Security Chaos Engineering

GameDays when Experiments are CyberAttacks

YURY NIÑO

Site Reliability Engineer

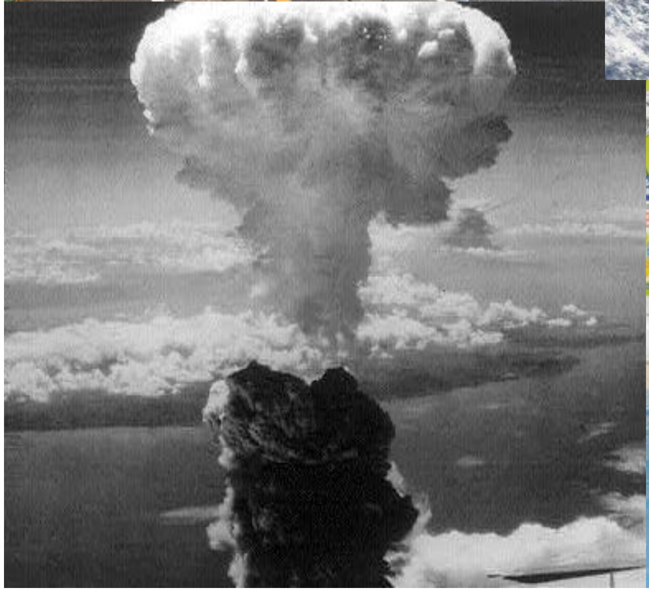
Chaos Engineering Advocate

Digital Labs

@yurynino

https://www.yurynino.dev/

JAPAN: CULTURE OF RESILIENCE



Google Photos

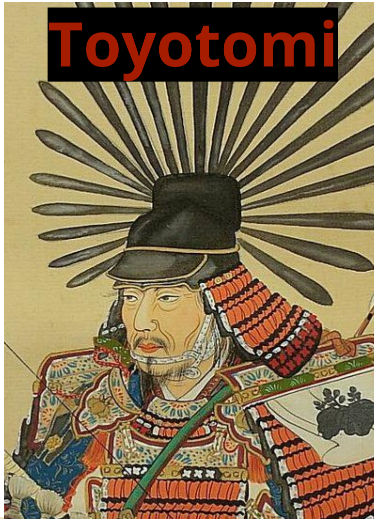
5 Famous Samurais

https://akimonogatari.es

Minamoto

Honda

Miyamoto Musashi


Toyotomi

Takeda

MIYAMOTO

SAMURAI & TEACHER

His instinct allowed him to improvise with absolute efficiency in any battle situation.

For him it was important to choose the weapon according to the circumstances.

The Book of Five Rings

Agenda

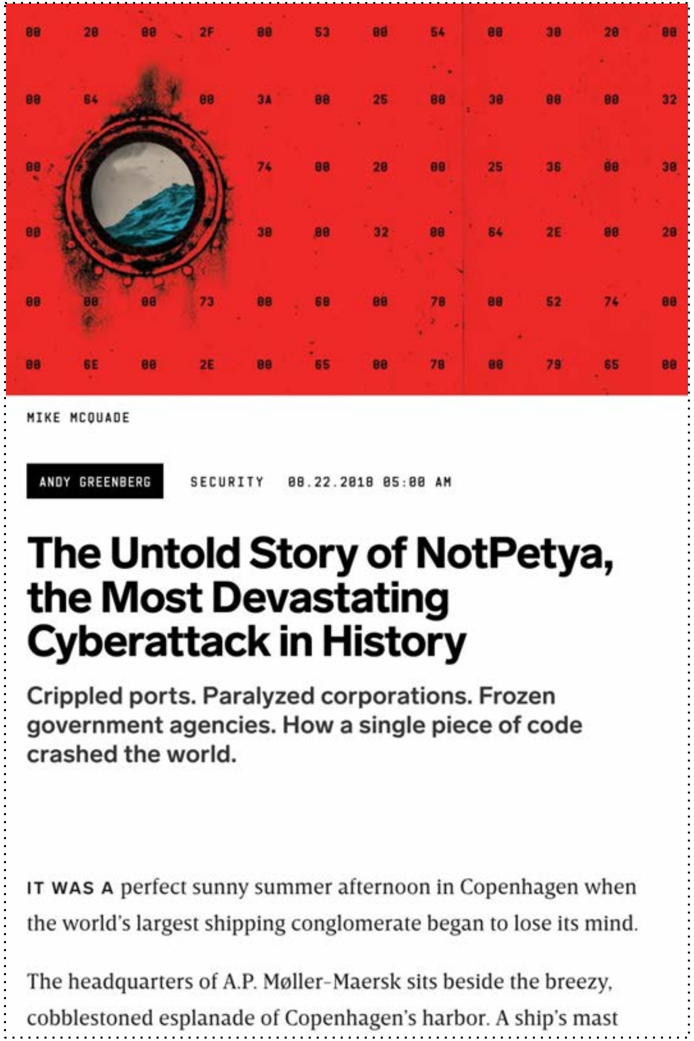
- Security Attacks
- Severity Incident Management
- When the incident is related to security
- Chaos GameDays
- **Our Framework**
- Learnings & Challenges

https://www.yurynino.dev/

Cyberwar is everywhere!

In the media, in the military, among politicians and in academia.

Some attacks!



MIKE MCQUADE

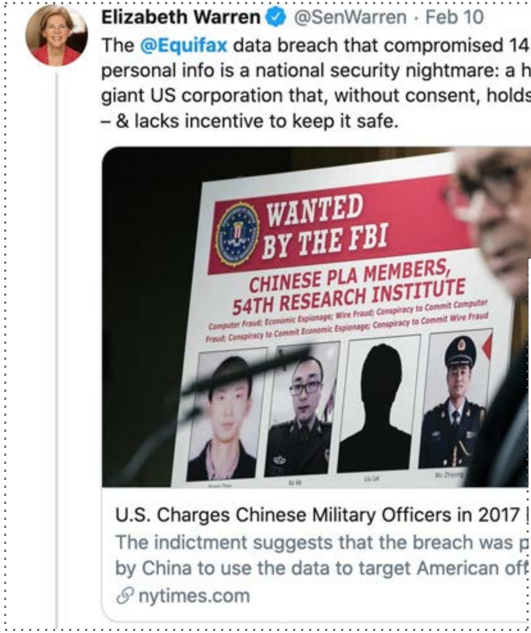
ANDY GREENBERG SECURITY 08.22.2018 05:00 AM

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

IT WAS A perfect sunny summer afternoon in Copenhagen when the world's largest shipping conglomerate began to lose its mind.

The headquarters of A.P. Møller-Maersk sits beside the breezy, cobblestoned esplanade of Copenhagen's harbor. A ship's mast



Elizabeth Warren @SenWarren · Feb 10

The @Equifax data breach that compromised 145 million Americans' personal info is a national security nightmare: a hostile foreign attack on a giant US corporation that, without consent, holds all of our personal data – & lacks incentive to keep it safe.

