Abstract

Talk Abstract

We turn to DevOps for speed. We turn to Cloud for flexibility. We adopt faster, leaner, more collaborative processes to drive change. And then? We turn to information security for protection. But can we secure the technology without slowing the pace? This session will share stories of how teams can.

Talk Description

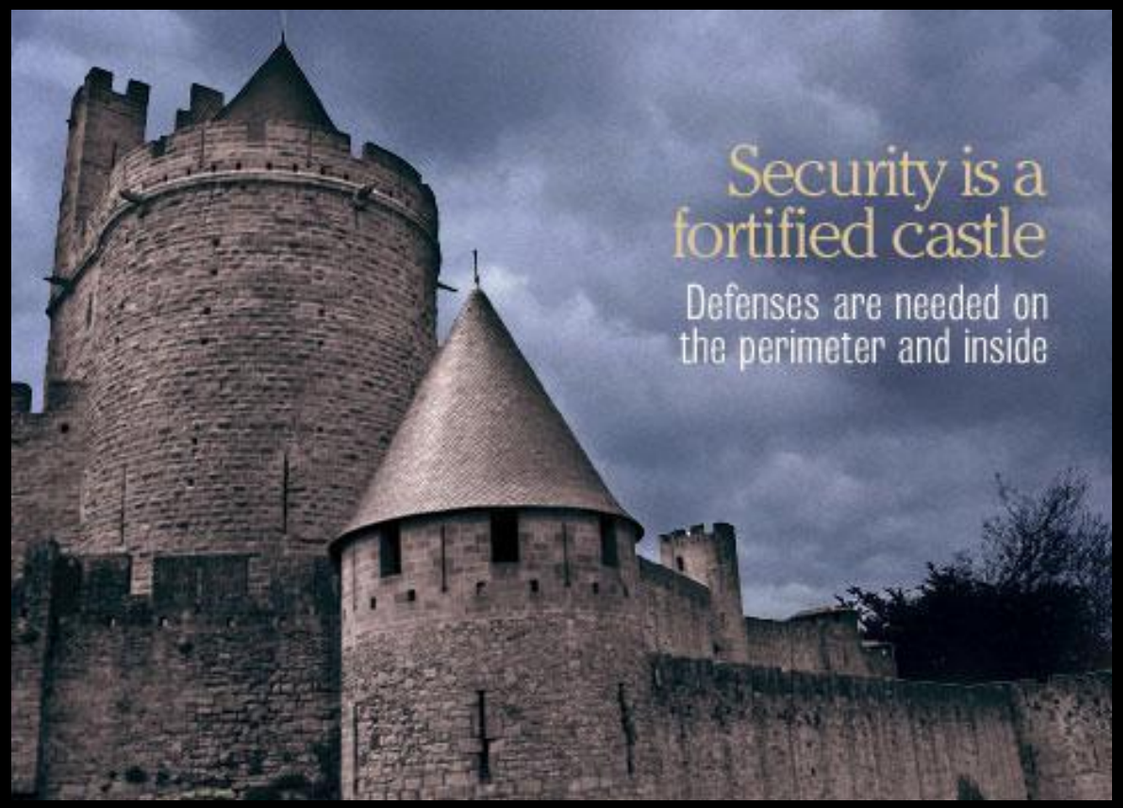
We turn to DevOps for speed. For the beginners in the room, the presentation introduces DevOps. We'll then cover some of the latest developments in the field for those with intermediate skills. Security concerns and case studies will be shared, illustrating some of the concerns and potential solutions.

