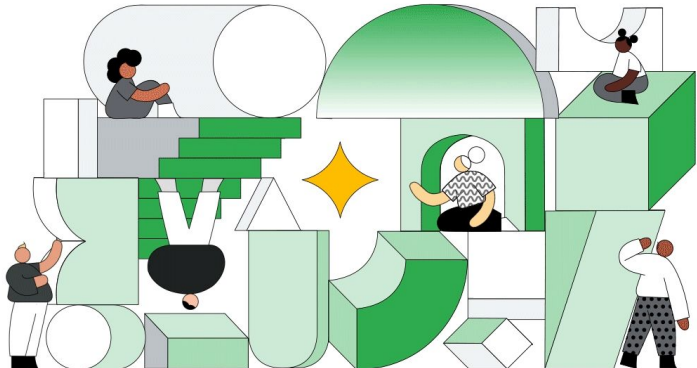
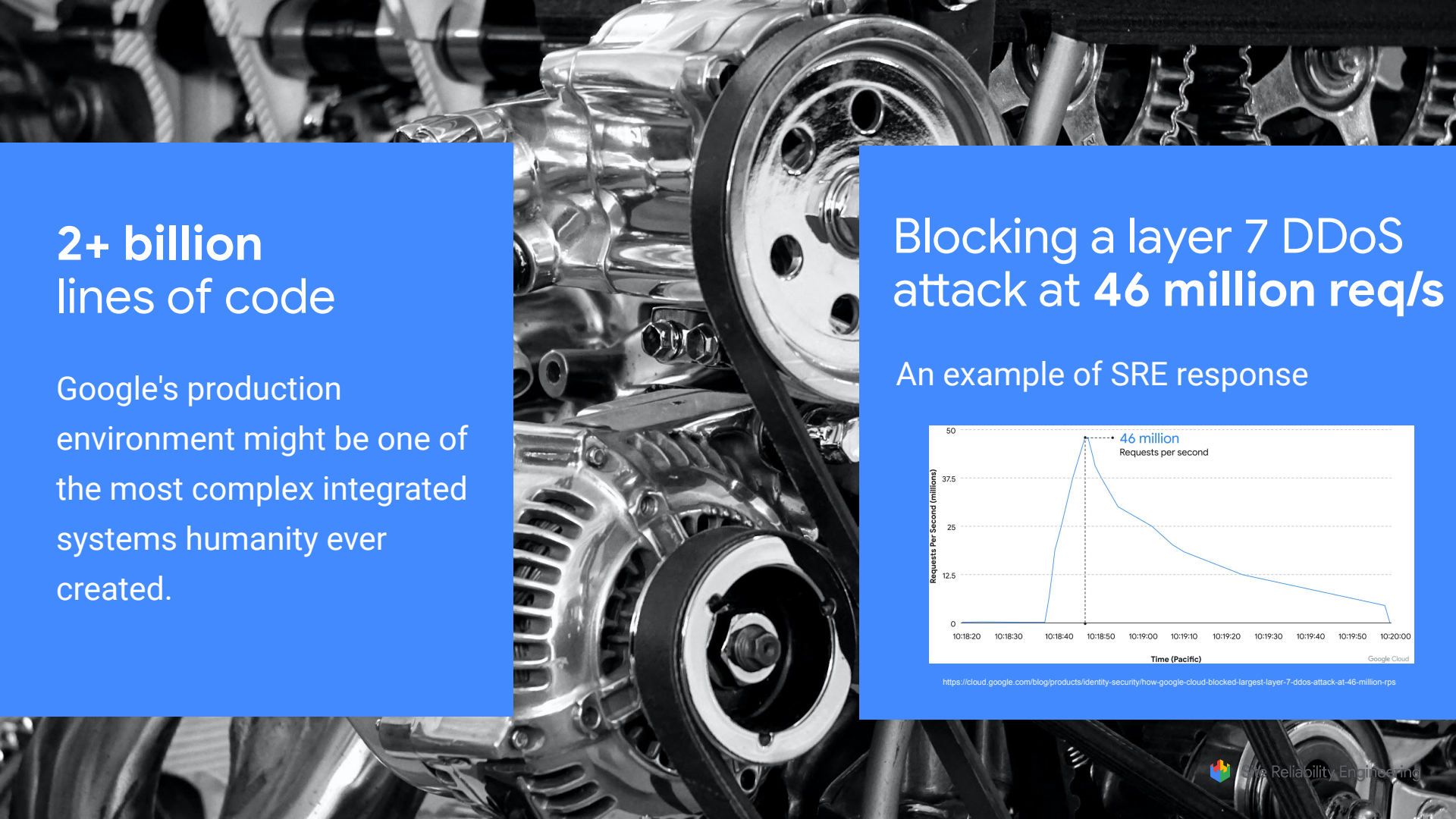
SRE for (cyber)security