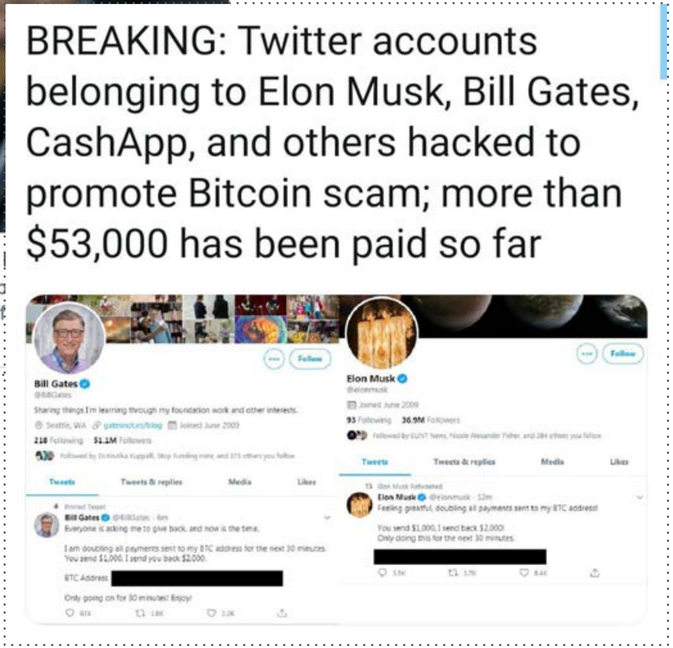
WANTED BY THE FBI
CHINESE PLA MEMBERS, 54TH RESEARCH INSTITUTE
Computer Fraud; Economic Espionage; Wire Fraud; Conspiracy to Commit Computer Fraud; Conspiracy to Commit Economic Espionage; Conspiracy to Commit Wire Fraud

U.S. Charges Chinese Military Officers in 2017

The indictment suggests that the breach was p

by China to use the data to target American off

nytimes.com



BREAKING: Twitter accounts belonging to Elon Musk, Bill Gates, CashApp, and others hacked to promote Bitcoin scam; more than $53,000 has been paid so far

Bill Gates
@BillGates
Sharing things I'm learning through my foundation work and other interests.
Seattle, WA gatesnotes/blog Joined June 2009
218 Following 51.1M Followers
Followed by Dr.Kirutika Kuppalli, Stop Funding Hate, and 373 others you follow

Tweets Tweets & replies Media Likes

Pinned Tweet
Bill Gates @BillGates · 6m
Everyone is asking me to give back, and now is the time.

I am doubling all payments sent to my BTC address for the next 30 minutes. You send $1,000, I send you back $2,000.

BTC Address [redacted]

Only going on for 30 minutes! Enjoy!

Elon Musk
@elonmusk
Joined June 2009
93 Following 36.9M Followers
Followed by ELENT News, Nicole Alexander Fisher, and 284 others you follow

Tweets Tweets & replies Media Likes

Elon Musk Retweeted
Elon Musk @elonmusk · 12m
Feeling greatful, doubling all payments sent to my BTC address!

You send $1,000, I send back $2,000!
Only doing this for the next 30 minutes.

[redacted]

Security

Attacks

https://blog.netwrix.com

Denial of Service

Attacker overwhelms a system's resources so that it cannot respond to service requests.

DoS doesn't provide direct benefits for attackers!

Man in Middle

Attacker hijacks a session between a trusted client and network server.

Session hijacking, IP spoofing and replay!

Phishing

Attacker sends emails that appear to be from trusted sources to gain access.

Social engineering and Technical trickery.

Security

Attacks

https://blog.netwrix.com

SQL Injection

Attacker executes a SQL query via an input data from the client to server.

“SELECT * FROM users WHERE account = ” or ‘1’ = ‘1’;”

Cross-Site Scripting

Attacker uses third-party web resources to run scripts in browsers or applications.

Steal cookies, keystrokes and collect information.

Malware

Attacker installs malicious software in the system without consentment of the owner.

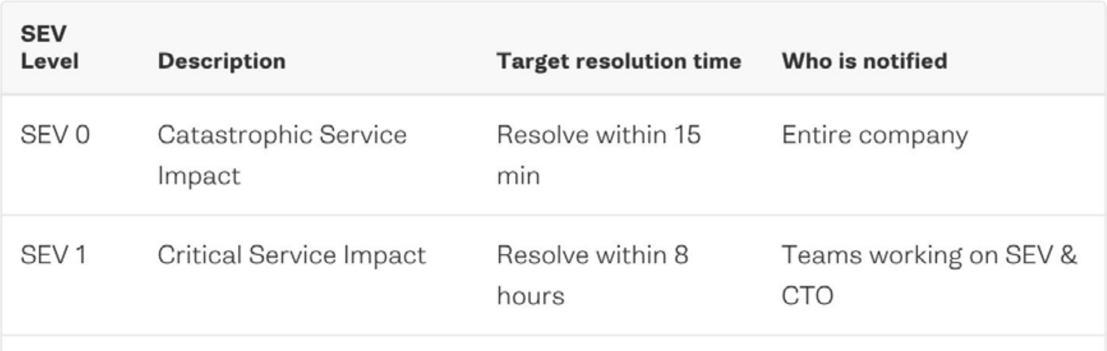
File infectors, trojans, worms, ransomware.

Respond to security critical issues before they impact your system!

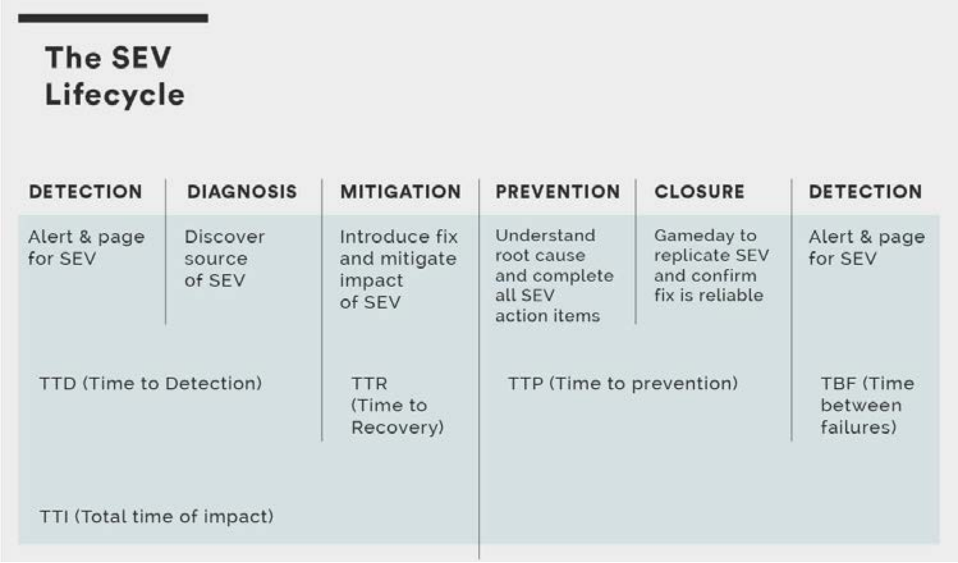
Severity **[Security]** Incident Management

is very useful here.