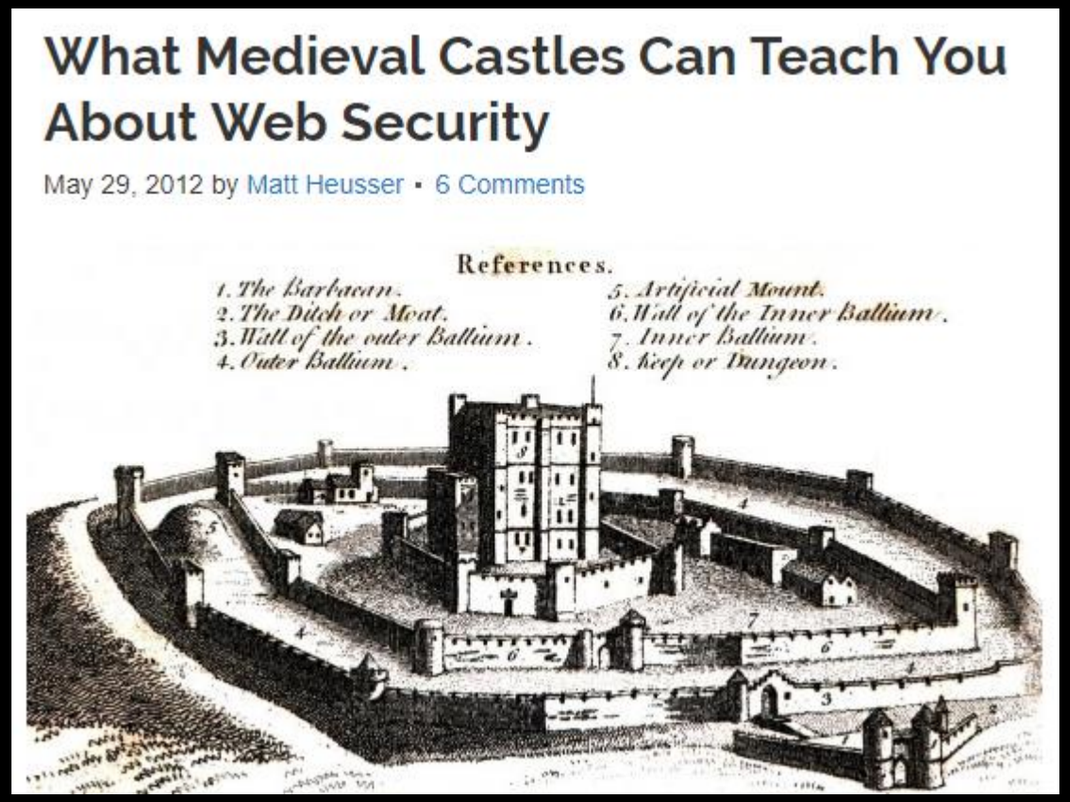
We turn to Cloud for flexibility. For the beginners in the room, the presentation introduces software, platform, and infrastructure as a service. We'll then cover some of the latest developments in the Cloud services for those with intermediate skills. Security concerns and case studies will be shared, illustrating some of the concerns and potential solutions.

We adopt faster, leaner, more collaborative processes to drive change. And then? We turn to information security for protection. Case studies of successful DevOps and Cloud security, leaning on Rugged and security culture, will be shared. The emphasis is on teams that secure the process and technology without sacrificing time.

But can we secure the technology without slowing the pace? Absolutely. The session concludes with lessons on how to do just that.