Nicolas Fischbach

Senior Director, Security, Privacy, Resilience and Cloud AI Site Reliability Engineering

SRECON EUROPE MIDDLE EAST AFRICA





2+ billion lines of code

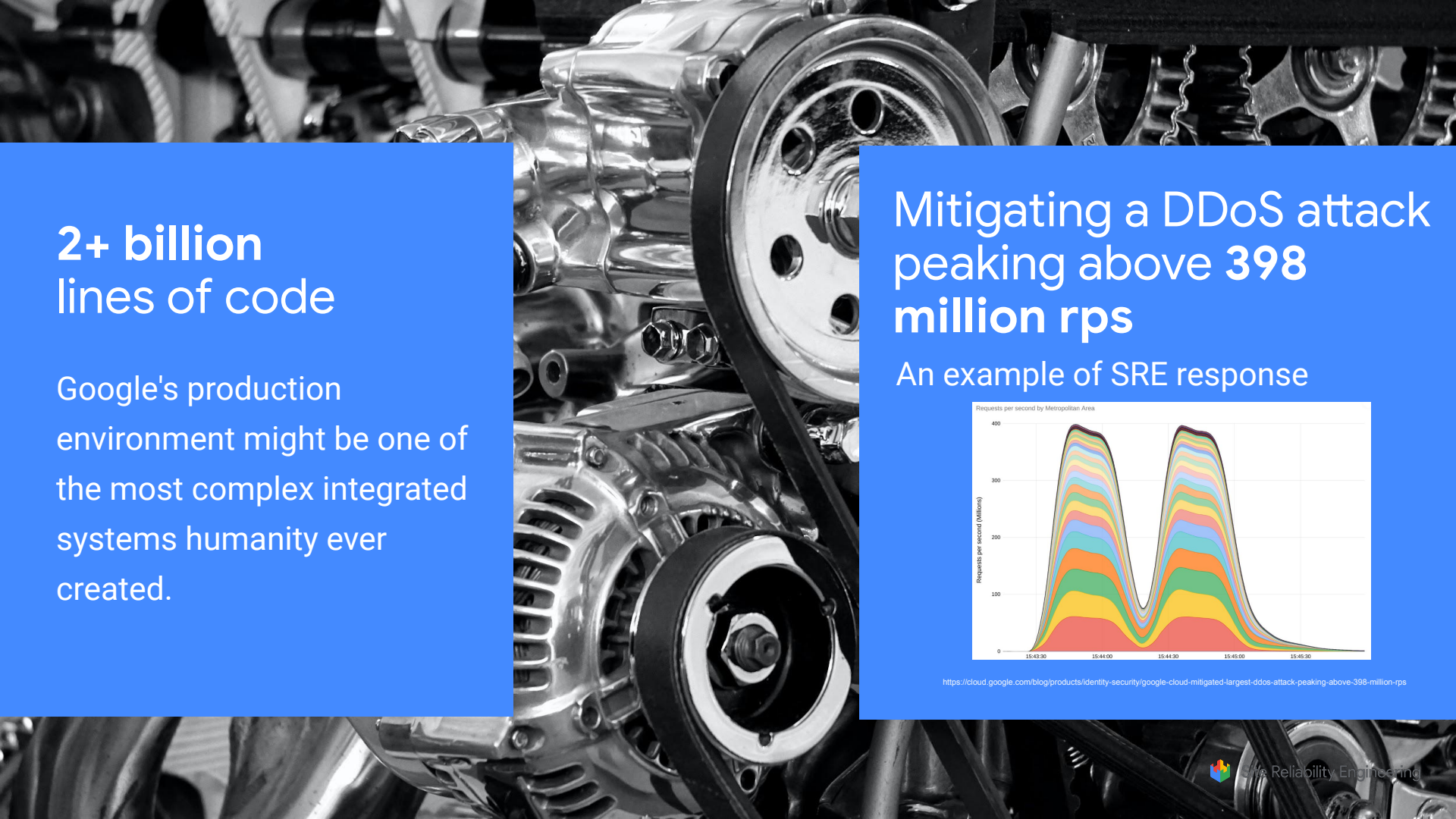
Google's production environment might be one of the most complex integrated systems humanity ever created.

