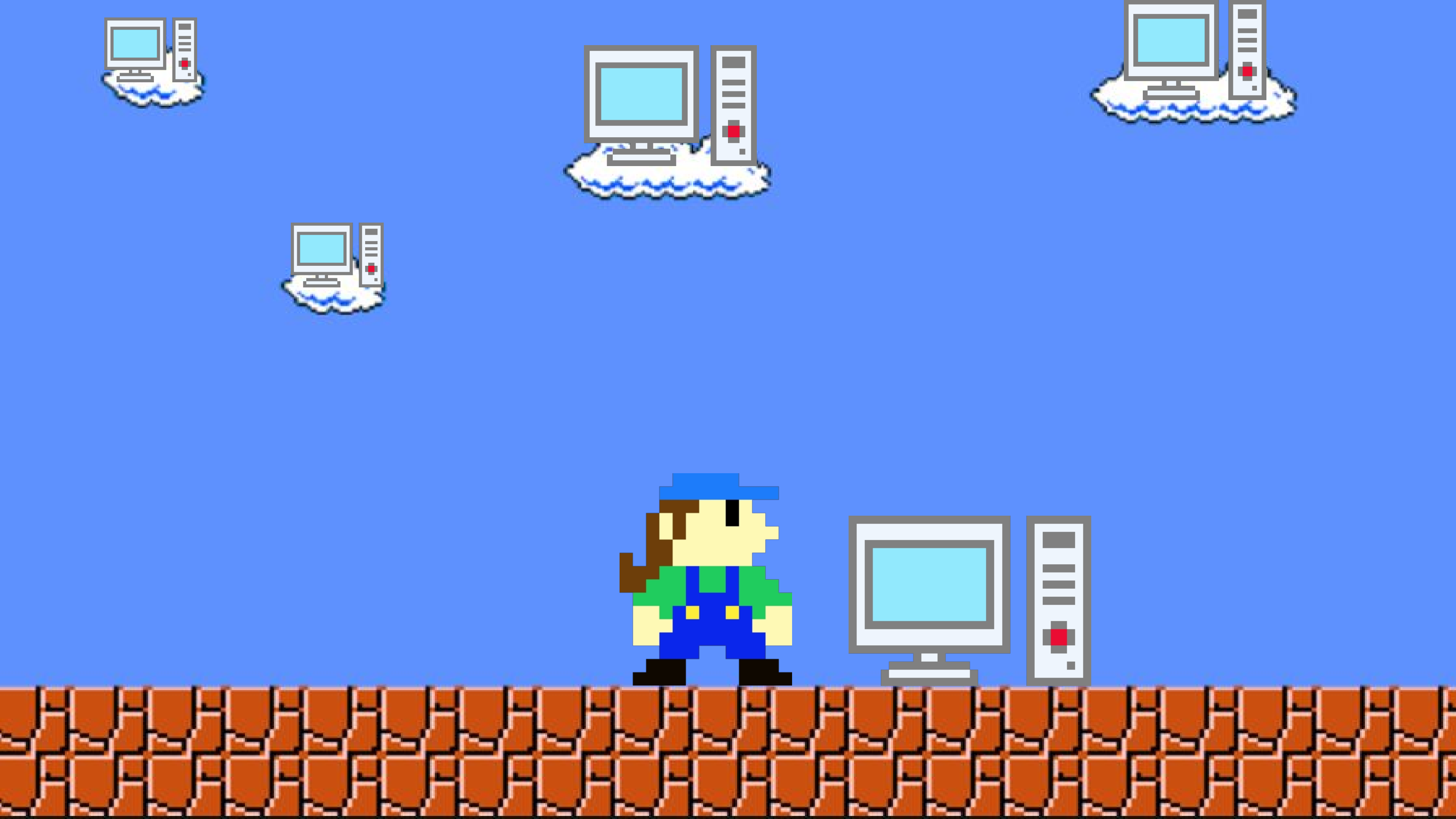
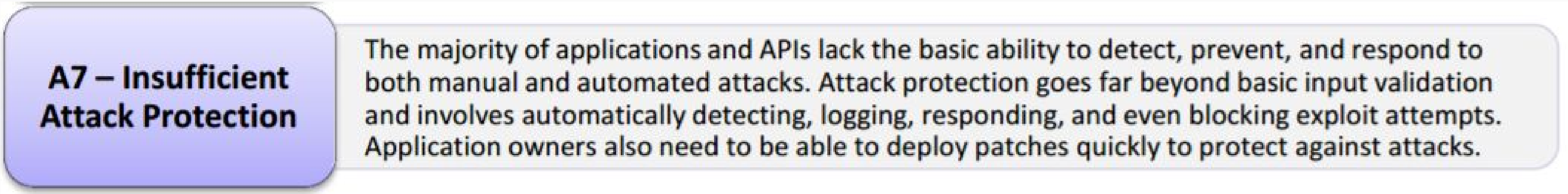
The Magical World of
Cloud Security