Securing without Slowing



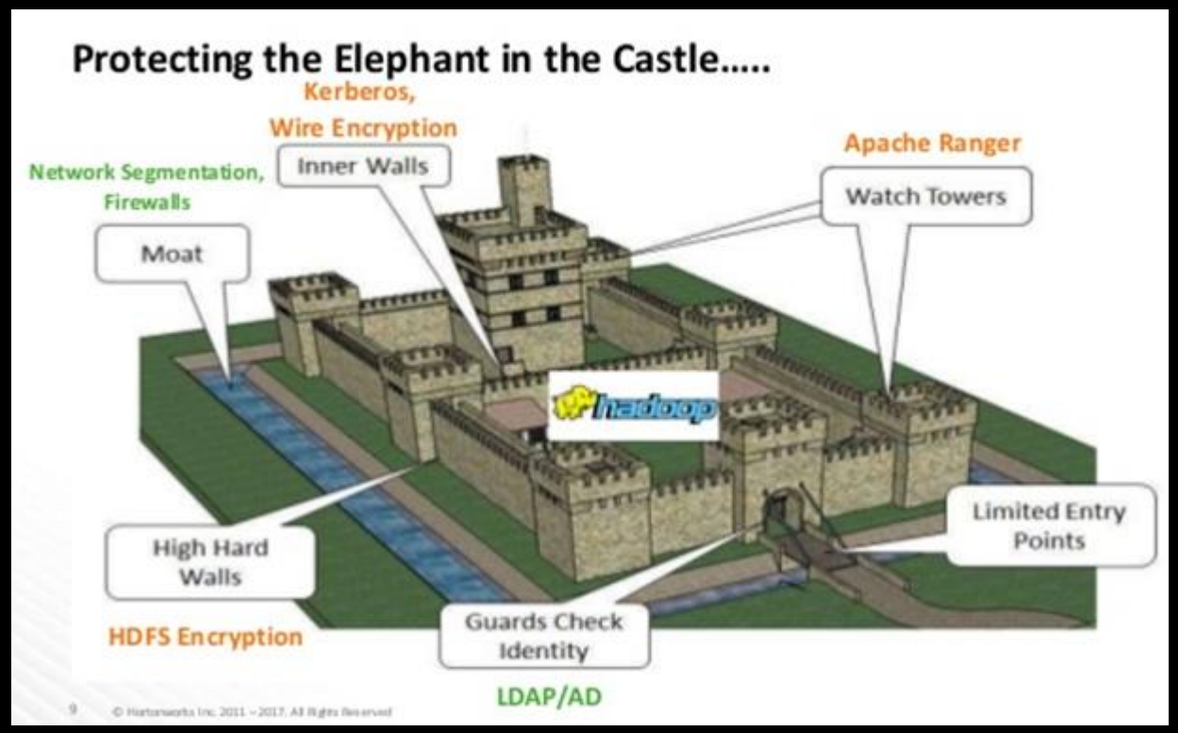


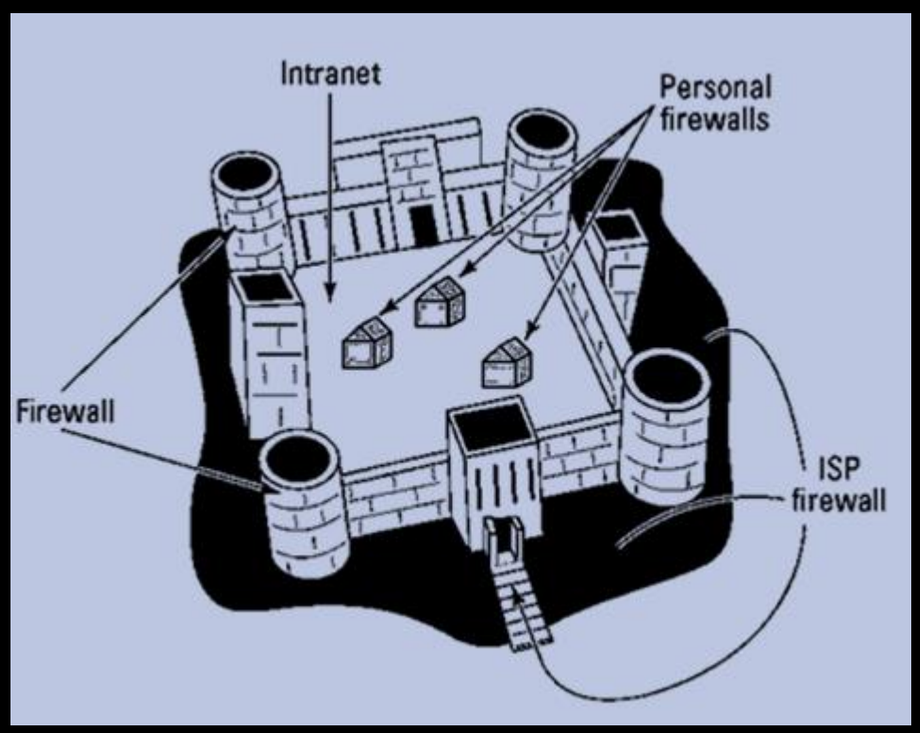
What Medieval Castles Can Teach You About Web Security

May 29, 2012 by Matt Heusser • 6 Comments

References.

1. The Barbacan.
2. The Ditch or Moat.
3. Wall of the outer Ballium.
4. Outer Ballium.
5. Artificial Mount.
6. Wall of the Inner Ballium.
7. Inner Ballium.
8. Keep or Dungeon.





@jwgoerlich

11th -15th Century

Kingdom's wealth

Decades to build

No one uses castles any more.