Blocking a layer 7 DDoS attack at **46 million req/s**

An example of SRE response

https://cloud.google.com/blog/products/identity-security/how-google-cloud-blocked-largest-layer-7-ddos-attack-at-46-million-rps

Site Reliability Engineering



2+ billion lines of code

Google's production environment might be one of the most complex integrated systems humanity ever created.

Mitigating a DDoS attack peaking above **398 million rps**

An example of SRE response

https://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps

Site Reliability Engineering

What I'll be covering today

- Lessons learned, stories and tactics from operating:
  - Google's low-level infrastructure security services
  - Google's Cloud/GCP Security products (incl. internally invented which graduated)
- Insights into our research and how we protect Google from LPHC (Low Probability High Consequence) events
- SRE at Google: culture, goals and metrics
- How to translate this into an Enterprise model

Where do I start?

May sound very 101 but…

- Visibility is critical
  - Asset management (we all have our stories)
  - Monitoring
- Training and more training
  - Exercise your response procedures and skills
  - Documentation and playbooks
  - “No heroes” / blameless policy
- BC/DR
  - e.g. Backups: yes. Restore: … !?

… what’s different then? Planet-scale

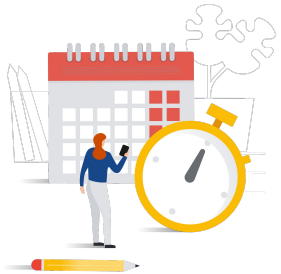
Oncall Health & Projects vs. Interrupts

Assessing pager fatigue, alert quality, and adequate team staffing:

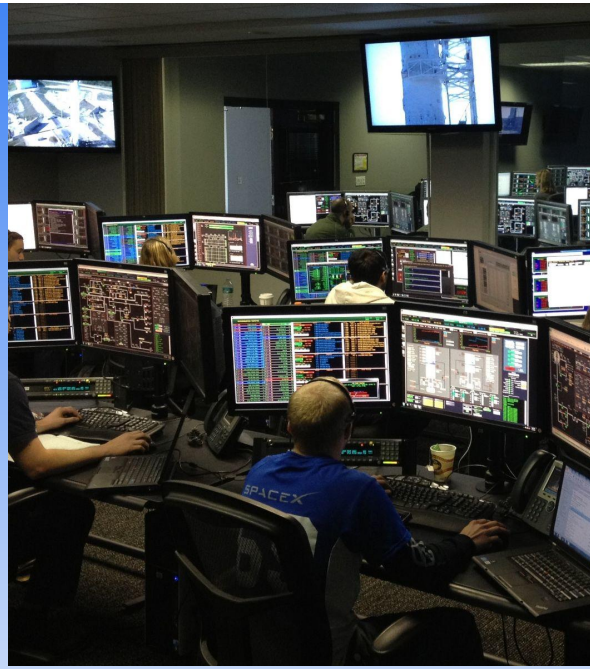
- Incident load
- Unactionable incidents
- Alert-to-incident ratio
- Oncall rotation staffing

Checking if the team has enough bandwidth to do impactful engineering work:

- OKR completion
- Ticket workload
- Interrupt escalation policy



Sounds like a SOC, no?



