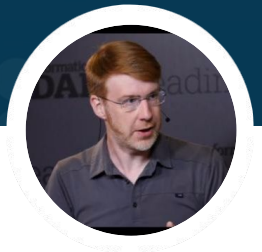
Security & SRE: Natural Force Multipliers

SREcon18

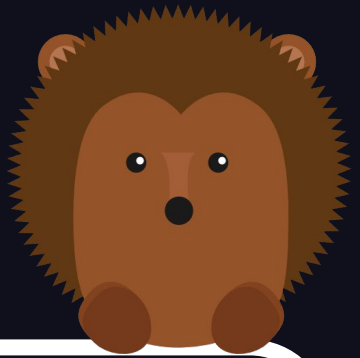


Cory Scott

CHIEF INFORMATION SECURITY OFFICER

Why should Security and SRE be so closely aligned?

LinkedIn's Engineering Hierarchy of Needs



"the fox knows many things, but the hedgehog knows one big thing."

-- Archilochus, *Greek Poet*

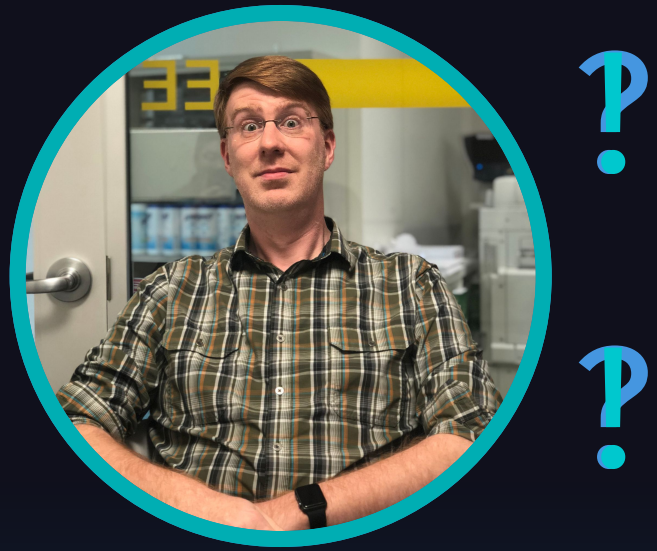

OS

2018

FAST RATE OF EVOLUTION

PRODUCT VISUALIZED IN AM, DEPLOYED IN PM

3RD PARTY ADOPTION EXPLODING



MICROSERVICE ARCHITECTURE SCALING TO MEET DEMANDS

DATACENTER TECH ACCESSIBLE FOR EVERYONE

"What's the state of product development and infrastructure?"

That seems..... great?

NETWORK ACCESS CONTROL?

ENDPOINT SECURITY PRODUCTS SUCH AS ANTI-VIRUS?

MAGIC BOXES?

BOUNTIES?

COMPLIANCE INITIATIVES?

CUSTOMER ASSURANCE?

"How are we doing on defense?"

What!?!

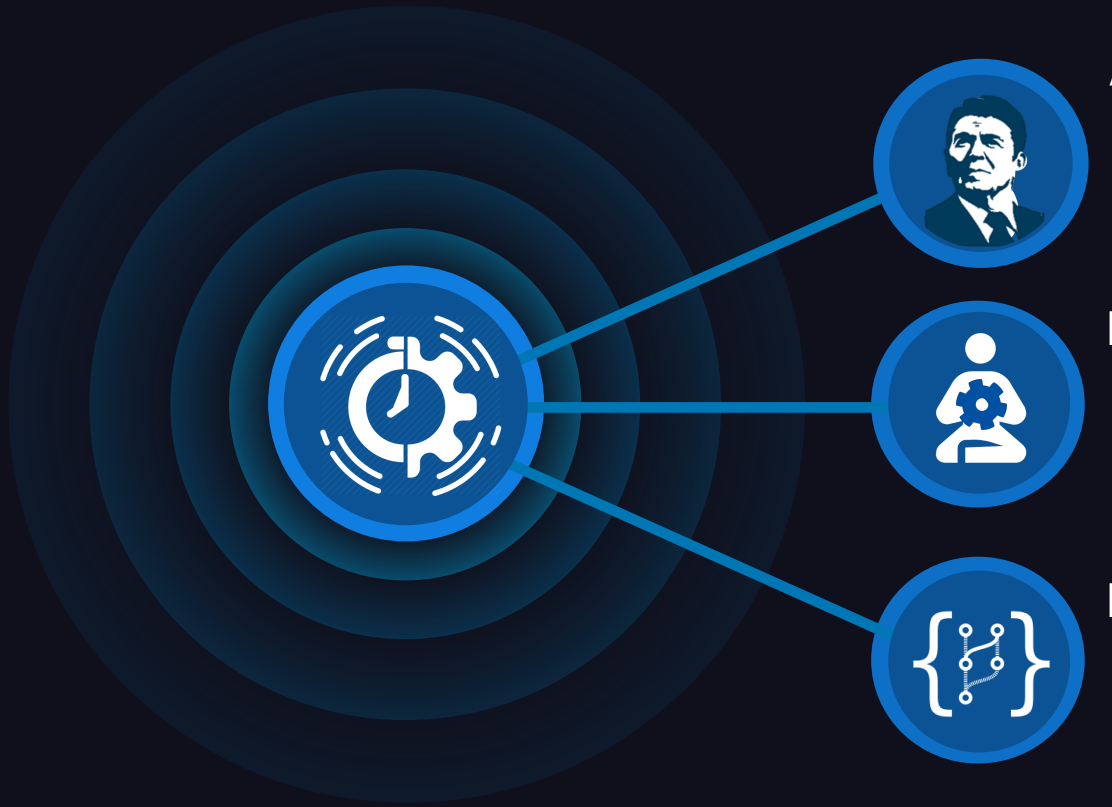
...

SRE Hierarchy of Needs from Google SRE book

Site Reliability Hierarchy of Needs

“Changes in production applications are happening at a greater rate than ever before. New product ideas can be visualized in the morning and implemented in code in the afternoon.”

Innovation and Rate Of Change



“Trust but Verify”

- Security to follow SRE “trust but verify” approach towards engineering partners

Embrace the Error Budget

- Self Healing & Auto Remediation
- Reduction of Manual Process

Inject Engineering Discipline

- Review when architecture changes reach a certain complexity point.

“Testing in production is the new norm”

Establishing Safe & Reliable Test Environments

“Microservice architectures are exploding to meet scalability requirements”

Microservice Architecture

SECURITY CHALLENGES ARE SIMILAR TO SRE

SRE Challenges

- Latency & Performance Impact
- Cascading Failure Scenarios
- Service Discovery

Security Challenges

- Authentication
- Authorization
- Access Control Logic

“Dependencies on third-party code and services can be collected faster than you can inventory them.”

Visibility in Your Third-Party Services

“Data center technologies can all be controlled with a single web application in the hands of a devops intern.”

Production Access & Change Control

- Start with a known-good state
- Asset management and change control discipline
- Ensure visibility
- Validate consistently and constantly

Configuration as code, leveraging source code control paradigms, are a huge boon to security. Rollback ruthlessly.

TAKEAWAYS OR GIVEAWAYS

(DEPENDING ON YOUR POSITION IN THE AUDIENCE)

Overall Lessons for Security

1

Your data pipeline is your security lifeblood

2

Human-in-the-loop is your last resort, not your first option

3

All security solutions must be scalable and default-on, just like SREs build it

Overall Lessons for SRE

1

Remove single points of security failure like you do for availability

2

Assume that an attacker can be anywhere in your system or flow

3

Capture and measure meaningful security telemetry