RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SEM-M04A

Infrastructure in Transition; Securing Your Cloud Environment

Sam Bisbee
CSO
Threat Stack
@sbisbee

Today's discussion

- Applies to all public cloud providers and is industry agnostic
- Why is public cloud unique and what is this intel based on?
- Where public cloud leveraged attacks started -- tired of hearing about leaky AWS S3 buckets?
- Observed bad actors' growing public cloud sophistication in attacks

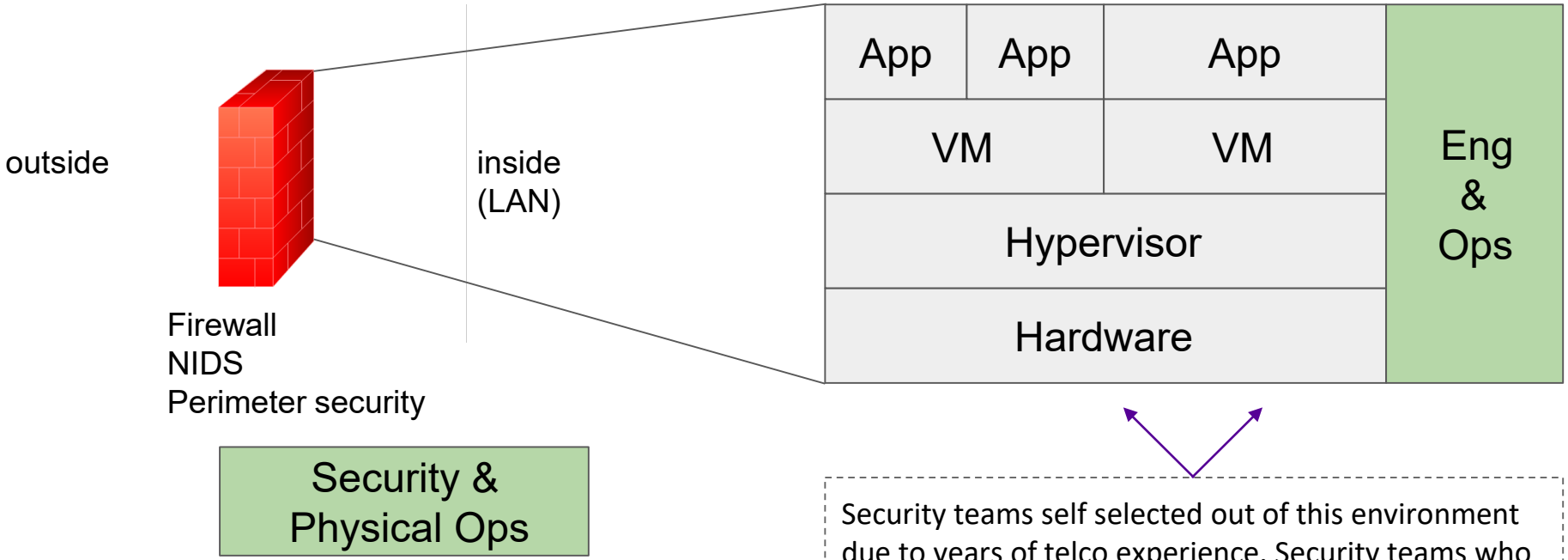
Note on the intelligence & data

- All intelligence and data is from production customer environments and therefore is anonymized
- Certain technical details have been modified that do not change the analysis or intelligence
- Data and technical details from multiple breaches have been combined in this report - we are ***not*** discussing a single observed breach and make no claims about attribution