1 PLAYER GAME – @sputina



2017 Updates

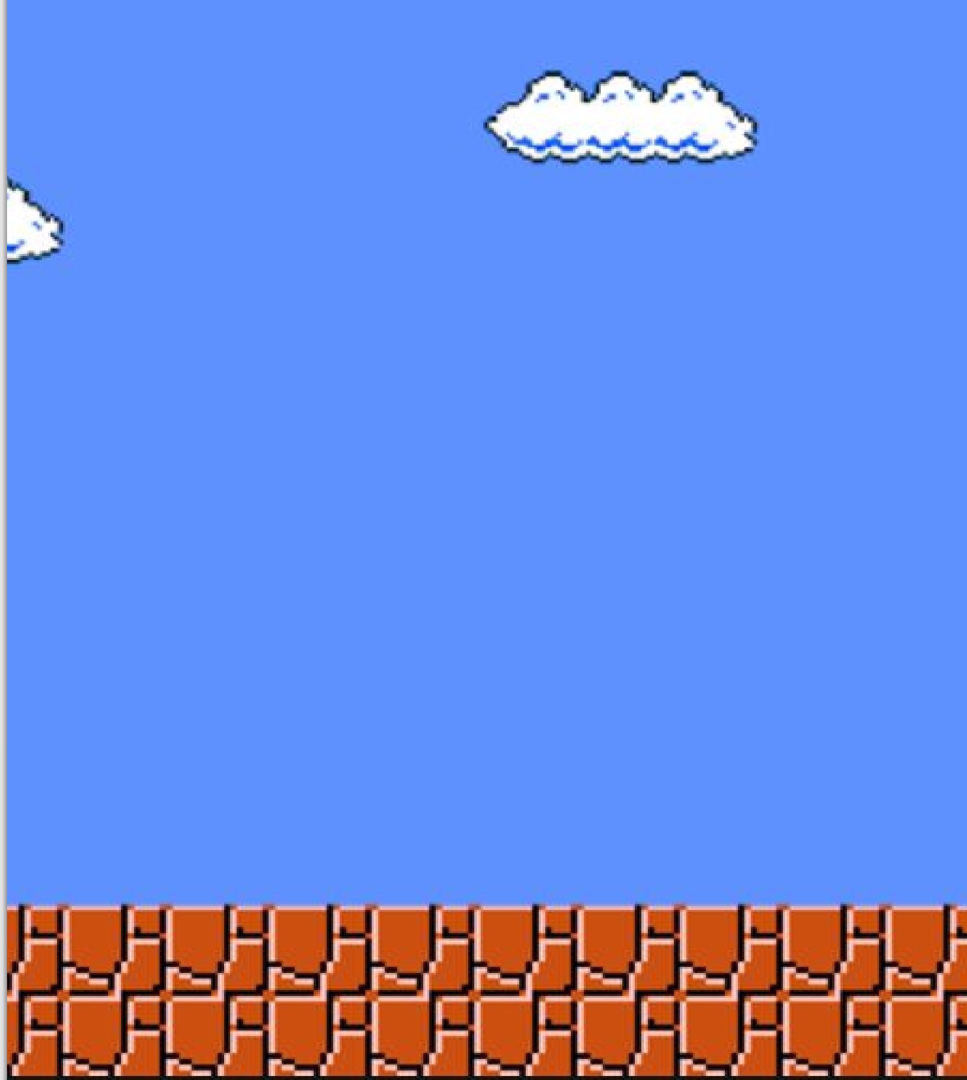


A7 – Insufficient Attack Protection

The majority of applications and APIs lack the basic ability to detect, prevent, and respond to both manual and automated attacks. Attack protection goes far beyond basic input validation and involves automatically detecting, logging, responding, and even blocking exploit attempts. Application owners also need to be able to deploy patches quickly to protect against attacks.

