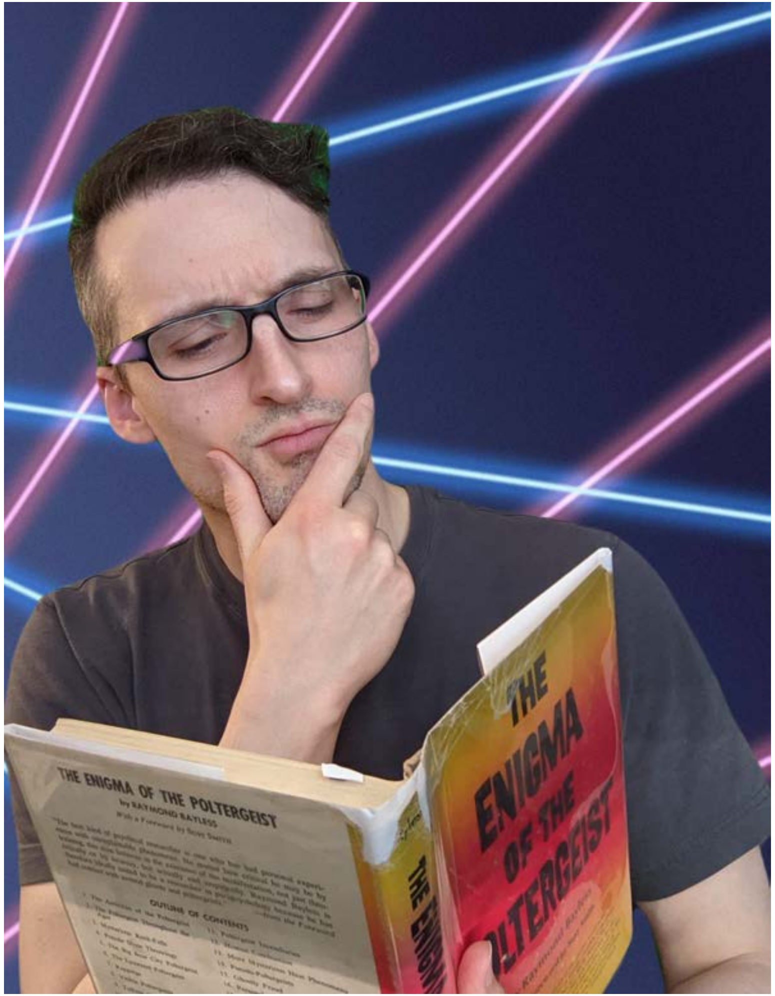
CONF42 CHAOS ENGINEERING 2024

FEBRUARY 15 • ONLINE

Security Chaos Engineering

How to Fix Things (you didn't know were broken) and Make Friends While Doing It



David Lavezzo

- Makes people happy
- Makes people sad
- Writes music
- Done Security Chaos Engineering since 2017
- Contributing Author on *Security Chaos Engineering Report*, and *Security Chaos Engineering: Sustaining Resilience in Software and Systems*

Please Note

- This is not Red Teaming
- This is not a Penetration Test
- This helps take care of the fundamentals before paying pure Offensive teams to steal your lunch money

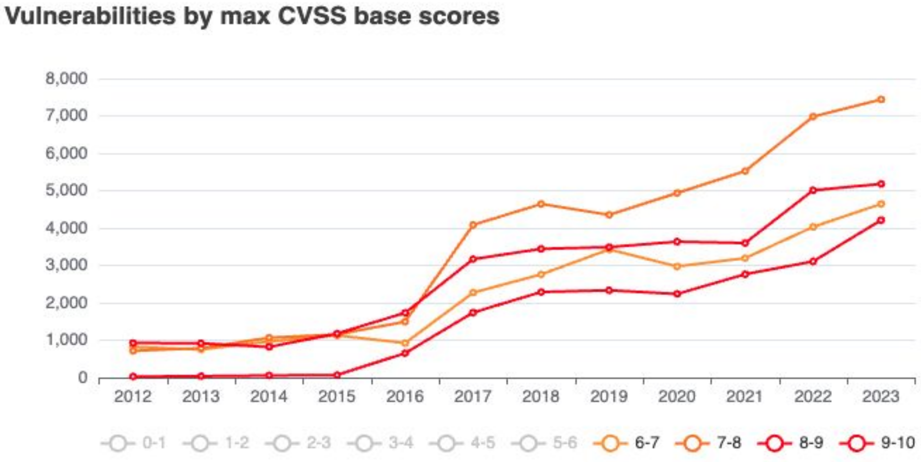
Part 1 - Nothing works how we think it works

Doom loops are scary and impede the decision making process

- Constant bombardment on threats that only $vendor tool can protect against
- Advanced threats everywhere while companies everywhere struggle with fundamentals
- Bloodhound is still frightening
- How do we identify how things actually work?

