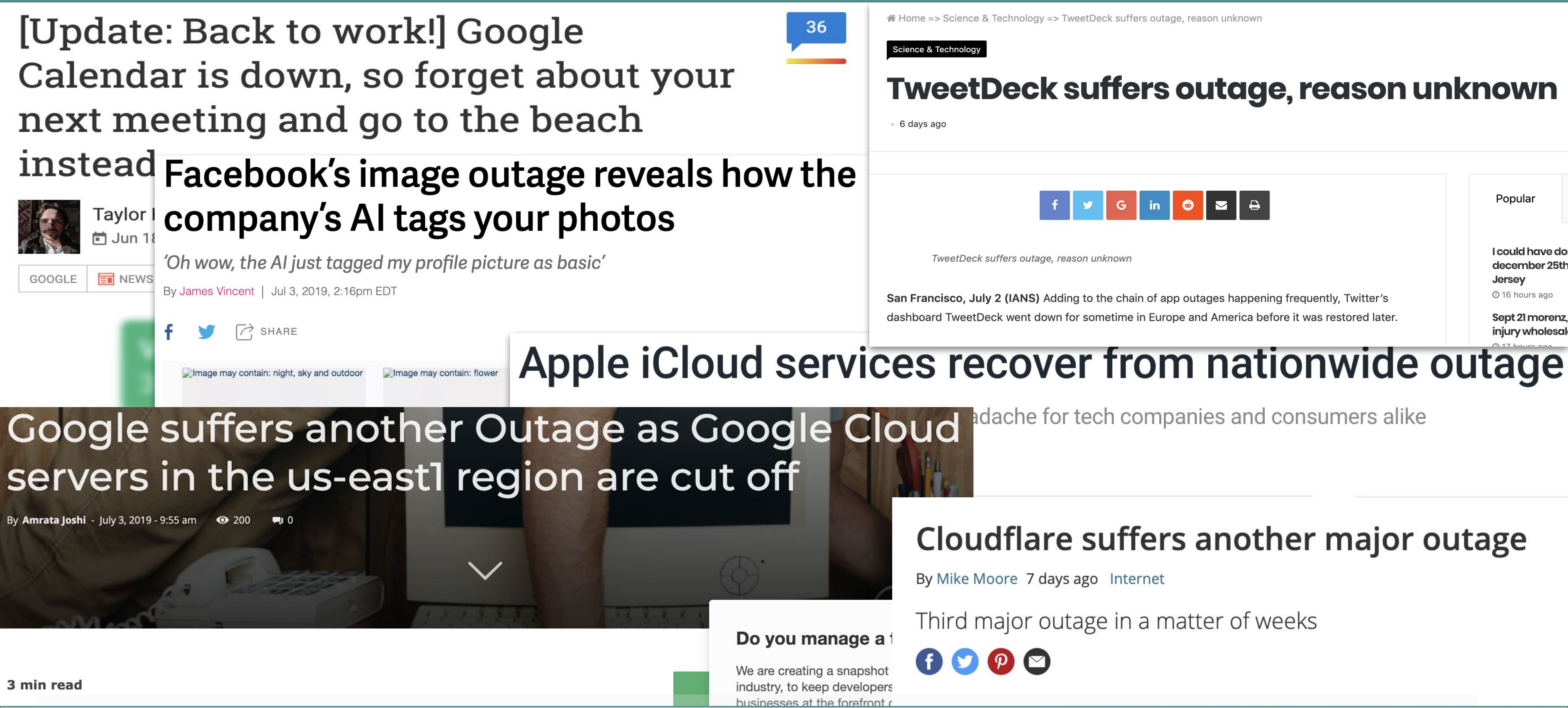
Security Chaos Engineering

TIC 4302 - Information Security Practicum II

Most of the materials are taken from “Security Chaos Engineering” presented in DevSecOps Day 20019 Singapore by Aaron Rinehard (Verica)