World 1-1

Host-level Security

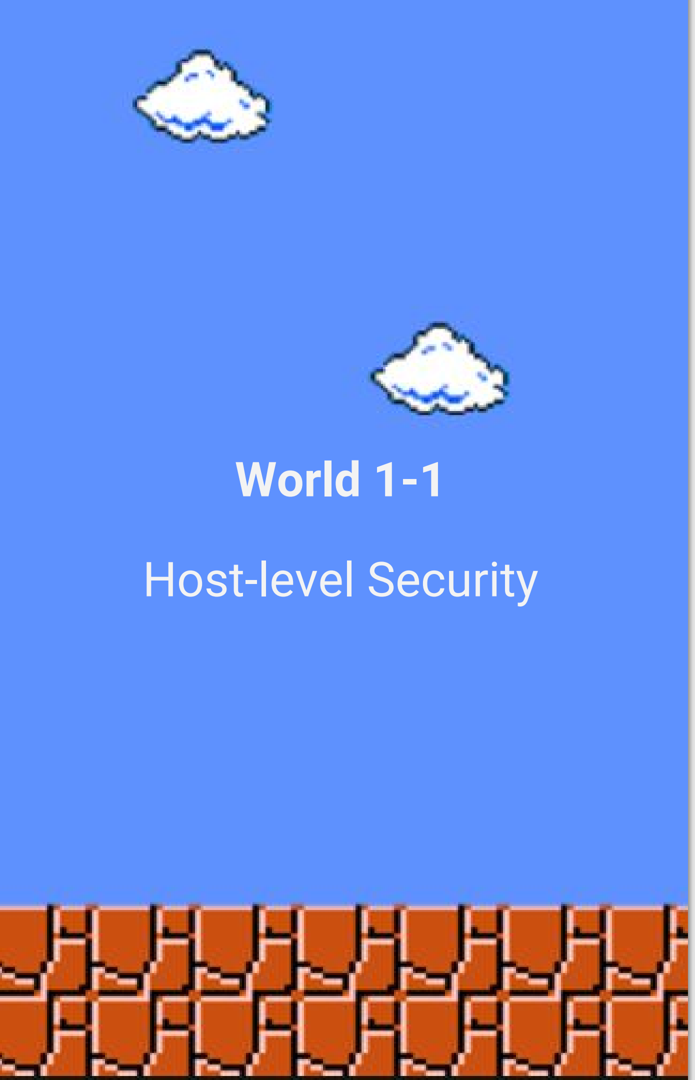


World 1-1

Host-level Security

Storing & using secrets - Access controls to access storage & encrypting the objects

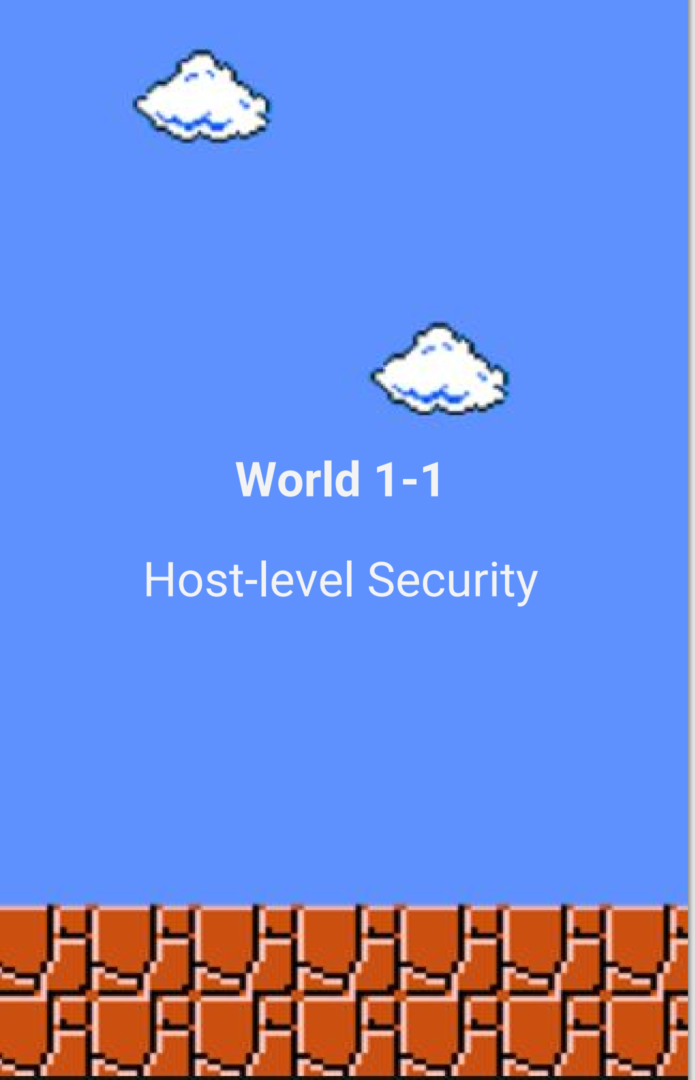
- Don’t commit these
- AWS Parameter Store
- Azure Key Vault
- Cloud Storage + Access Controls + Encryption Key