SEV



SEV Level	Description	Target resolution time	Who is notified
SEV 0	Catastrophic Service Impact	Resolve within 15 min	Entire company
SEV 1	Critical Service Impact	Resolve within 8 hours	Teams working on SEV & CTO
SEV 2	High Service Impact	Resolve w hours	



The SEV Lifecycle

DETECTION	DIAGNOSIS	MITIGATION	PREVENTION	CLOSURE	DETECTION
Alert & page for SEV	Discover source of SEV	Introduce fix and mitigate impact of SEV	Understand root cause and complete all SEV action items	Gameday to replicate SEV and confirm fix is reliable	Alert & page for SEV

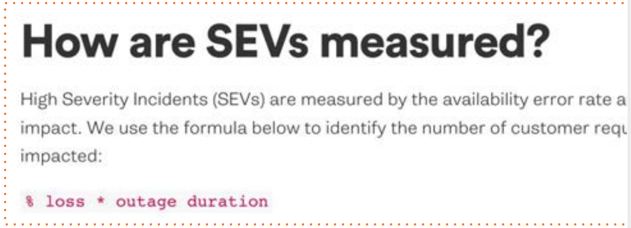
TTD (Time to Detection)

TTR (Time to Recovery)

TTP (Time to prevention)

TBF (Time between failures)

TTI (Total time of impact)



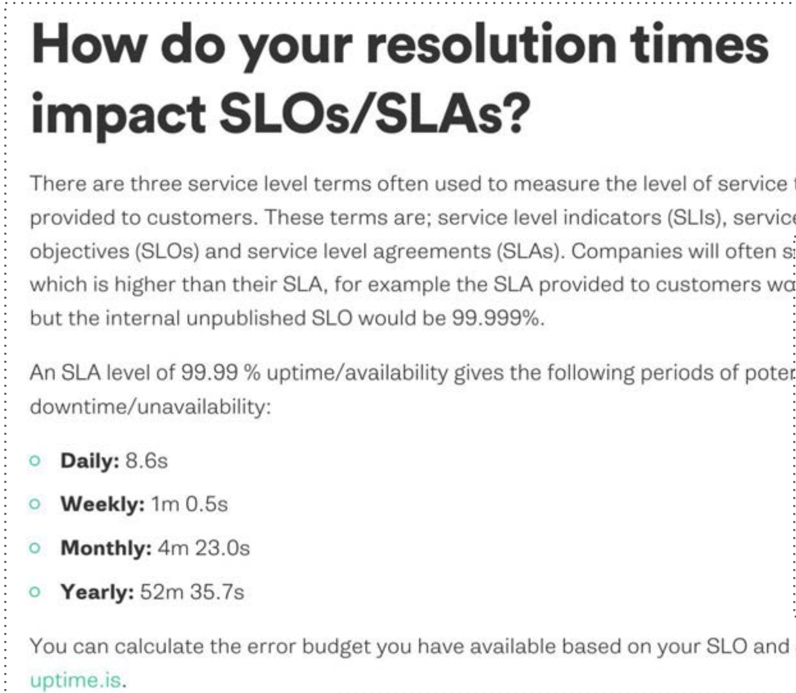
How are SEVs measured?

High Severity Incidents (SEVs) are measured by the availability error rate a impact. We use the formula below to identify the number of customer requ impacted:

```
% loss * outage duration
```

https://www.gremlin.com/

SEV



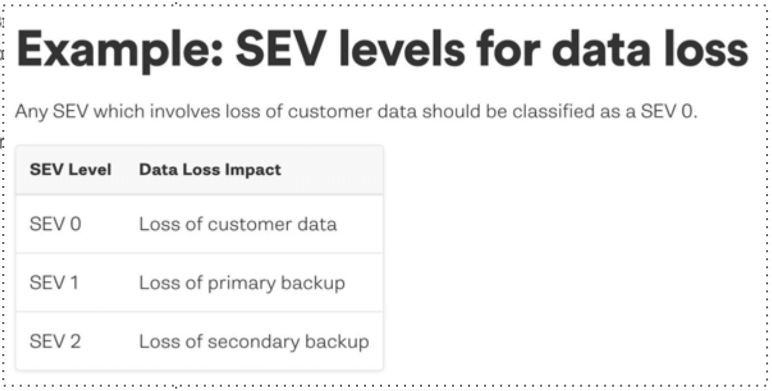
How do your resolution times impact SLOs/SLAs?

There are three service level terms often used to measure the level of service that will be provided to customers. These terms are; service level indicators (SLIs), service level objectives (SLOs) and service level agreements (SLAs). Companies will often s which is higher than their SLA, for example the SLA provided to customers wo but the internal unpublished SLO would be 99.999%.

An SLA level of 99.99 % uptime/availability gives the following periods of poter downtime/unavailability:

- **Daily:** 8.6s
- **Weekly:** 1m 0.5s
- **Monthly:** 4m 23.0s
- **Yearly:** 52m 35.7s

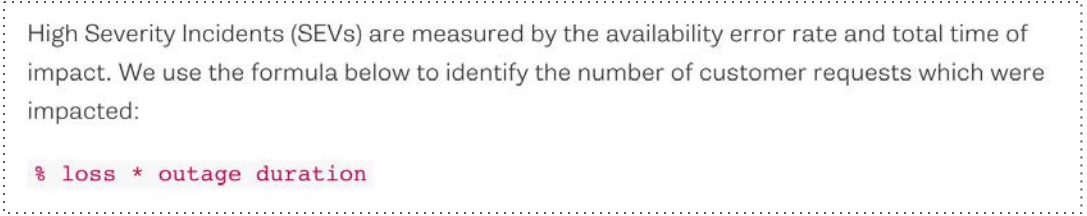
You can calculate the error budget you have available based on your SLO and SLA at uptime.is.



Example: SEV levels for data loss

Any SEV which involves loss of customer data should be classified as a SEV 0.

SEV Level	Data Loss Impact
SEV 0	Loss of customer data
SEV 1	Loss of primary backup
SEV 2	Loss of secondary backup



High Severity Incidents (SEVs) are measured by the availability error rate and total time of impact. We use the formula below to identify the number of customer requests which were impacted:

```
% loss * outage duration
```

https://www.gremlin.com/

What about **[Security]**?

If security teams have largely focused on confidentiality and reliability, when the issue is a cyberattack we don't commit ...

Security

Which should be the SLA?

Environment	Develop		Stage		Production	
Incident	AT	RT	AT	RT	AT	RT
High Priority Affected service/ degraded operation	00:15	01:00	00:15	03:00	00:15	04:00
Medium Priority Imminent service affected	00:15	02:00				
Low Priority Not affected service	00:15	04:00	00:15	08:00	00:15	10:00

Disclaimer

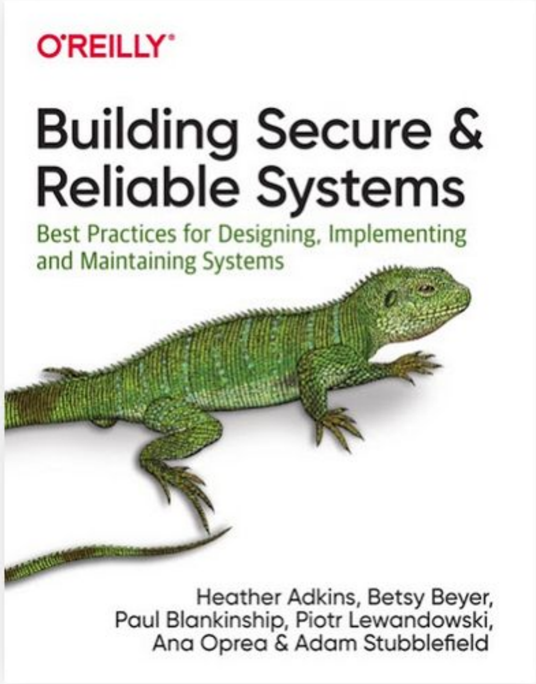
This does not apply if the incident is related to Security