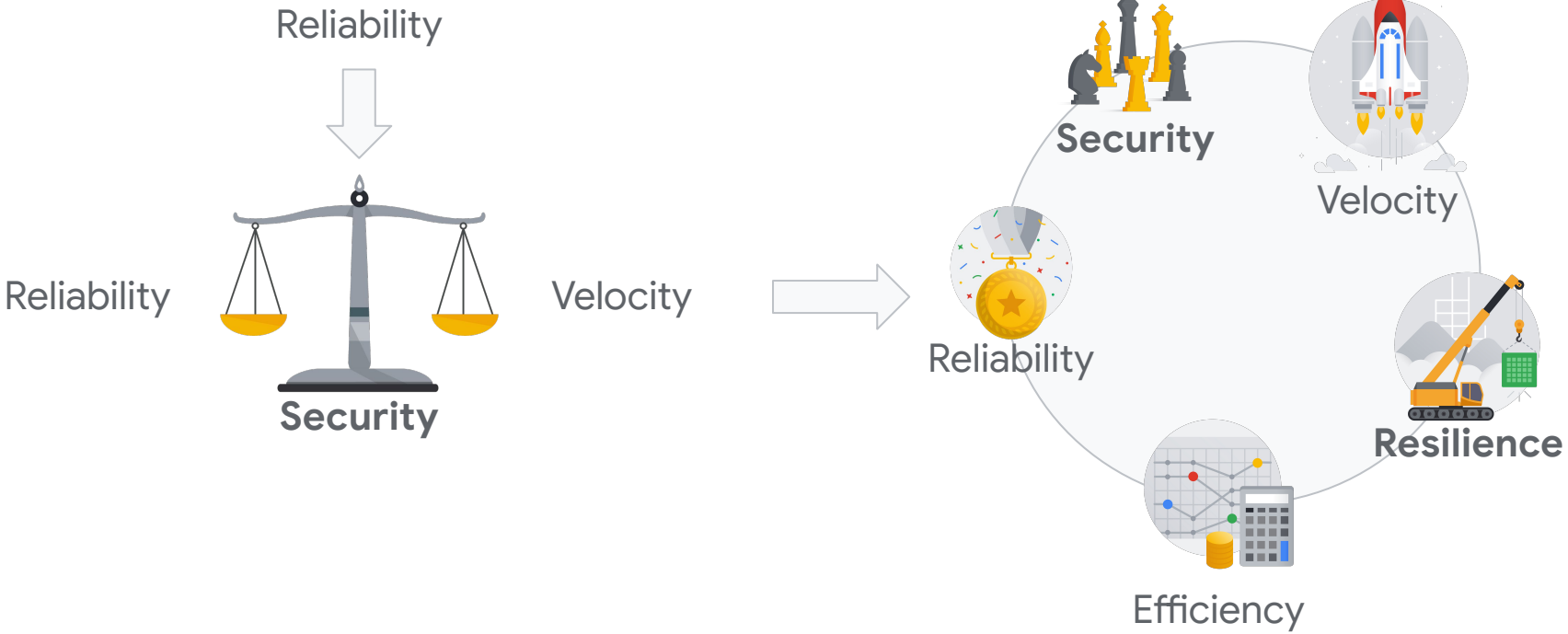
SLOs & Postmortems - Reliability + Security

Is system performance and security posture measured, aligned with the users' needs, and actively followed up on?

- SLOs defined and signed off
- SLO measurement and compliance
- Monitoring for error rates & security events
- Understanding end-to-end performance (impact & dependencies) and threat posture

- Useful postmortems for outages get written and action items get resolved
- Blameless culture
- Connecting SRE with customers

How the approach evolved over time...



... and is codified into $production_principles

How to foster adoption, and measure implementation?