RSAConference2019

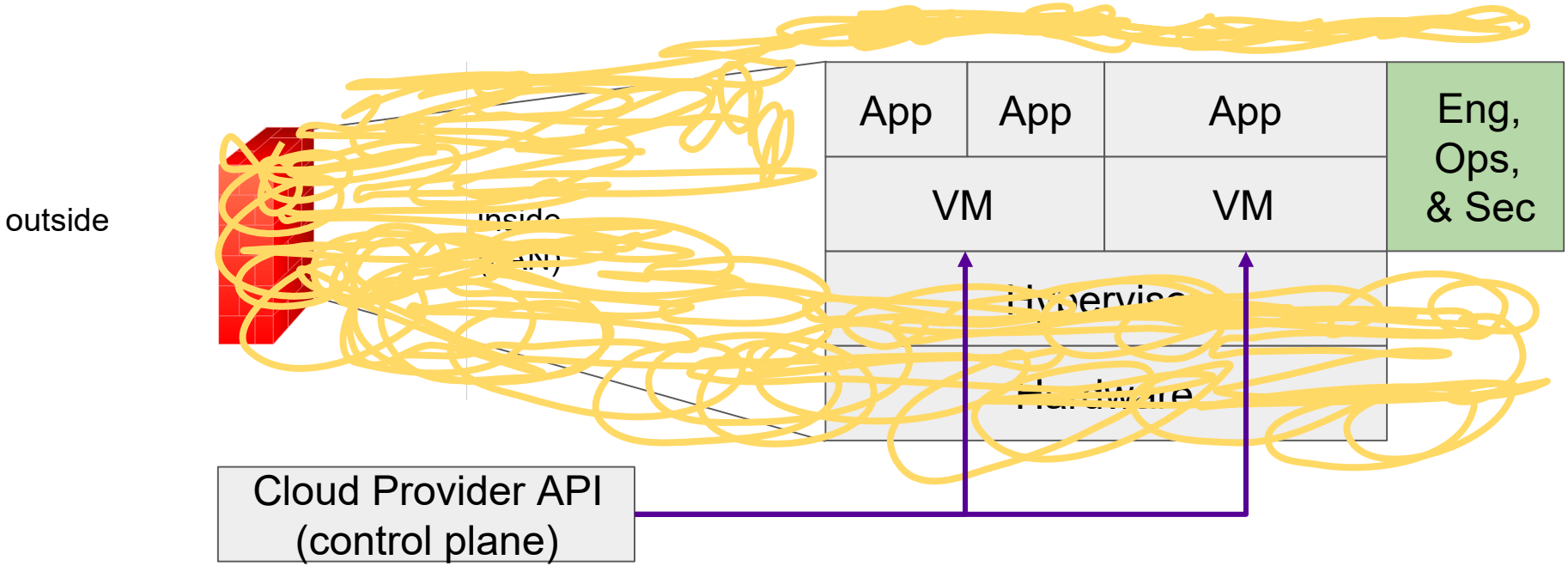
What changed?
How'd we get here?

Traditional security architecture, modern data center



Security teams self selected out of this environment due to years of telco experience. Security teams who wanted in were locked out due to post dot-com “time to market” business edict.

What public cloud did to your architecture



Never forget...

- Public cloud provider APIs are accessible anywhere with a set of credentials -- this is your infrastructure control plane!
- Therefore, public cloud provider API or console access is the equivalent of ***physical data center access***
- Fancy network architectures to combat this create too much cognitive load for relatively minimal security program ROI

How to think about these breaches

1. **Opportunistic** - scanning infrastructure of any organization, generic objectives
   a. Typically botnets scanning public cloud provider IP address ranges
   b. *Base threat for anyone running anything on the Internet and most common source of remote attack*

2. **Persistent** - attempting to gain specific objectives in specific organizations
   a. Higher value objectives
   b. Likely recon their target heavily, including corporate environment

Where the attacks started (AWS as example provider)

- **Credential theft** - admin user/pass or AWS Access Key, used to spin up EC2 instances or gain direct data access to S3 and RDS
- **Persistence** - create new credentials and Access Keys, leverage AssumeRole and IAM misconfiguration complexity
  - Ex., Code Spaces shutdown after AWS console was ransomed (2014)
- **AWS Service Use** - mostly traditional AWS services like IAM, EC2, and S3