@jwgoerlich

Guédelon

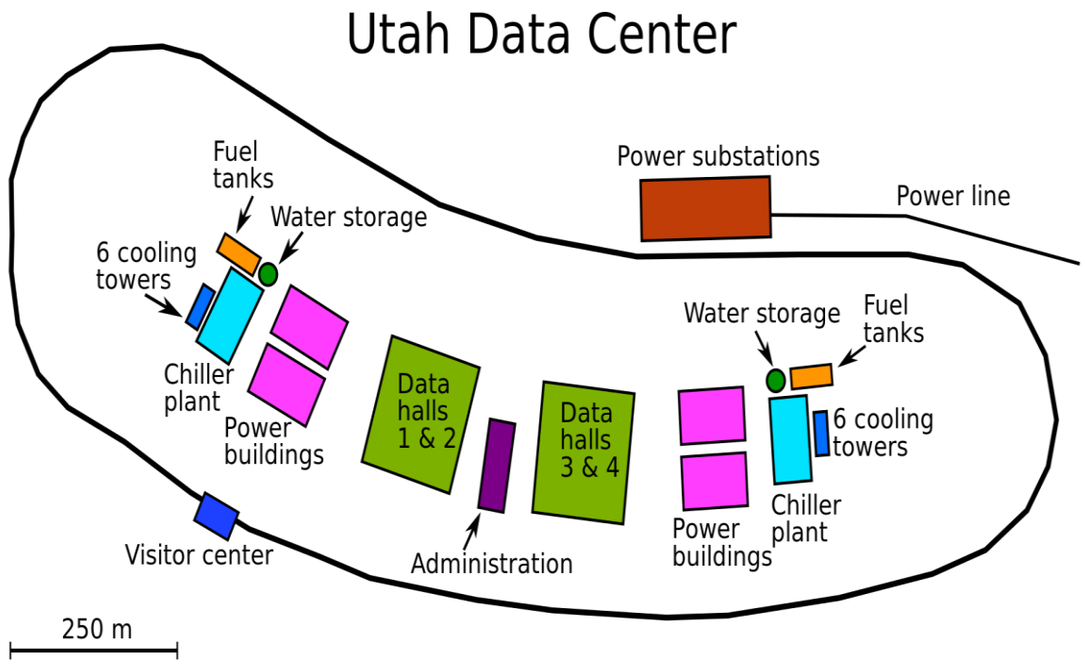
(Almost no one)

Started in 1997

50 expert craftsmen

25 year build time

$10 million cost


Utah Data Center
Fuel tanks
Water storage
6 cooling towers
Chiller plant
Power buildings
Power substations
Power line
Data halls 1 & 2
Data halls 3 & 4
Water storage
Fuel tanks
6 cooling towers
Chiller plant
Power buildings
Visitor center
Administration
250 m

@jwgoerlich

Securing without Slowing

Principles

Stop building castles
Survey the land first and often
Leverage standards and practices
Defend from a position of strength
Create cyber security street smarts

We turn to DevOps for speed.

We turn to Cloud for flexibility.


DEVOPS
+
CLOUD
4EVER

I am rugged and, more importantly, my code is rugged.

I recognize that software has become a foundation of our modern world.

I recognize the awesome responsibility that comes with this foundational role.

I recognize that my code will be used in ways I cannot anticipate, in ways it was not designed, and for longer than it was ever intended.

@jwgoerlich

I am rugged because I refuse to be a source of vulnerability or weakness.