World 1-1

Host-level Security

- **Multi-factor authentication** - for sensitive services & accessing your instance
  - privacyIDEA
  - Google Authenticator

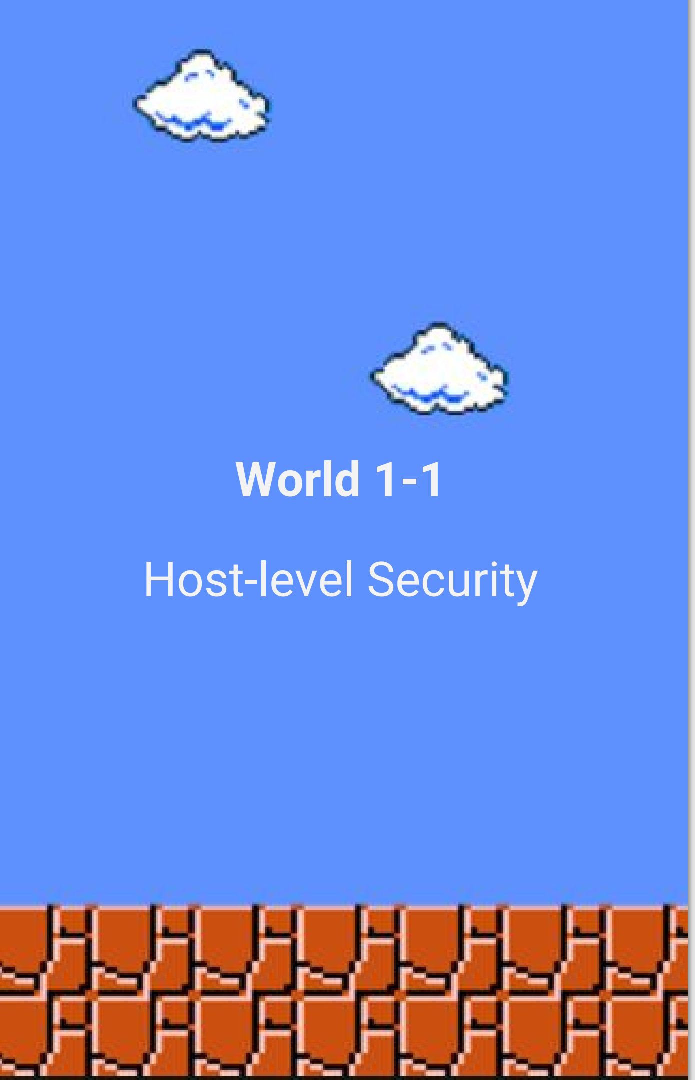


World 1-1

Host-level Security

TLS certificates & decrypting traffic - for every service; everywhere

- Free TLS certificate service - Let’s Encrypt
- Recommended private key size, strong protocols, strong ciphers - OWASP TLS Cheat Sheet