[Update: Back to work!] Google Calendar is down, so forget about your next meeting and go to the beach instead

36

Taylor

Jun 18

GOOGLE NEWS

Home => Science & Technology => TweetDeck suffers outage, reason unknown

Science & Technology

TweetDeck suffers outage, reason unknown

6 days ago

Facebook's image outage reveals how the company's AI tags your photos

'Oh wow, the AI just tagged my profile picture as basic'

By James Vincent | Jul 3, 2019, 2:16pm EDT

SHARE

Image may contain: night, sky and outdoor

Image may contain: flower

TweetDeck suffers outage, reason unknown

San Francisco, July 2 (IANS) Adding to the chain of app outages happening frequently, Twitter's dashboard TweetDeck went down for sometime in Europe and America before it was restored later.

Popular

I could have do december 25th Jersey

16 hours ago

Sept 21 morenz, injury wholesal

Apple iCloud services recover from nationwide outage

adache for tech companies and consumers alike

Google suffers another Outage as Google Cloud servers in the us-east1 region are cut off

By Amrata Joshi - July 3, 2019 - 9:55 am 200 0

3 min read

Do you manage a

We are creating a snapshot industry, to keep developers businesses at the forefront

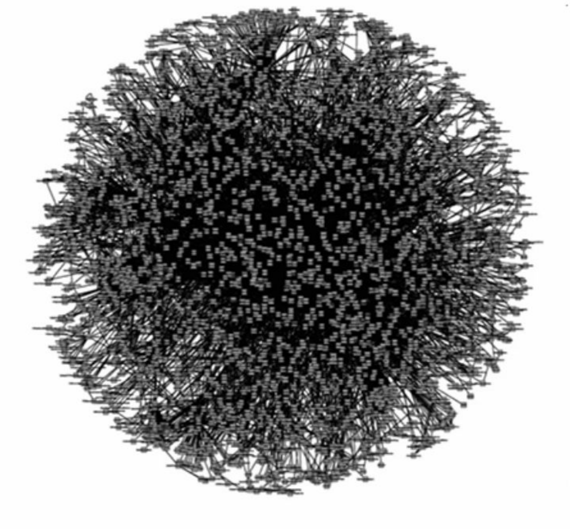
Cloudflare suffers another major outage

By Mike Moore 7 days ago Internet

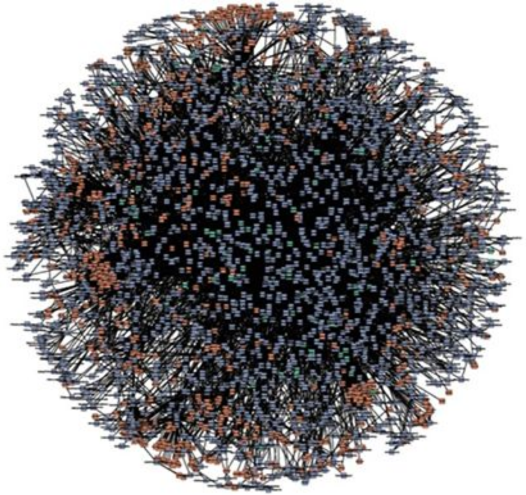
Third major outage in a matter of weeks

Security Breach is "costly" and "obvious" Problem but why is happening more so often?

Our systems have evolved beyond human ability to mentally model their behavior.



