to GitHub, the threat actor began enumerating metadata about customer repositories with the downloaded OAuth tokens on April 8, 2022. On April 9, 2022, the threat actor downloaded a subset of the Heroku private GitHub repositories from GitHub, containing some Heroku source code. Additionally, according to GitHub, the threat actor accessed and cloned private repositories stored in GitHub owned by a small number of our customers. When this was detected, we notified customers on April 15, 2022, revoked all existing tokens from the Heroku Dashboard GitHub integration, and prevented new OAuth tokens from being created.

We began investigating how the threat actor gained initial access to the environment and determined it was obtained by leveraging a compromised token for a Heroku machine account. We determined that the unidentified threat actor gained access to the machine account from an archived private GitHub repository containing Heroku source code. We assessed that the threat actor accessed the repository via a third-party integration with that repository. We continue to work closely with our partners, but have been unable to definitively confirm the third-party integration that was the source of the attack.

Further investigation determined that the actor accessed and exfiltrated data from the database storing usernames and uniquely hashed and salted passwords for customer accounts. While the passwords were hashed and salted, we made the decision to rotate customer accounts on May 5, 2022, out of an abundance of caution due to not all of the customers having multi-factor authentication (MFA) enabled at the time and potential for password reuse.

https://www.heroku.com/blog/april-2022-incident-review/

Summary of the Amazon DynamoDB Service Disruption in the Northern Virginia (US-EAST-1) Region

We wanted to provide you with some additional information about the service disruption that occurred in the N. Virginia (us-east-1) Region on October 19 and 20, 2025. While the event started at 11:48 PM PDT on October 19 and ended at 2:20 PM PDT on October 20, there were three distinct periods of impact to customer applications. First, between 11:48 PM on October 19 and 2:40 AM on October 20, Amazon DynamoDB experienced increased API error rates in the N. Virginia (us-east-1) Region. Second, between 5:30 AM and 2:09 PM on October 20, Network Load Balancer (NLB) experienced increased connection errors for some load balancers in the N. Virginia (us-east-1) Region. This was caused by health check failures in the NLB fleet, which resulted in increased connection errors on some NLBs. Third, between 2:25 AM and 10:36 AM on October 20, new EC2 instance launches failed and, while instance launches began to succeed from 10:37 AM, some newly launched instances experienced connectivity issues which were resolved by 1:50 PM.

DynamoDB

Between 11:48 PM PDT on October 19 and 2:40 AM PDT on October 20, customers experienced increased Amazon DynamoDB API error rates in the N. Virginia (us-east-1) Region. During this period, customers and other AWS services with dependencies on DynamoDB were unable to establish new connections to the service. The incident was triggered by a latent defect within the service's automated DNS management system that caused endpoint resolution failures for DynamoDB.

Many of the largest AWS services rely extensively on DNS to provide seamless scale, fault isolation and recovery, low latency, and locality. Services like DynamoDB maintain hundreds of thousands of DNS records to operate a very large heterogeneous fleet of load balancers in each Region. Automation is crucial to ensuring that these DNS records are updated frequently to add additional capacity as it becomes available, to correctly handle hardware failures, and to efficiently distribute traffic to optimize customers' experience. This automation has been designed for resilience, allowing the service to recover from a wide variety of operational issues. In addition to providing a public regional endpoint, this automation maintains additional DNS endpoints for several dynamic DynamoDB variants including a FIPS compliant endpoint, an IPv6 endpoint, and account-specific endpoints. The root cause of this issue was a latent race condition in the DynamoDB DNS management system that resulted in an incorrect empty DNS record for the service's regional endpoint (**dynamodb.us-east-1.amazonaws.com**) that the automation failed to repair. To explain this event, we need to share some details about the DynamoDB DNS management architecture. The system is split across two independent components for availability reasons. The first component, the DNS Planner, monitors the health and capacity of the load balancers and periodically creates a new DNS plan for each of the service's endpoints consisting of a set of load balancers and weights. We produce a single regional DNS plan, as this greatly simplifies capacity management and failure mitigation when capacity is shared across multiple endpoints, as is the case with the recently launched IPv6 endpoint and the public regional endpoint. A second component, the DNS Enactor, which is designed to have minimal dependencies to allow for system recovery in any scenario, enacts DNS plans by applying the required changes in the Amazon Route53 service. For resiliency, the DNS Enactor operates redundantly and fully independently in three different Availability Zones (AZs). Each of these independent instances of the DNS Enactor looks for new plans and