** AT Attention Time hh:mm
** RT Resolution Time hh:mm

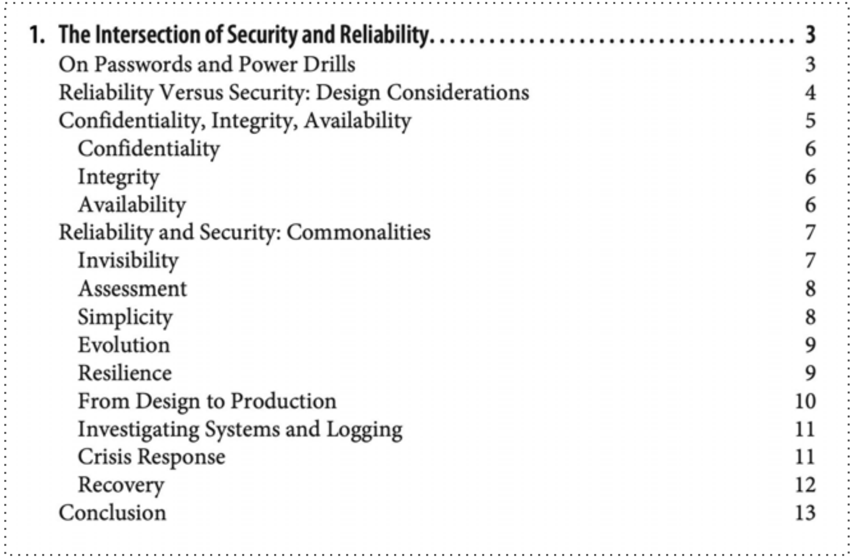
https://www.yurynino.dev/

Security

I went to the Books!

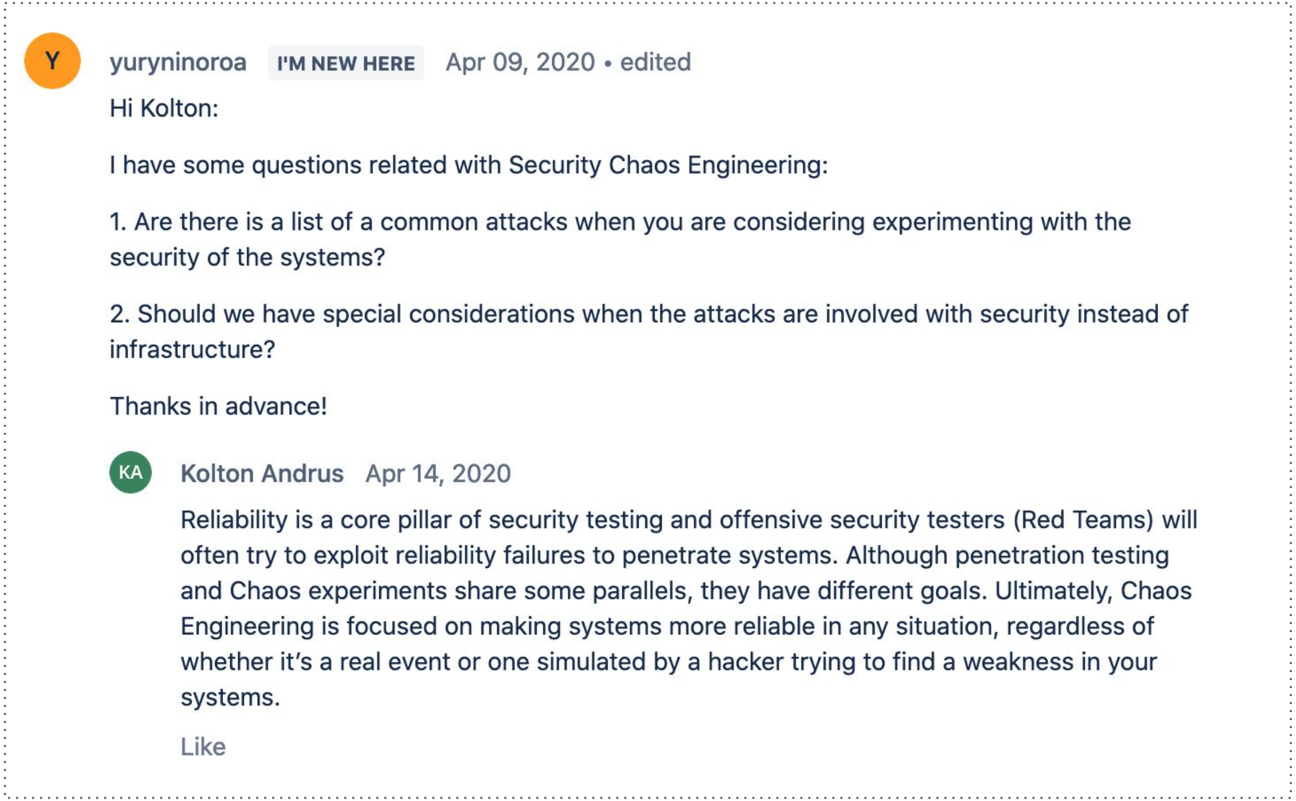

O'REILLY
Building Secure & Reliable Systems
Best Practices for Designing, Implementing and Maintaining Systems
Heather Adkins, Betsy Beyer, Paul Blankinship, Piotr Lewandowski, Ana Oprea & Adam Stubblefield

Security and Reliability, both features are often hidden in their expectations: if they're working well, your customers don't notice them.



Security

I asked the Experts!



yuryninoroa I'M NEW HERE Apr 09, 2020 • edited

Hi Kolton:

I have some questions related with Security Chaos Engineering:

1. Are there is a list of a common attacks when you are considering experimenting with the security of the systems?

2. Should we have special considerations when the attacks are involved with security instead of infrastructure?

Thanks in advance!

Kolton Andrus Apr 14, 2020

Reliability is a core pillar of security testing and offensive security testers (Red Teams) will often try to exploit reliability failures to penetrate systems. Although penetration testing and Chaos experiments share some parallels, they have different goals. Ultimately, Chaos Engineering is focused on making systems more reliable in any situation, regardless of whether it's a real event or one simulated by a hacker trying to find a weakness in your systems.

Build a Culture of **Security** and **Reliability**

Training Security Teams...

https://www.yurynino.dev/

Define Roles

Designer/Facilitator

The person leading the discussion

Scribe

Takes notes in a communication tool, such as Slack, on what is occurring in the room.

Observer

Looks at and shares relevant graphs with the rest of the group.

Commander

The person executing the commands.

Correspondent

keeps an eye on #alerts-channel and makes sure the on-call is aware of the experiment occurring and what the expected impact is.

https://www.yurynino.dev/
Chaos Engineering Book

Training

Red Team Exercises

- They were originated with the US Armed Forces by Bryce Hoffman.
- Adversarial approach that imitates the behaviors and techniques of attackers in the most realistic way possible.
- Two common forms of **Red Teaming** seen in the enterprise are:
  - Ethical hacking
  - Penetration testing.
- **Blue Teams** are the defensive counterparts to the Red teams in these exercises.
- Recommendations: Think-Write-Share and Devil’s advocacy.