SRE CON EUROPE MIDDLE EAST AFRICA

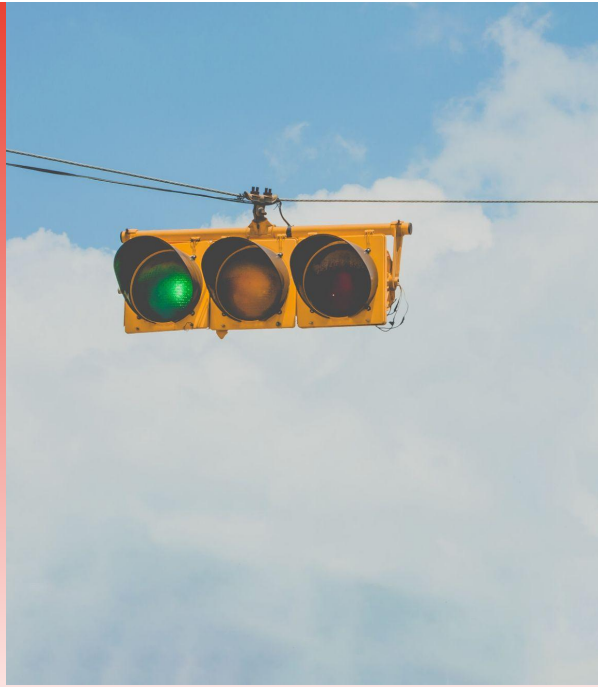
- At large scale the question of “cost-to-implement” is important
- Influenced by Regulatory & Compliance demands
- In various large organizations (e.g. “independent” BUs rolling up to a Global CISO) what’s the best approach to get 1) buy-in, 2) achieve company goals?
- Evolve your “ProdEx” (Production/Operational Excellence) KPIs to include $security_production_principles

Making and Keeping “Prod” Secure & LPHC: Low Probability High Consequence

- Partnering with the business and injecting SRE experience / domain & system resilience knowledge
- Macro risks (e.g. climate change, geopolitical tension, war, energy supply, etc), security events, etc.
- Partnering with Red & Orange Teams
- “Think global, act local”
- *Schrödinger’s kat* (k as in key)

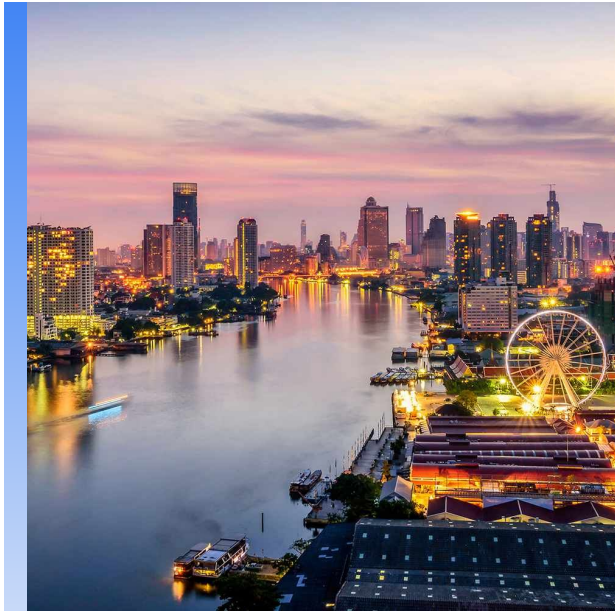
Disaster Resilience

- A natural evolution of Reliability + Security
- **Normal** (Incident) | **Disaster** | **Emergency** Mode
- Tabletop / Wheel of (mis)fortune exercises, at scale
- Preparedness is and remains key

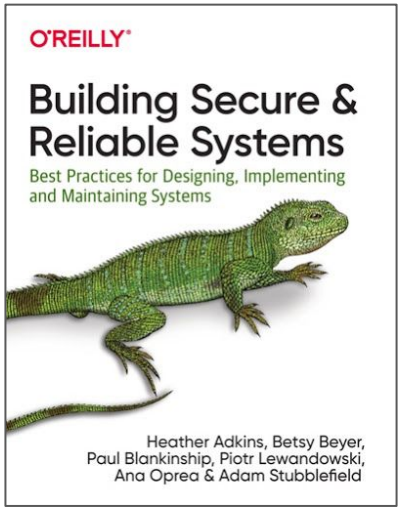


How to make this work for you?

- Don’t try to mirror / be like Google (and a little story)
- Tech-island vs mainland | Enterprise point-solutions | Platforms
  - How to rethink build-vs-buy (COTS)
- DevOps, SRE or DevOps + SRE?
  - System-thinking vs vertical expertise



Thank you



sre.google/resources

Google Cloud CISO Community

SRECON EUROPE MIDDLE EAST AFRICA

Site Reliability Engineering