Rising sophistication

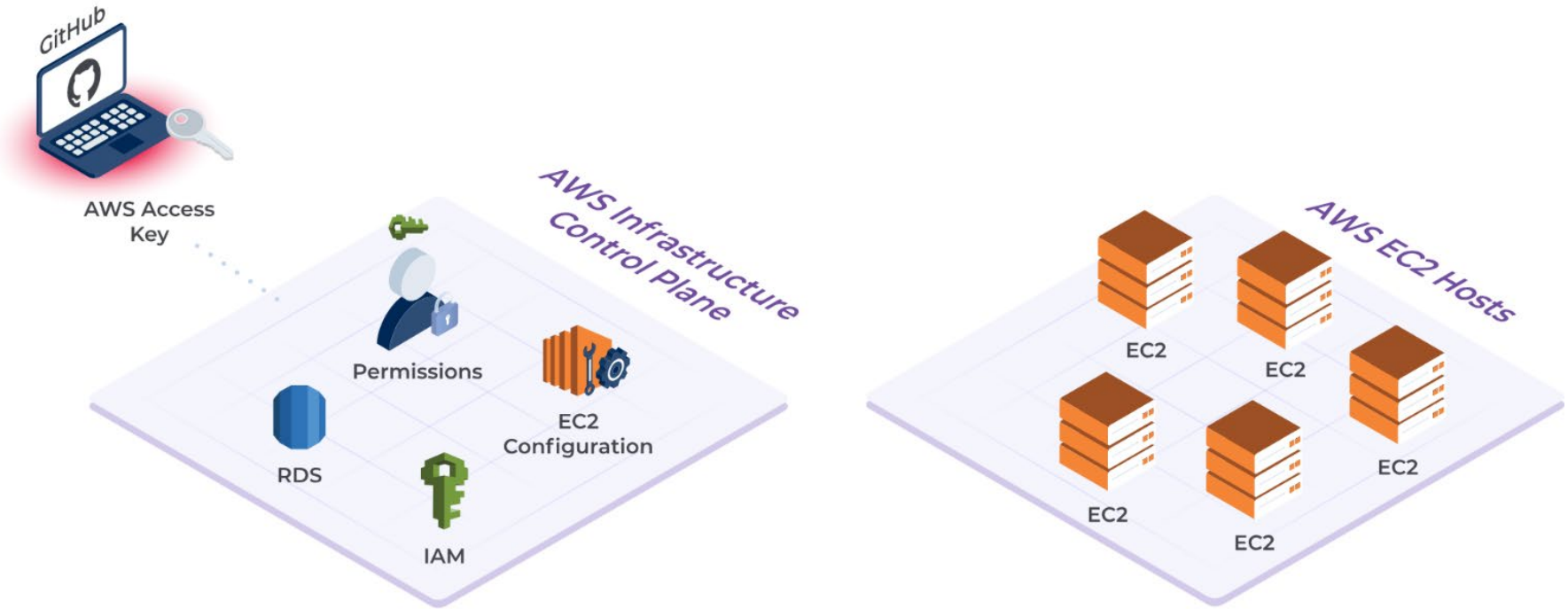
- Began observing mid-to-late 2016, gained momentum in 2017
- Attacks crossing the membrane between AWS APIs and hosts multiple times
- Leveraging lesser known or often forgotten EC2/IAM attributes
  - EC2 instances have IAM roles (effectively users)
  - EC2 instance metadata service: *curl http://169.254.169.254/*
- Chaining multiple AWS APIs with traditional network attacks