https://whatis.techtarget.com

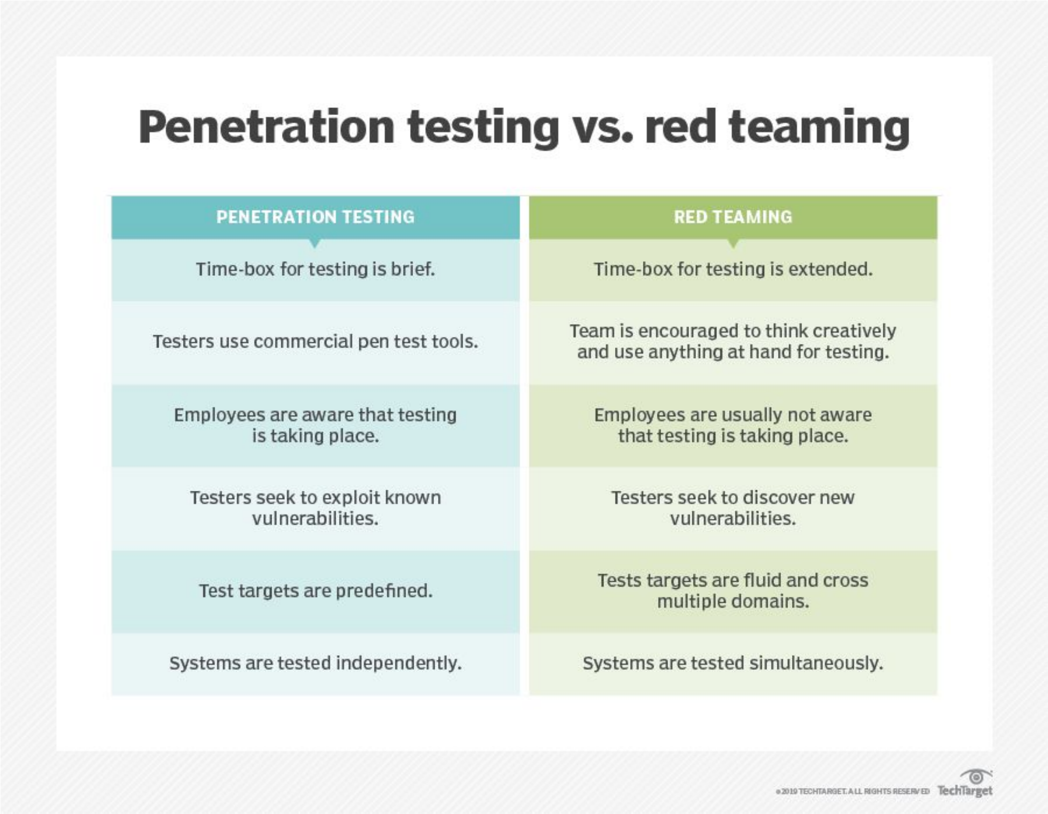
Purple Team Exercises

- They were intended as an evolution of **Red Team** exercises by delivering a more cohesive experience between the offensive and defensive teams.
- The **“Purple” in Purple Teaming** reflects the cohesion of **Red** and **Blue** Teaming.
- The goal of these exercises is the collaboration of offensive and defensive tactics to improve the effectiveness of both groups in the event of an attempted compromise.
- The intention is to increase transparency as well as provide a conduit for the security apparatus to learn about how effective their preparation is when subjected to a live fire exercise.

https://whatis.techtarget.com

Training

Strategies



Penetration testing vs. red teaming

PENETRATION TESTING	RED TEAMING
Time-box for testing is brief.	Time-box for testing is extended.
Testers use commercial pen test tools.	Team is encouraged to think creatively and use anything at hand for testing.
Employees are aware that testing is taking place.	Employees are usually not aware that testing is taking place.
Testers seek to exploit known vulnerabilities.	Testers seek to discover new vulnerabilities.
Test targets are predefined.	Tests targets are fluid and cross multiple domains.
Systems are tested independently.	Systems are tested simultaneously.

https://whatis.techtarget.com

PenTests are not enough!

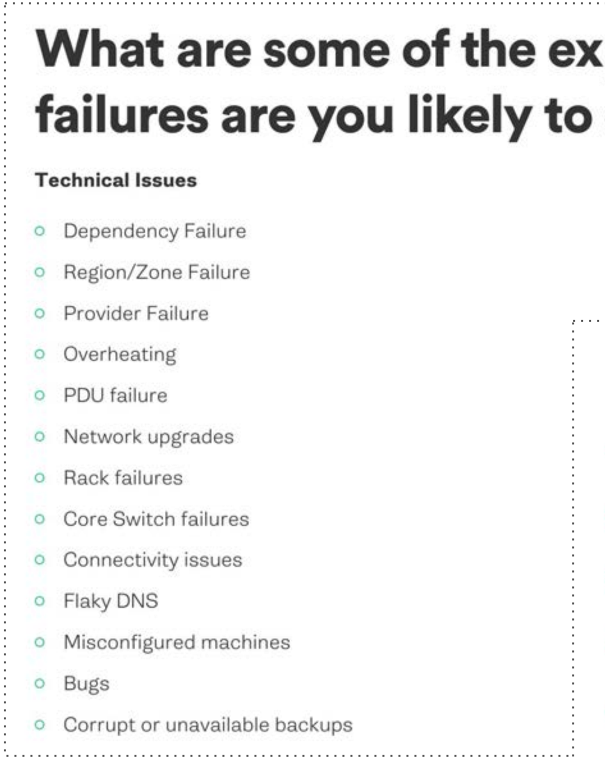
This requires a fundamentally new approach to cybersecurity, one that keeps pace with the rapidly evolving world of software engineering.

What is Chaos Engineering?

It is the discipline of experimenting failures in production in order to reveal their weakness and to build confidence in their resilience capability.

https://principlesofchaos.org/

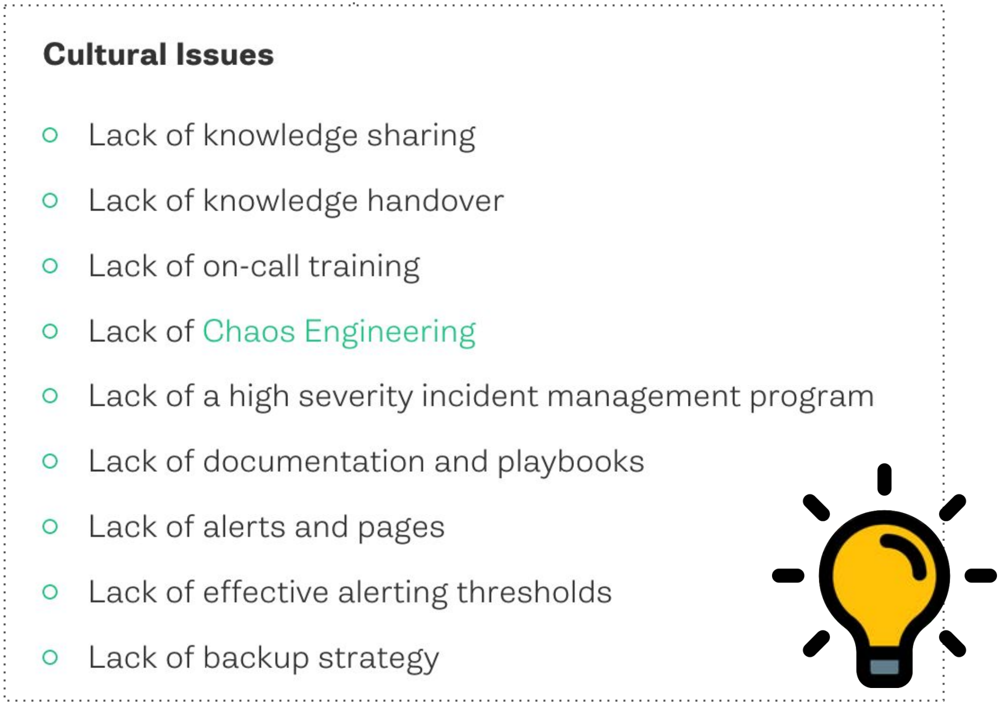
Attacks



What are some of the expected failures are you likely to experience?