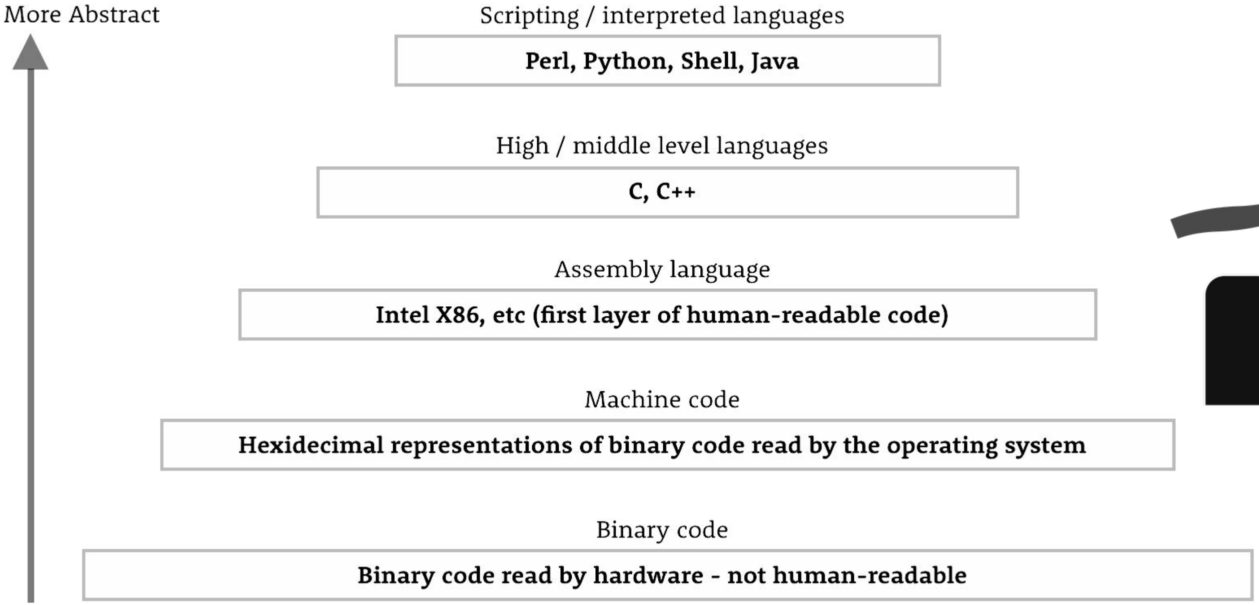
everyone else



amazon.com

NETFLIX

Software Only Increases in Complexity



More Abstract

Scripting / interpreted languages

Perl, Python, Shell, Java

High / middle level languages

C, C++

Assembly language

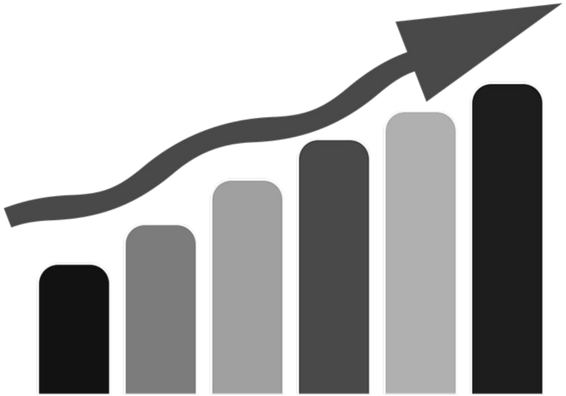
Intel X86, etc (first layer of human-readable code)

Machine code

Hexidecimal representations of binary code read by the operating system

Binary code

Binary code read by hardware - not human-readable



Complex?

Continuous Delivery

Distributed Systems

Microservice Architectures

Automation Pipelines

Blue/Green Deployments

Containers

DevOps

Continuous Integration

Immutable Infrastructure

Infracode

Cloud Computing

CI/CD

Service Mesh

API

Auto Canaries

Circuit Breaker Patterns

Security?