RSAConference2019

Example Kill Chain

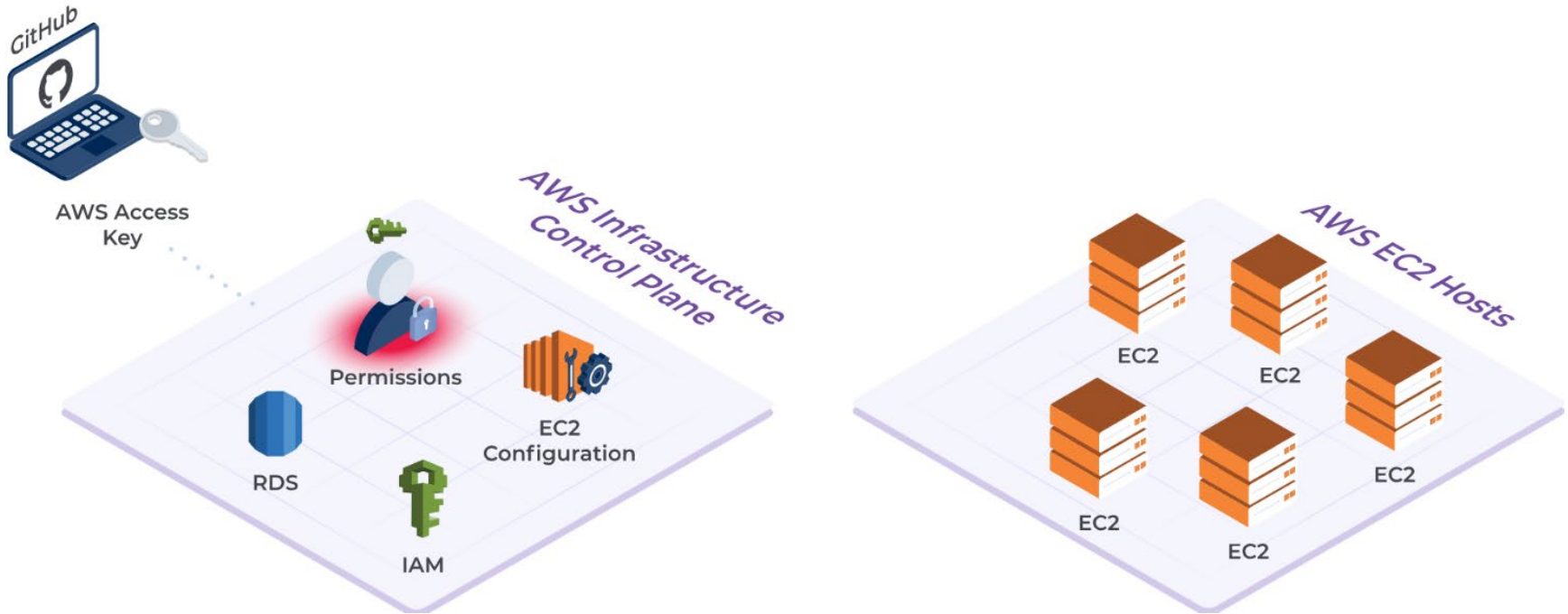
Assembled from multiple breaches of production environments, leveraging an example AWS architecture

Credential theft from laptop, build systems, etc.