Technical Issues

- Dependency Failure
- Region/Zone Failure
- Provider Failure
- Overheating
- PDU failure
- Network upgrades
- Rack failures
- Core Switch failures
- Connectivity issues
- Flaky DNS
- Misconfigured machines
- Bugs
- Corrupt or unavailable backups



Cultural Issues

- Lack of knowledge sharing
- Lack of knowledge handover
- Lack of on-call training
- Lack of Chaos Engineering
- Lack of a high severity incident management program
- Lack of documentation and playbooks
- Lack of alerts and pages
- Lack of effective alerting thresholds
- Lack of backup strategy

https://www.gremlin.com/

What about **[Security]**? Again!!

Friendly Reminder: If security teams have largely focused on confidentiality and reliability, when the issue is a cyberattack we don't commit …

What is Security Chaos Engineering?

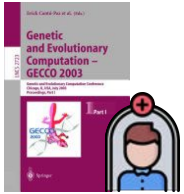
It is the identification of security control failures through proactive experimentation to build confidence in the system’s ability to defend against malicious conditions in production.

Chaos Engineering Book. 2020

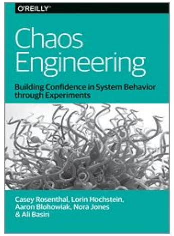
History

TECHNOLOGY RADAR

Search · About the Radar · Build your Radar · Subscribe

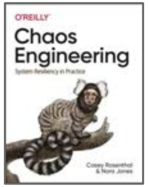


Artificial Immune Systems


O'REILLY
Chaos Engineering
Building Confidence in System Behavior through Experiments
Casey Rosenthal, Lorin Hochstein, Aaron Blohowiak, Nora Jones & Ali Basiri

Aaron Rinehart
first articles

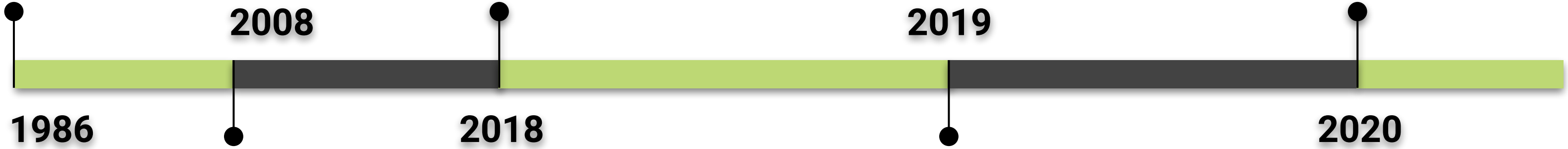
ChaoSlingr



Security Chaos Engineering for Cloud Services
(Work In Progress)

Kennedy A. Torkura, Muhammad I.H. Sukmana, Feng Cheng and Christoph Meinel
Hasso-Plattner-Institute for Digital Engineering,
University of Potsdam,
Potsdam, Germany
Email: firstname.lastname@hpi.de

Chapter dedicated to **Security CE**



Chaos Engineering
was born

NETFLIX

Artificial Intelligence
for data security

CROWDSTRIKE

VERICA

O'REILLY Velocity

https://www.yurynino.dev/

It is not the intention to overlook the value of Red and Purple Team Exercises or other security testing methods.

With Security Chaos Engineering we can introduce false positives into production, to check whether procedures are capable of identifying security failures under controlled conditions.

Chaos Engineering Book. 2020

- - -

Chaos GameDays

Everything fails, all the time! ...

Werner Vogels

https://www.yurynino.dev/

Current

GameDays → Chaos Gamedays

AWS GameDay

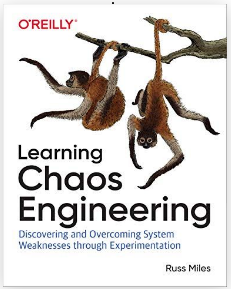
GameDays are interactive team-based learning exercises designed to give players a chance to put their skills to the test in a real-world, gamified, risk-free environment.

powered by aws

A **Chaos GameDay** is a practice event, and although it *can* take a whole day, it usually requires only a few hours. The goal of a **GameDay** is to practice how you, your team, and your supporting systems deal with real-world turbulent conditions.

DIUS

TARGET


O'REILLY

Learning Chaos Engineering

Discovering and Overcoming System Weaknesses through Experimentation

Russ Miles

Current

Framework

Before

- Pick a hypothesis.
- Pick a style.
- Decide who.
- Decide where.
- Decide when.
- Document.
- Get approval!

During

- Detect the situation.
- Take a deep breath.
- Communicate.
- Visit dashboards.
- Analyze data.
- Propose solutions.
- Apply and solve!

After

- Write a postmortem.
- What Happened
- Impact
- Duration
- Resolution Time
- Resolution
- Timeline
- Action Items

https://www.yurynino.dev/

Human factors in cybersecurity are perhaps the biggest challenge when building an effective threat prevention strategy.

Vircom

Considerations for

Security Chaos **GameDays**

OUR FRAMEWORK

Our

Framework

Before

- Pick a hypothesis.
- Pick a style.
- Decide who.
- Decide where.
- Decide when.
- Document.
- Get approval!

During

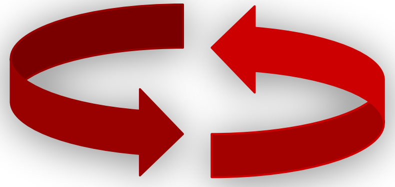
- Detect the situation.
- Take a deep breath.
- Communicate.
- Visit dashboards.
- Analyze data.
- Propose solutions.
- Apply and solve!

After

- Write a postmortem.
- What Happened
- Impact
- Duration
- Resolution Time
- Resolution
- Timeline
- Action Items

Evolve

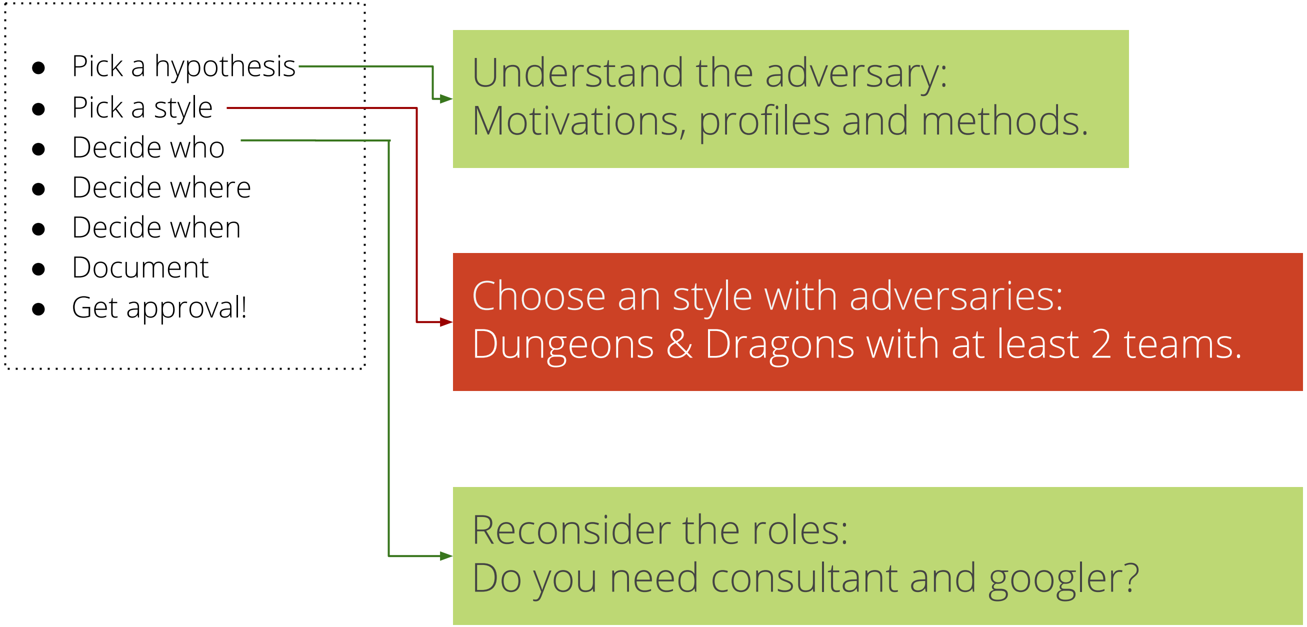
- Improve vulnerability DB.
- Refine the process.
- Adjust metrics.
- Validate CMM position.
- Adapt next Gameday.
- Continuous Verification.