Mostly Monolithic

Expert Systems

Stateful in nature

Prevention focused

Poorly Aligned

Adversary Focused

Defense in Depth

Requires Domain Knowledge

DevSecOps not widely adopted

Security incidents are <u>not effective measures of detection</u> because at that point it's already too late

No System is inherently Secure by Default, its Humans that make them that way

People Operate Differently when they expect things to fail

Chaos Engineering

"Chaos Engineering is the discipline of experimenting on a distributed system in order to build confidence in the system's ability to withstand turbulent conditions"

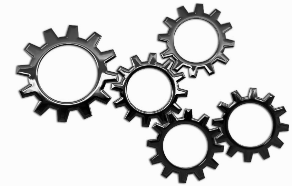
Developing a Learning Culture around Failure

- Safety as part of security
- Building safety margin into systems
- Replace blame culture with learning culture
- Telemetry, experimentation, and instrumentation

Chaos Monkey Story

NETFLIX

- During Business Hours
- Born out of Netflix Cloud Transformation
- Put well defined problems in front of engineers.
- Terminate VMs on Random VPC Instances



Chaos Engineering Operational Models

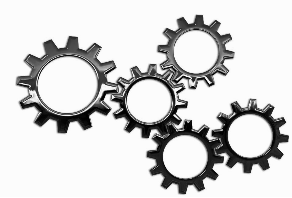
- Organization-Wide Chaos Engineering Team
- Provide a Chaos Engineering Solution for Teams to Consume
- Central Team runs periodic Chaos Experiments as a Service
- Provide SREs with Chaos Toolsets

"At Netflix Chaos Engineering was always meant to be a tools practice for SREs"

- Casey Rosenthal

Security Chaos Engineering is…

“The discipline of instrumentation, identification, and remediation of failure within security controls through proactive experimentation to build confidence in the system's ability to defend against malicious conditions in production.”



Security Chaos Engineering includes...

- Continuous Security Verification
- Proactively Manage & Measure
- Reduce Uncertainty by Building Confidence
- Build Confidence in What Actually Works

Security Chaos Engineering: Is NOT

- Red Teaming
- Penetration Testing
- Adversary Based
- Focused on Attacks

- The process of creating the experiment and sharing the learnings is the highest-value of Chaos Engineering
- Chaos Engineering Goal: Share Team Mental Models is of High Importance

Use Cases

- Incident Response
- Solutions Architecture
- Security Control Validation
- Security Observability
- Continuous Verification
- Compliance Monitoring

ChaoSlingr

An Open Source Tool

ChaoSlingr Product Features

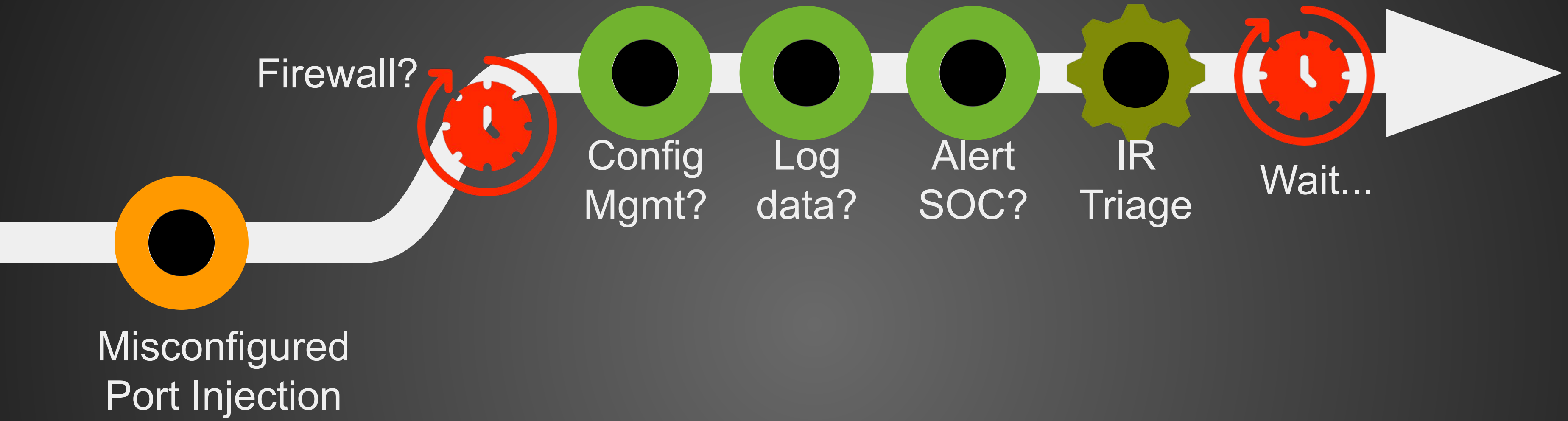
- ChatOps Integration
- Configuration-as-Code
- Example Code & Open Framework