World 1-1

Host-level Security

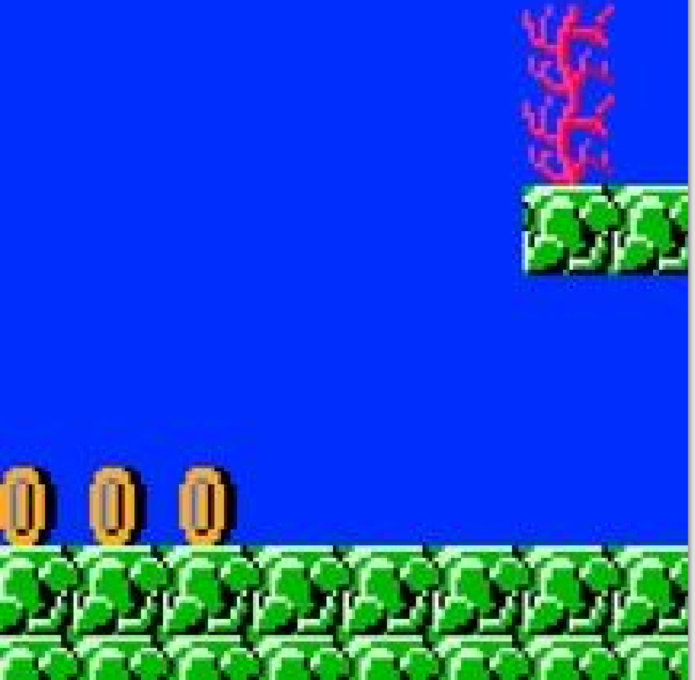
- **Host-based monitoring -** Gateway inspection - or - Manager + Agent on each host
  - OSSEC Open Source Host-based Intrusion Detection System

World 1-2

Platform-level Security

World 1-2

Platform-level Security



- **Access, user, and role management -** Rule of least privilege
  - Most attacks rely on bad access controls - Rich Jones @ CCC & Daniel Grzelak
  - Cloudsploit - Analysis of security API activity
  - Newer, trust-less architecture models are going to rely on his even more

World 1-2

Platform-level Security

- **System log monitoring** - Aggregating and analysing
  - Be able to correlate from multiple sources and understand when things are going wrong
  - Open source models include Elasticsearch for search, Logstash for data collection, and Kibana for data visualisation - Like Graylog