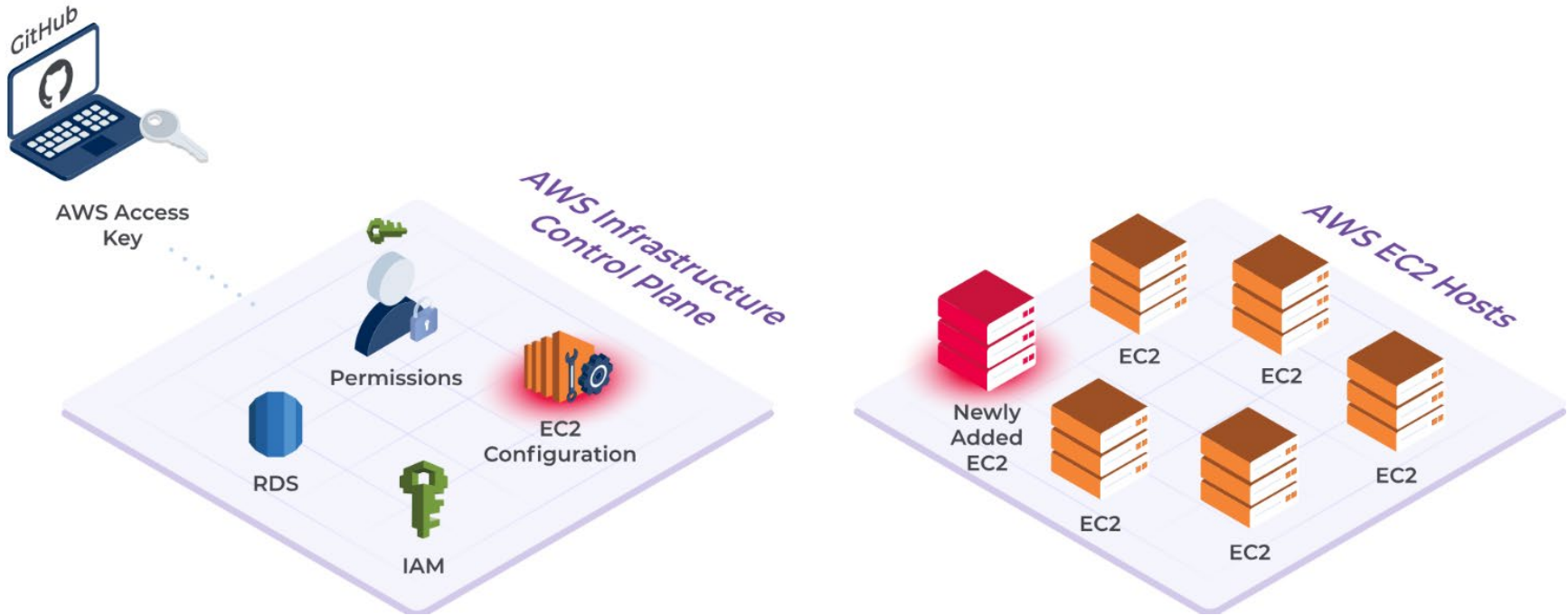
Illustrative example using AWS as cloud provider.

Persistence into cloud's infrastructure control plane



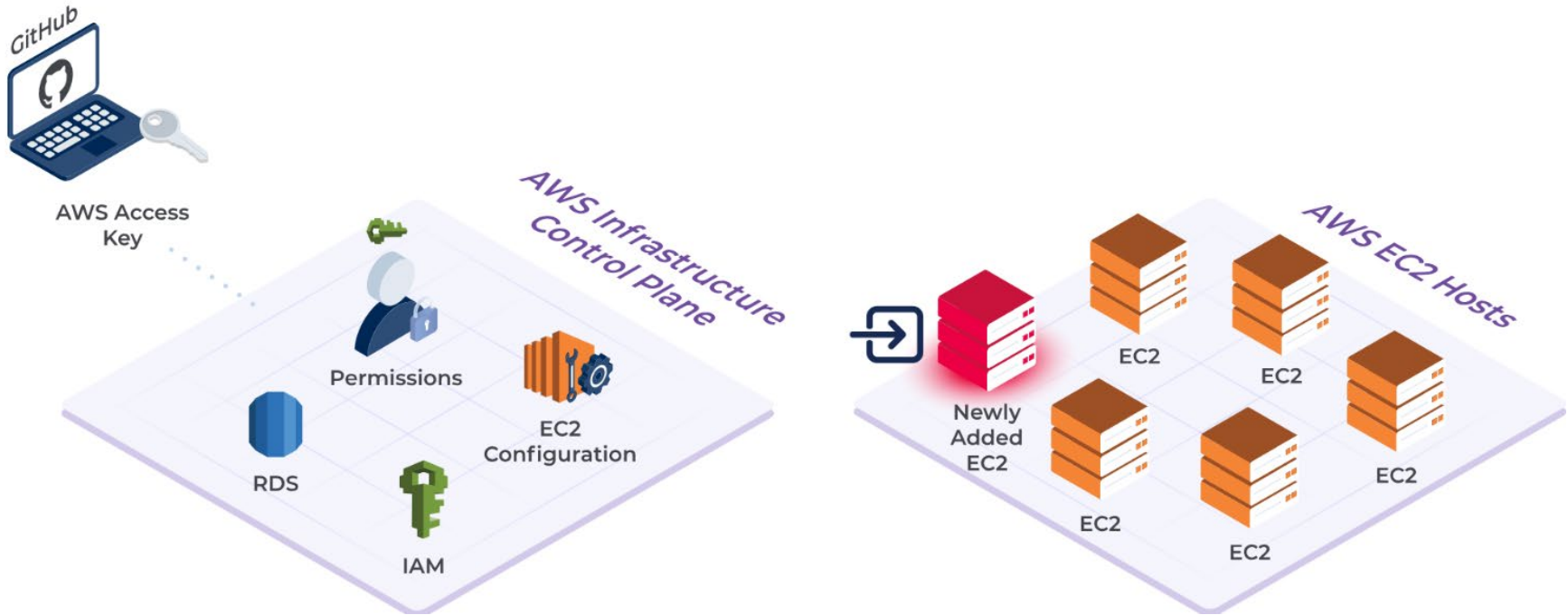
Illustrative example using AWS as cloud provider.