Is Security getting better, or better at shifting responsibility?

- Vulnerabilities keep climbing
- Verizon DBIR points to misconfigurations, not vulns
- Security often does not operate at the speed of business
- Shift left!
- Complicated



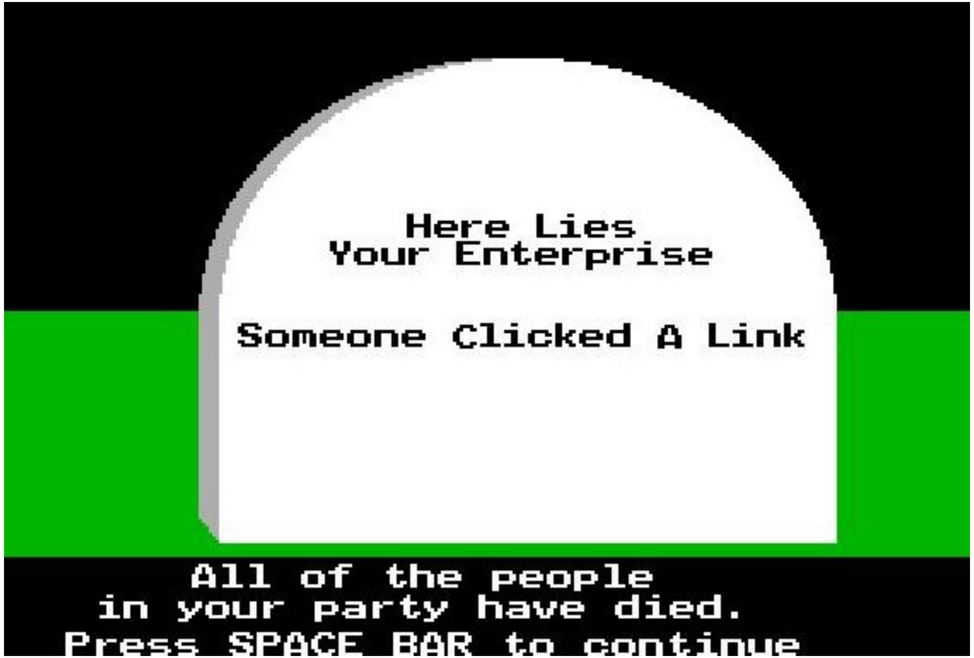
With all the hot fresh defensive tools available, making it all work together is still difficult

- “The basics” are actually kind of hard
  - Why do so many struggle with native controls and instead pay vendors to manage the control
- What are we protecting?
- Need to understand how tools work, if they work, and continue to work
- Bad user experience doesn’t make it easy

Security incidents are poor methods to measure detection because the bad thing already happened

- It’s too late. Fetch happened
- Three bullets look better than two
- We have to discover potential issues before they mature to incidents

Hope is not a valid strategy



Here Lies
Your Enterprise

Someone Clicked A Link

All of the people
in your party have died.
Press SPACE BAR to continue

Part not mean secure

WE NEED YOU ALL
TECH DEBT GUARANTEES EMPLOYMENT
WOULD YOU LIKE TO KNOW MORE ?
EH! 2013

SCE isn't creating chaos, it helps manage the chaos around us

- Reliable defenses are secure* defenses
- Planned changes can fundamentally alter how a system operates
- Failing safely is paramount
- Security restrictions create developer innovations in control bypassing

*yes I know nothing is secure, but I think you get the point

Failure is normal, expected, and should be embraced

- Complex systems have complex problems
- Failures in defenses can have many causes
  - Misconfigurations
  - Bugs
  - Configuration drift
- Stop focusing on preventing failure, embrace failure and adapt gracefully
- Attack trees w/https://www.deciduous.app/

Placeholder info

- Change stuff

Part 3 - Experiments in madness

Identifying what you care about is crucial to success

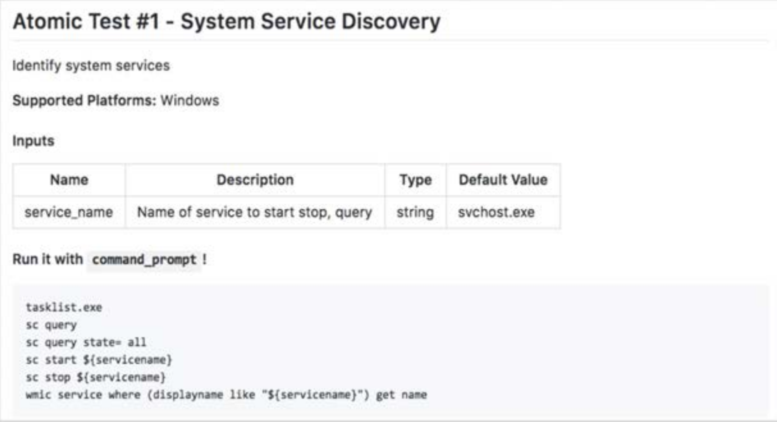
- What do your customers care about?
- What do you care about?
- How do you want to show your group is doing great work?
- Let’s prove your value