World 1-2

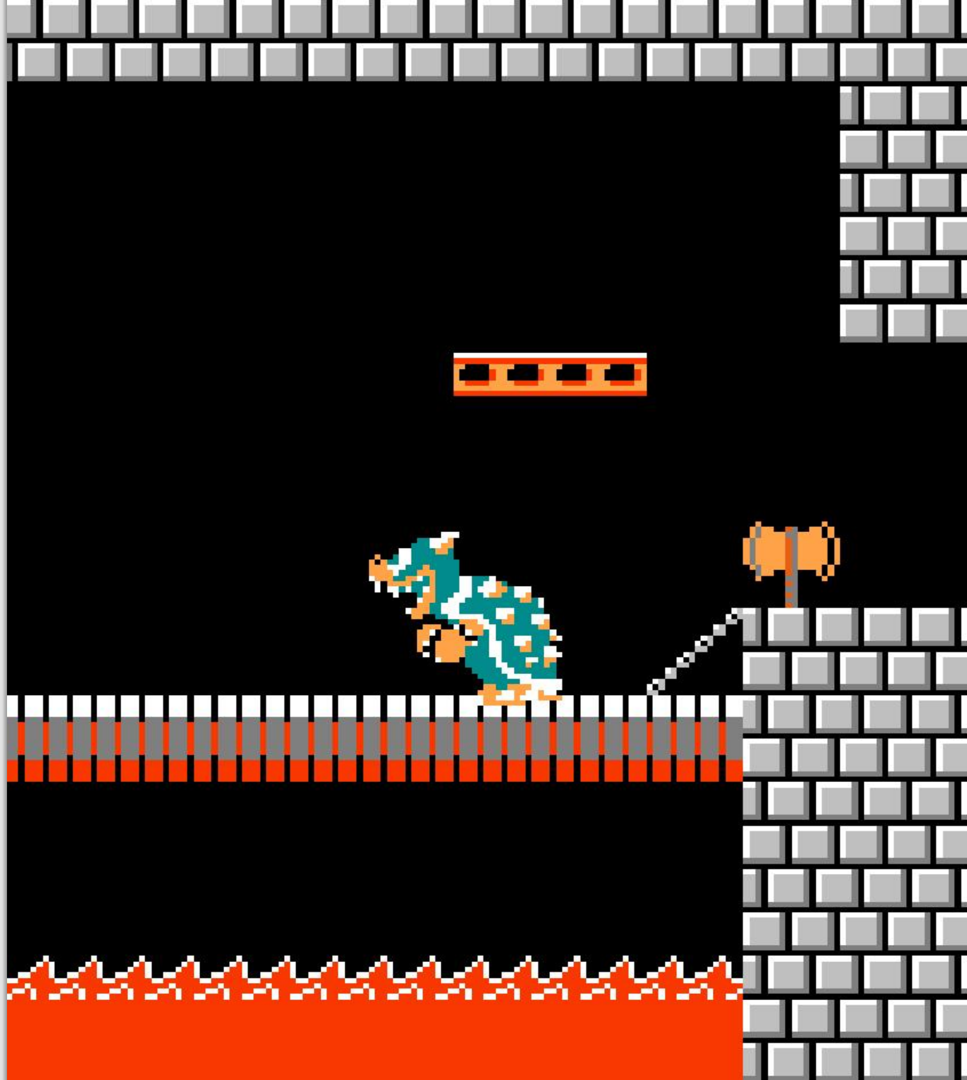
Platform-level Security

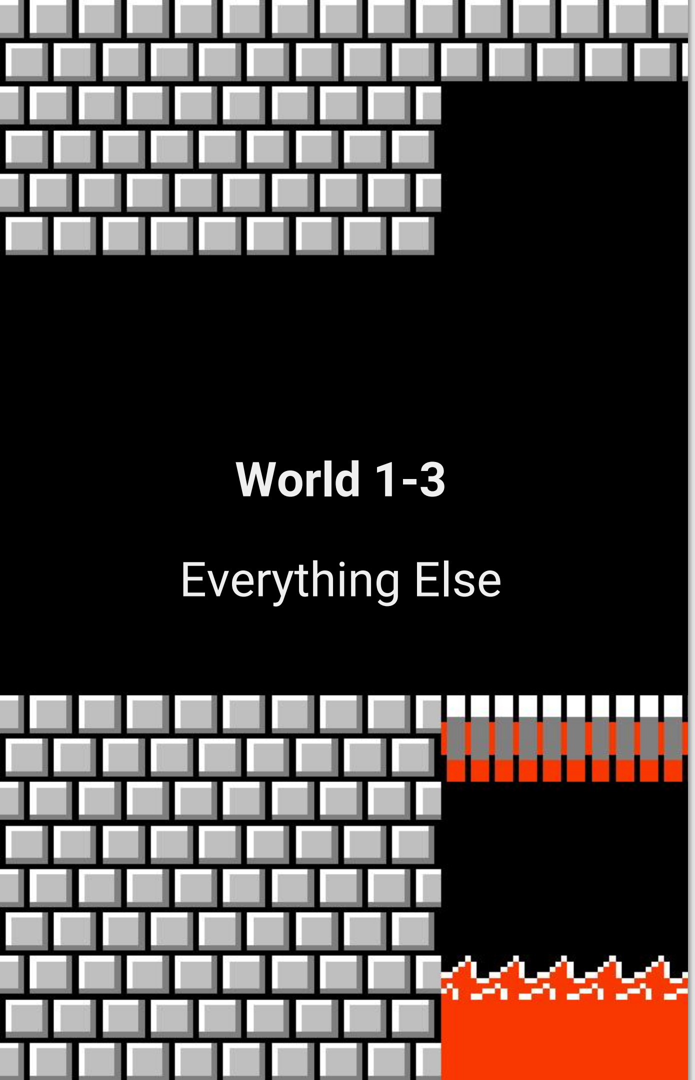
Ingress & Egress - Security monitoring & alerting

- Tools that scan traffic as it comes in / leaves your application server - intrusion detection, network & application filtering, rate limiting
- Requires the traffic be decrypted (& perhaps re-encrypted after)
- Start from the bottom with security rules and policies

World 1-3

Everything Else
(i.e. someone else’s network)





World 1-3

Everything Else

- **Content Distribution Networks** - Other networks that can help with performance & security
  - Step up from the library/framework CDN like javascript libraries
  - Limited control, and places trust in the product as it requires traffic to be decrypted (& hopefully re-encrypted to your cloud infrastructure)
  - Shared responsibility model - similar to the trust with cloud providers to **secure the cloud**, and your responsibility for **security in the cloud**

Final Flagpole

- Take these back to your teams and understand what your environment looks like, understand the architecture, **provide input**!
- **Play** and **contribute** with the open source tools you enjoy.
- No tools or technologies fix **orphaned/outdated code** or **technical debt**
- Refactoring code can be **just as good** as a new feature

Thank you!