https://www.yurynino.dev/

Before

Considerations



- Pick a hypothesis
- Pick a style
- Decide who
- Decide where
- Decide when
- Document
- Get approval!

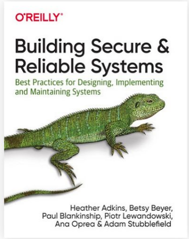
Understand the adversary:
Motivations, profiles and methods.

Choose an style with adversaries:
Dungeons & Dragons with at least 2 teams.

Reconsider the roles:
Do you need consultant and googler?

During

Considerations


O'REILLY
Building Secure & Reliable Systems
Best Practices for Designing, Implementing and Maintaining Systems
Heather Adkins, Betsy Beyer, Paul Blankinship, Piotr Lewandowski, Ana Oprea & Adam Stubblefield

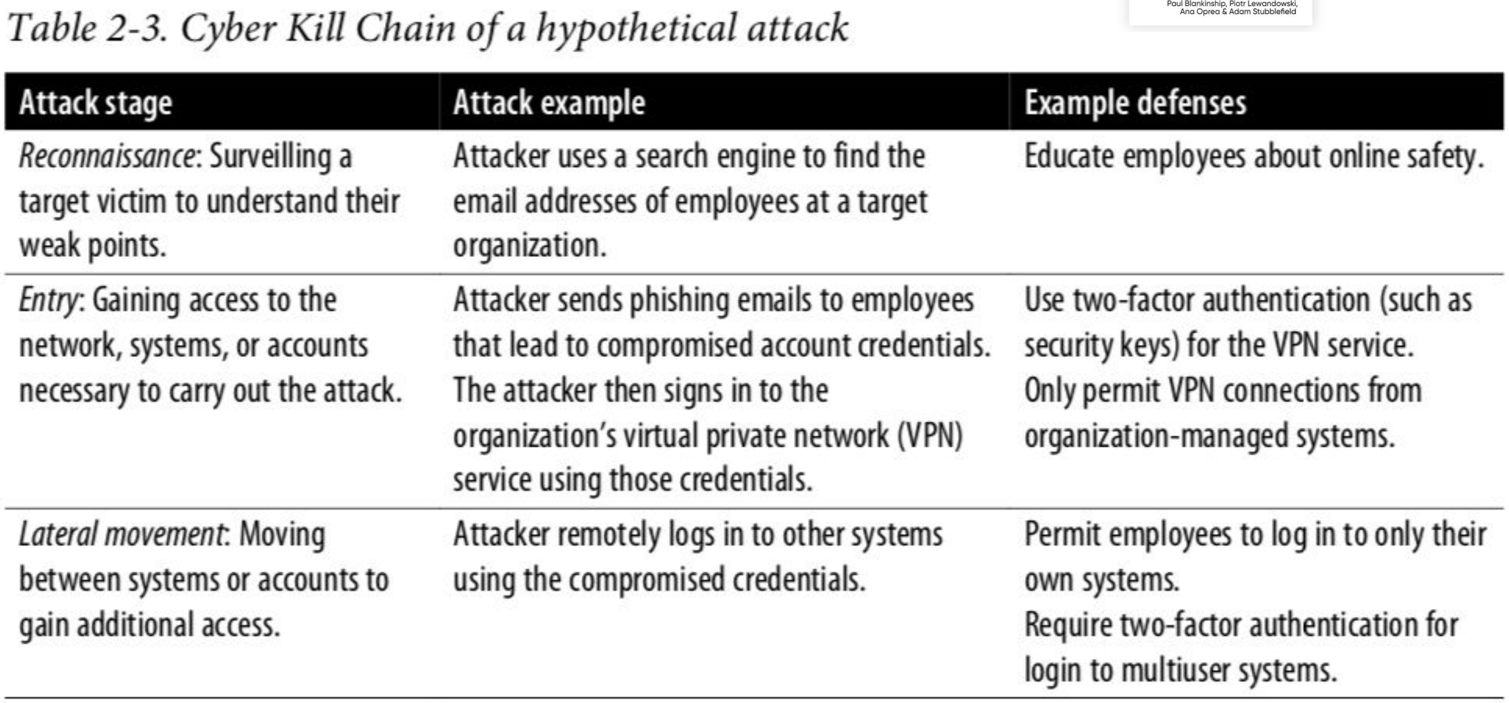


Table 2-3. Cyber Kill Chain of a hypothetical attack

Attack stage	Attack example	Example defenses
Reconnaissance: Surveilling a target victim to understand their weak points.	Attacker uses a search engine to find the email addresses of employees at a target organization.	Educate employees about online safety.
Entry: Gaining access to the network, systems, or accounts necessary to carry out the attack.	Attacker sends phishing emails to employees that lead to compromised account credentials. The attacker then signs in to the organization's virtual private network (VPN) service using those credentials.	Use two-factor authentication (such as security keys) for the VPN service. Only permit VPN connections from organization-managed systems.
Lateral movement: Moving between systems or accounts to gain additional access.	Attacker remotely logs in to other systems using the compromised credentials.	Permit employees to log in to only their own systems. Require two-factor authentication for login to multiuser systems.

During

Considerations

- Introduce latency on security controls.
- Drop a folder like a script would do in production.
- Software secret clear text disclosure.
- Permission collision in a shared IAM role policy.
- Disable service event logging.
- API gateway shutdown.
- Unencrypted S3 Bucket.
- Disable MFA.

During

Hypothesis:

After the owner of Root account in AWS left the company, we could use our cloud in a normal way.

Result:

Hypothesis disproved. In this experiment the access to AWS was connected to the Active Directory. When an employee left the company his account is dropped and we lost the access to AWS.

Side Effect:

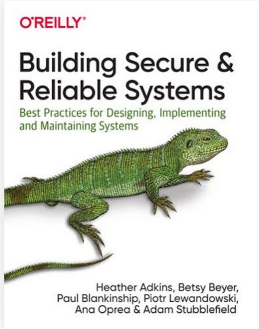
Thinking in this scenario allows to consider another applications connected to Active Directory.

After

Considerations

A **security postmortem** covers technology issues that the attacker exploited, and also recognizes opportunities for improved incident handling.

Document the time frames and efforts associated with these action items, and decide which action items.