The Anatomy of an Experiment

- Design a hypothesis
  - “When X happens, we expect this system will respond with Y”
- Create an experiment
  - Outline why we’re doing it
  - What is expected to happen
- Collect evidence
  - Did everything work as expected?
  - Are there gaps or deviations?
- Repeat
  - Forever

Building your experiments

- Break down the attack
- thedfirreport.com is a good starting point
- It’s okay if you can’t do everything, start with what you can control
    - Endpoint is usually the easiest
    - Please don’t actually ransomware yourself
- For malicious payloads, go with something non-destructive
    - Like mimikatz
    - EICAR?



Atomic Test #1 - System Service Discovery

Identify system services

Supported Platforms: Windows

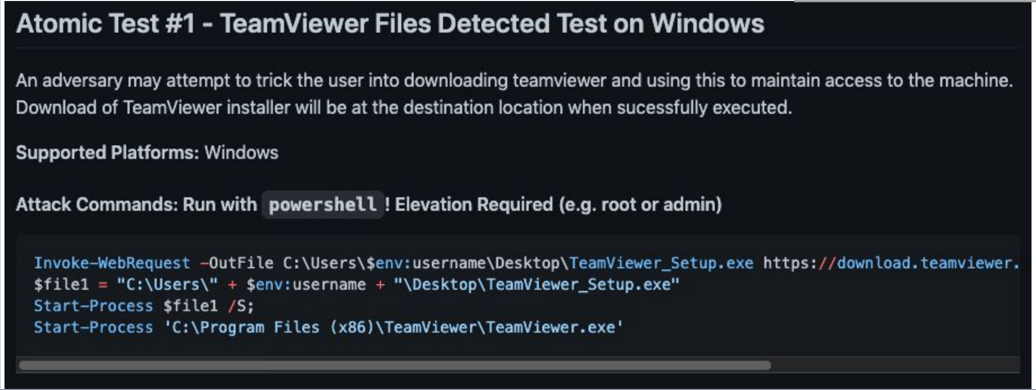
Inputs

Name	Description	Type	Default Value
service_name	Name of service to start stop, query	string	svchost.exe

Run it with `command_prompt` **!**

```
tasklist.exe
sc query
sc query state= all
sc start ${servicename}
sc stop ${servicename}
wmic service where (displayname like "${servicename}") get name
```

	endpoint	proxy	IDS	IPS
iwr	X	X	X	X
start-process	X			
tasklist	X			
sc query	X			
dreams				X



Atomic Test #1 - TeamViewer Files Detected Test on Windows

An adversary may attempt to trick the user into downloading teamviewer and using this to maintain access to the machine. Download of TeamViewer installer will be at the destination location when sucessfully executed.

Supported Platforms: Windows

Attack Commands: Run with `powershell` **! Elevation Required (e.g. root or admin)**

```
Invoke-WebRequest -OutFile C:\Users\$env:username\Desktop\TeamViewer_Setup.exe https://download.teamviewer.
$file1 = "C:\Users\" + $env:username + "\Desktop\TeamViewer_Setup.exe"
Start-Process $file1 /S;
Start-Process 'C:\Program Files (x86)\TeamViewer\TeamViewer.exe'
```

Events should be everywhere

Experiments in practice

Attack Stage	Description	Tags	Firewall	IPS	IDS	Web Proxy	HIDS	App Control	AV	EDR
Delivery	Staged Download	T1105								
Discovery	System Information Discovery	T1082								
Persistence	Modified Scheduled Task	T1053								
Command and Control	POST beacon	T1102								

This chart is for entertainment purposes only

Proving Outcomes

- Deploying Tool X will make us more secure
  - Prove it by comparing against the current baseline
- System Y is critical to the security of $thing
  - Design a hypothesis and an experiment to validate the assumption
  - If System Y experiences issues, what else will go wrong?
- We want/need systems that can adapt to failure
  - How do we work around it?
  - Can we make it more reliable?