Launch malicious host



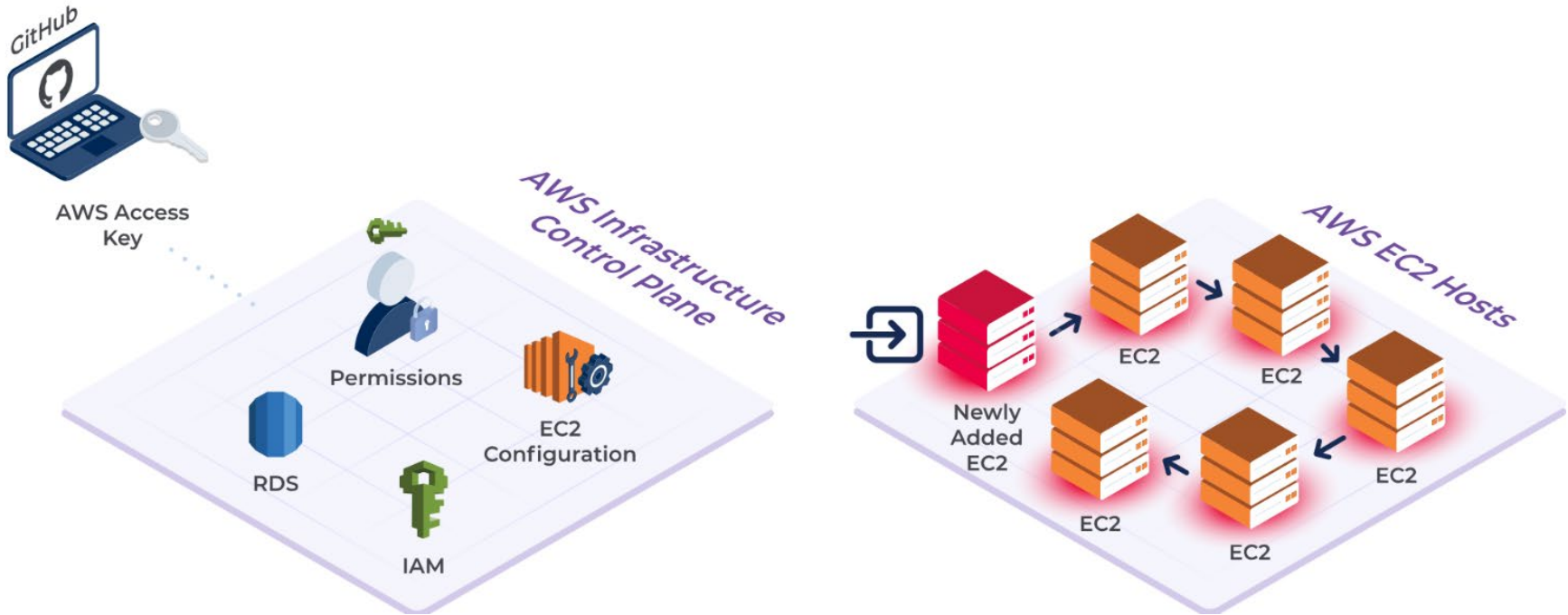
Illustrative example using AWS as cloud provider.