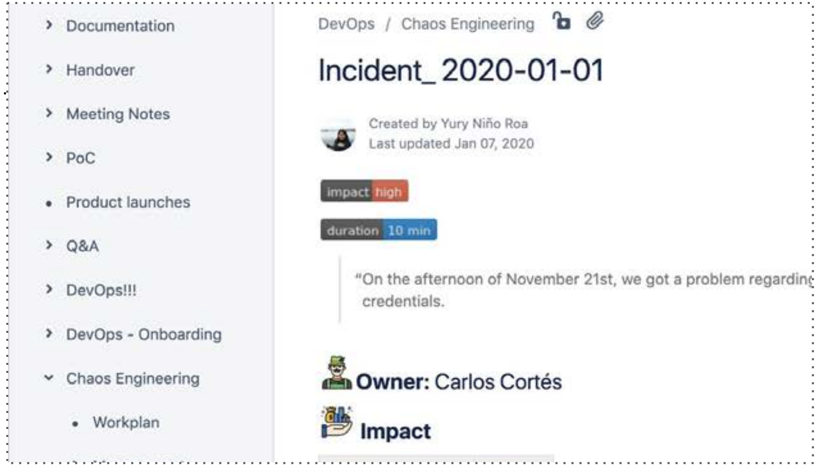


O'REILLY

Building Secure & Reliable Systems

Best Practices for Designing, Implementing and Maintaining Systems

Heather Adkins, Betsy Beyer,
Paul Blankinship, Piotr Lewandowski,
Ana Oprea & Adam Stubblefield



Incident_ 2020-01-01

Created by Yury Niño Roa
Last updated Jan 07, 2020

impact high

duration 10 min

> "On the afternoon of November 21st, we got a problem regarding credentials.

Owner: Carlos Cortés

Impact

https://www.yurynino.dev/

Evolution

Considerations

- Improve vulnerability DB.
- Refine the process.
- Adjust metrics.
- Validate CMM position.
- Adapt next Gameday.
- Continuous Verification.

Continuous Verification encourages both of these requirements in a way that proactively educates engineers about the systems they operate.

It is emerging as a crucial practice for navigating complex software systems.

Continuous Verification is a game changer for complex software system management. In the future it will fundamentally change the scale and types of systems that we even consider building.

Learnings & Challenges

It is a fact that the future only can be improved if something is learned from past.

Resilience Engineering Book.

Learnings

Our Journey

- The adoption of SCE faces challenges: human factors to **Security issues.**
- Reducing potential damage and blast radius is critical in **Security.**
- Communication and observability: successful **Chaos Security GameDays.**
- Requirements may collision with experimentation in **Security.**
- You don’t need to be a security expert to start with **Security CE.**

Challenges

For the Future ...

The adoption of the **Security** Chaos Engineering principles across organizations remains as an open challenge.

Security may be included in the **Chaos Maturity Model** since combining a CMM and Security Chaos GameDays help newcomers to start their CE efforts and allow to build resilience on security.

It's an exciting time to be working in this space.

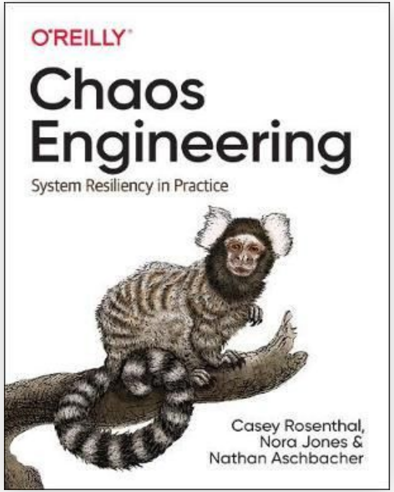
Humans operate differently when they expect things to fail!

Aaron Rinehart

References

My Recommended

Books

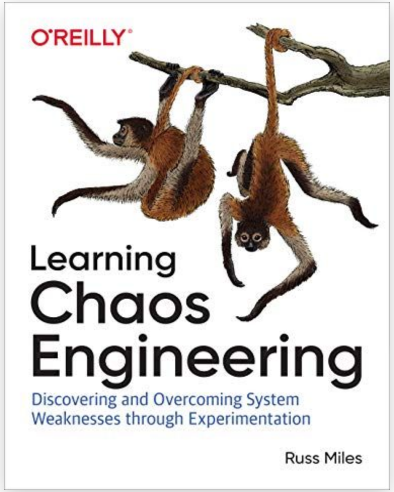


O'REILLY

Chaos Engineering

System Resiliency in Practice

Casey Rosenthal,
Nora Jones &
Nathan Aschbacher

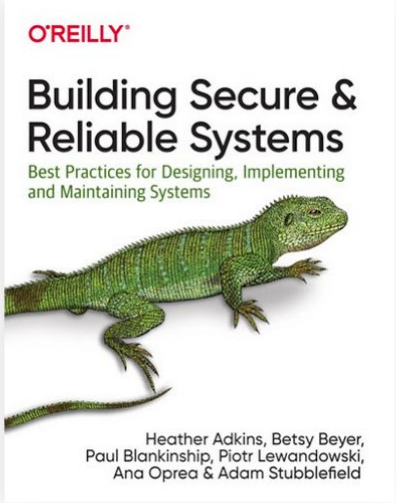


O'REILLY

Learning Chaos Engineering

Discovering and Overcoming System Weaknesses through Experimentation

Russ Miles

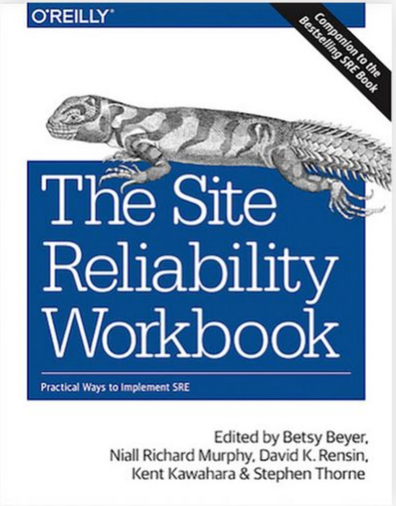


O'REILLY

Building Secure & Reliable Systems

Best Practices for Designing, Implementing and Maintaining Systems

Heather Adkins, Betsy Beyer,
Paul Blankinship, Piotr Lewandowski,
Ana Oprea & Adam Stubblefield



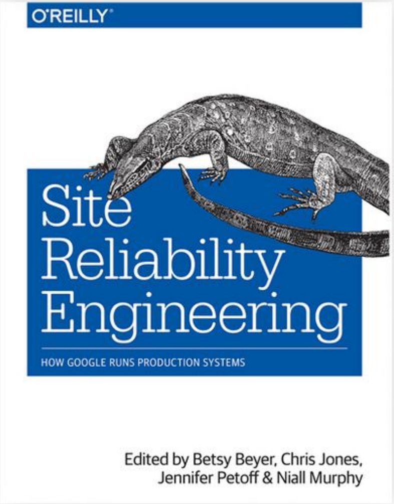
O'REILLY

Companion to the Bestselling SRE Book

The Site Reliability Workbook

Practical Ways to Implement SRE

Edited by Betsy Beyer,
Niall Richard Murphy, David K. Rensin,
Kent Kawahara & Stephen Thorne



O'REILLY

Site Reliability Engineering

HOW GOOGLE RUNS PRODUCTION SYSTEMS

Edited by Betsy Beyer, Chris Jones,
Jennifer Petoff & Niall Murphy

Don’t fear failure. In great attempts it is glorious even to fail.

Anonymous

One single vulnerability is all an attacker needs.

Window Snyder
Chief Security Officer, Fastly

@yurynino

Thanks for coming!