Getting started is the hardest part

- You will likely have to generate your own buy-in
- Choose something simple, impactful, and measurable
- Best case scenario - Everything works as expected and you’ve created a great baseline
- Worst case scenario - nothing works and it’s time to start fixing
- Frameworks can come in handy

Part 4 - Measuring Stuff

Frameworks can help you decide what needs to be done

- What do your customers care about?
- What do you care about?
-

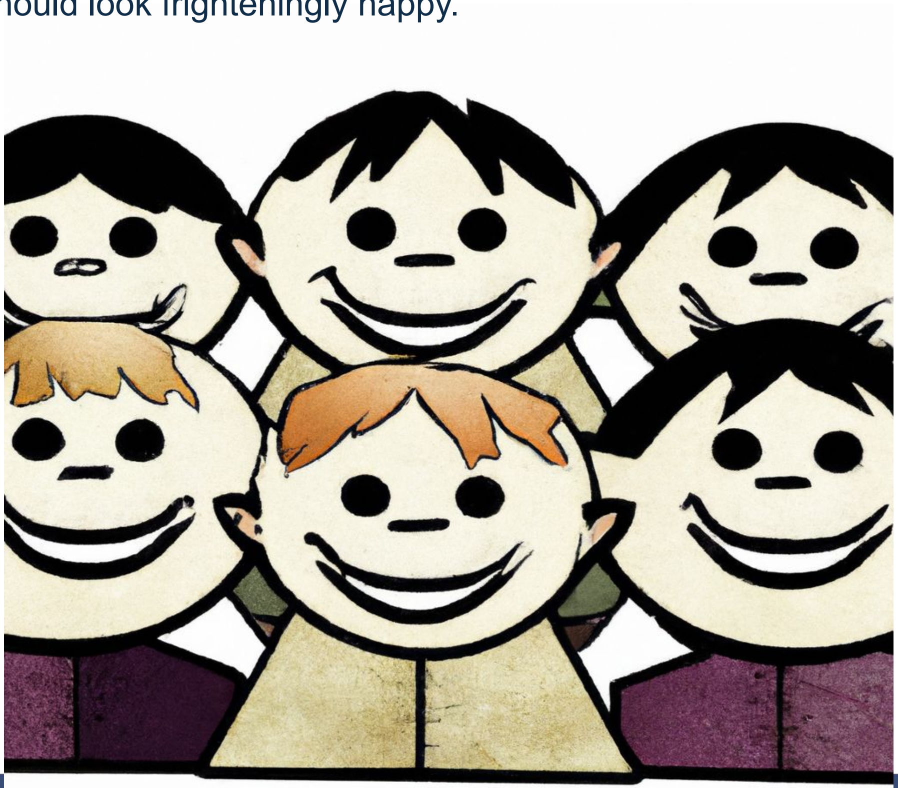
Measuring the reliability of defenses

- “We don’t know what we don’t know” needs to retire
- What if General Mills could only account for 8/10 Cheerios not containing pieces of glass?
- What percentage of glass are you missing?
- Raise the cost of a successful attack

Experiments in practice

Attack Stage	Description	Tags	Firewall	IPS	IDS	Web Proxy	HIDS	App Control	AV	EDR
Delivery	Staged Download	T1105	Missed	Logged	Logged	Logged	Logged	Blocked	Blocked	n/a
Discovery	System Information Discovery	T1082	n/a	n/a	n/a	n/a	Logged	Logged	Logged	Alerted
Persistence	Modified Scheduled Task	T1053	n/a	n/a	n/a	n/a	Logged	Missed	n/a	Alerted
Command and Control	POST beacon	T1102	Blocked	Missed	Logged	Logged	n/a	n/a	n/a	n/a

This chart is for entertainment purposes only an anime style photograph of five half human, half ravioli friends standing closely together smiling. They should look frighteningly happy.



Security Chaos Engineering shouldn’t be limited to engineering

- Hunting
  - Validating analytics continue to work as expected
  - Gap identification
- Architecture
  - Duplicative tooling where overlap is not desired
  - Coverage in depth
- Operations
  - Do critical alerts work? Will they continue to work?
  - What attacks are you vulnerable to? Do your tools work together to provide high quality signals for analysts?
- Product
  - Do you get expected value from expensive products?
  - Incremental improvement in security footprint and roadmap

Part 5 - Making Friends along the way

Making other programs better helps you make friends

- Enhancing friendships by helping teams look good
- Proving compliance by delivering secure programs
- Showing continuous improvements
- Supporting business objectives
- Building better systems

Security Chaos Engineering helps you ask better questions

- What are we building and why?
- Delivering protection designed to withstand failure
- How do we reduce the impact of a malicious actor in our environment?
- Not “what is the best AV we can buy?”

Making things palatable for others will make your life easier

- Start small in scope
- Not every miss is a gap to fix
- Understand you're looking at things differently and it may not align with common knowledge
- Target business goals
- Don't be a pigeon

YOU CAN DO IT

Part 6 - Stuff I learned along the way