https://aws.amazon.com/message/101925/

https://flickr.com/photos/loozrboy/3024161612/

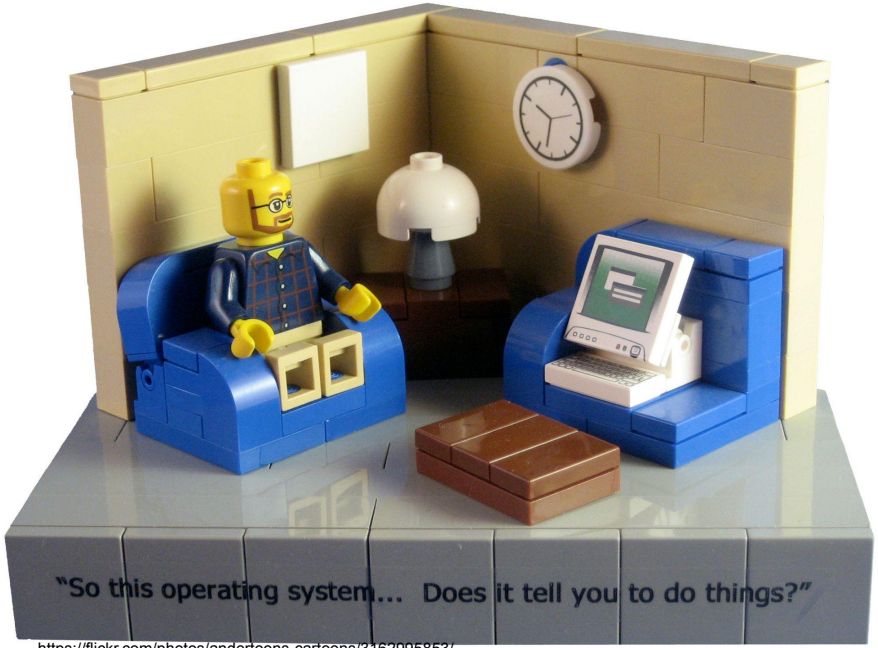
https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

https://www.ncsc.gov.uk/section/exercise-in-a-box/overview

https://flickr.com/photos/137234632@N06/23403663196/

@jkuemerle@infosec.exchange

GenAI in IR



https://flickr.com/photos/andertoons-cartoons/3162995853/

Preparation

Response Planning
IOC Documentation
Runbooks/Checklists
Threat Model
Disaster Recovery
Business Continuity
Tabletop Exercises

Identification

Log Analysis
Metrics
Behavioral Patterns
Data Queries

Containment

Emergency Fixes
Session Invalidation
Data Operations Limits

Eradication

Persistence Analysis
Activity Log
Pivot Mapping

Recovery

Transactional Analysis
Configuration Recovery
Data Recovery

Lessons Learned

RCA
Update Materials
New Work Planning
Patching

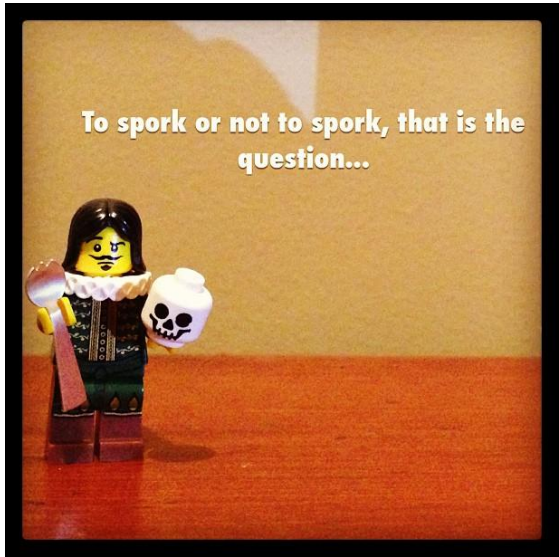
References / Q & A

Incident Response for Developers

- https://www.securitymetrics.com/blog/6-phases-incident-response-plan
- https://www.atlassian.com/incident-management/incident-response/lifecycle#atlassian-incident-response-lifecycle
- https://docs.aws.amazon.com/security-ir/latest/userguide/security-incident-response-guide.html
- https://www.sygnia.co/blog/incident-response-team/
- https://academy.semgrep.dev/courses/Incident-response-for-devs
- https://dfirdiva.com/
- https://github.com/meirwah/awesome-incident-response
- https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages
- https://www.ncsc.gov.uk/section/exercise-in-a-box/overview
- Slides in Discord and Github
  - https://codemash.org/discord
  - https://github.com/codemash-conference/session-slides/
- CTF: codemashctf.com

@jkuemerle@infosec.exchange

https://www.linkedin.com/in/joekuemerle/



https://flickr.com/photos/betsyweber/8729701344/