- Serverless App in AWS
- 100% Native AWS
- Configurable Operational Mode & Frequency
- Opt-In | Opt-Out Model

slack

HashiCorp Terraform

amazon web services™



Misconfigured Port Injection

Firewall?

Config Mgmt?

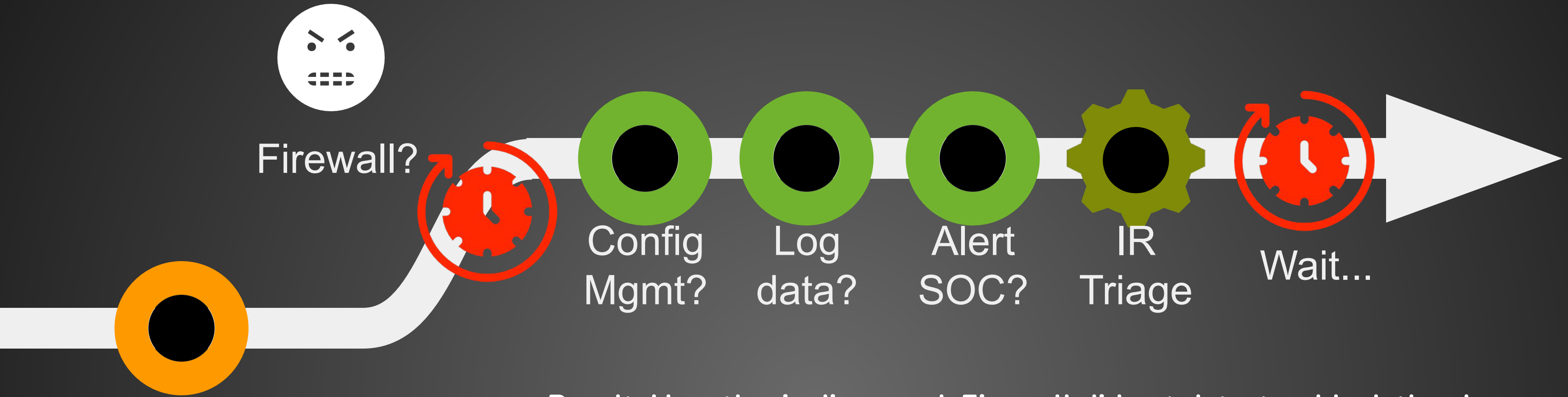
Log data?

Alert SOC?

IR Triage

Wait...

Hypothesis: If someone accidentally or maliciously introduced a misconfigured port then we would immediately detect, block, and alert on the event.



Misconfigured Port Injection

Result: Hypothesis disproved. Firewall did not detect or block the change on all instances. Standard Port AAA security policy out of sync on the Portal Team instances. Port change did not trigger an alert and log data indicated successful change audit.
However we unexpectedly learned the configuration mgmt tool caught change and alerted the SoC.

More Experiment Examples

- Software Secret Clear Text Disclosure
- Permission collision in Shared IAM Role Policy
- Disabled Service Event Logging
- Introduce Latency on Security Controls
- API Gateway Shutdown

- Internet exposed Kubernetes API
- Unauthorized Bad Container Repo
- Unencrypted S3 Bucket
- Disable MFA
- Bad AWS Automated Block Rule

"Resilience is the story of the outage that never happened."

- John Allspaw