Achieve network beachhead



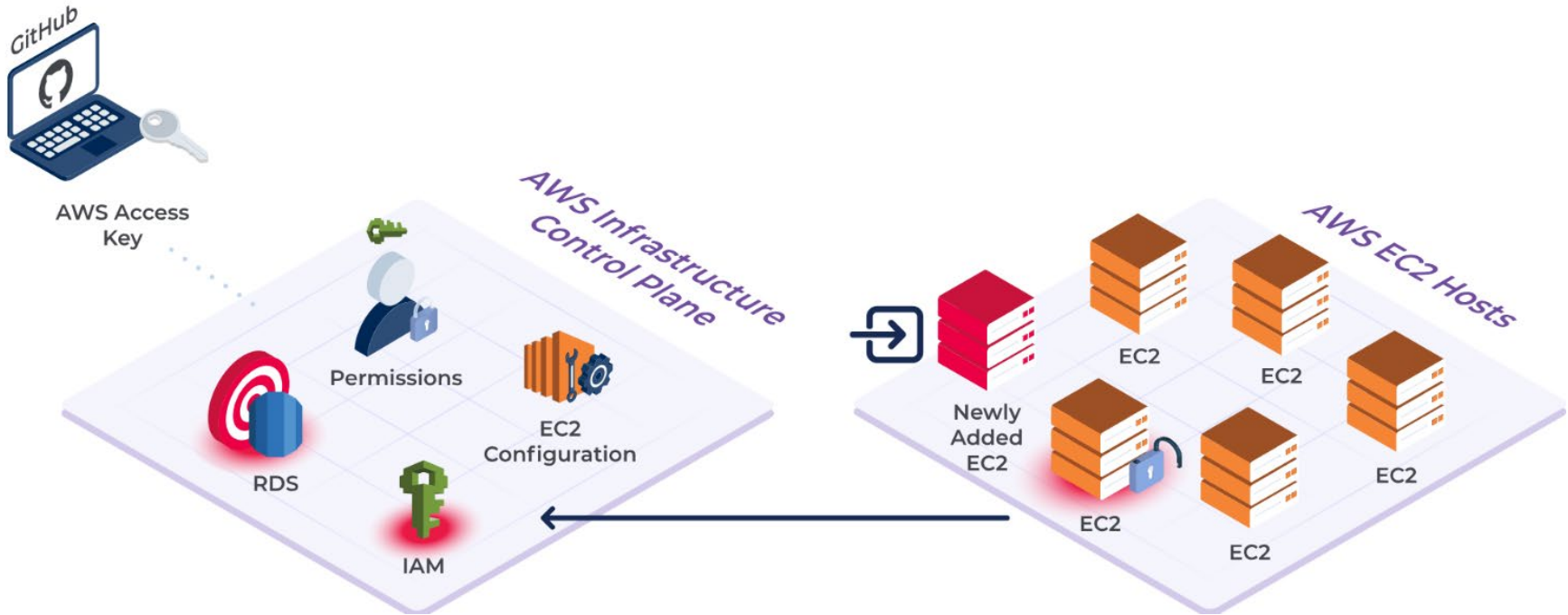
Illustrative example using AWS as cloud provider.

Traditional network lateral moves with new objective



Illustrative example using AWS as cloud provider.

Objective achieved: RDS access



Illustrative example using AWS as cloud provider.

Key takeaways // Reach out to chat! @sbisbee

- Your control plane is on the Internet now
  - Action: tight account monitoring, MFA, and break glass access
  - Action: treat cloud console/API access as physical access
- Employees and servers are increasingly indistinguishable, using the same APIs and public cloud services
  - Action: monitor whole control plane and all assets in single place
- Attacker objectives have moved off the host to black boxes
  - Action: evolve your threat models, architecture, and detection