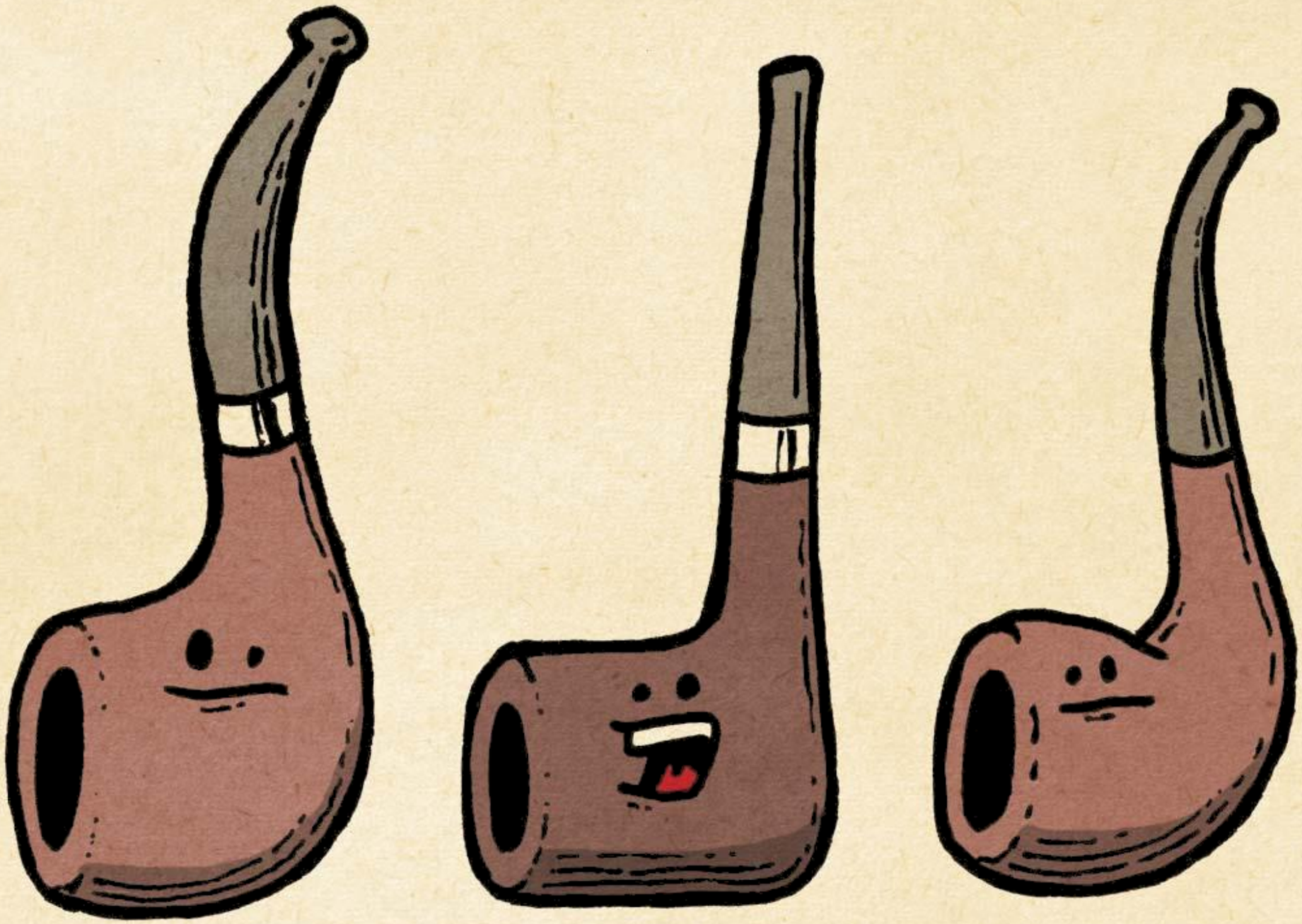
I am rugged because I assure my code will support its mission.

I am rugged because my code can face these challenges and persist in spite of them.

I am rugged, not because it is easy, but because it is necessary and I am up for the challenge.

@jwgoerlich

We're in the pipeline.



DevOps Pipeline

Code: code development and review
Build: continuous integration tools
Test: continuous testing tools
Package: deployment staging
Release: change management
Configure: Infrastructure as Code tools
Monitor: performance monitoring

DevOps Tooling

Developer / Operations Toolset
Continuous Integration / Continuous Deployment (CI-CD)


@jwgoerlich

DevOps Development Lifecycle

Security Review: Design Review
Security Review: Code Review
Static Application Security Testing (SAST)
Dynamic Application Security Testing (DAST)
Interactive Application Security Testing (IAST)
Software Composition Analysis (SCA)
Change Monitoring
File Integrity Monitoring (FIM)
Infrastructure Vulnerability Management
Runtime Application Self-Protection (RASP)
Web Application Firewall (WAF)

Penetration Testing

@jwgoerlich

Write a single line of code.

Increase the attack surface.

Defect Density

Coverity report analyzes more than 450 million lines of software in the largest public-private sector research project focused on software integrity.

0.69 defects
per 1,000 lines

Real World Example

Exploitable defect in:
  Jakarta Multipart Parser
Distributed as part of:
  Apache Struts
Running software for:
  Equifax
Enables a breach

Defect Density

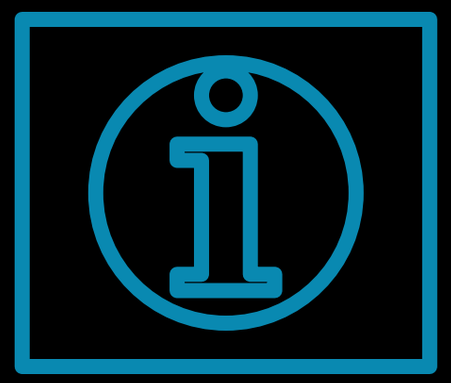
Security Review: Code Review

Static Application Security Testing (SAST)

@jwgoerlich

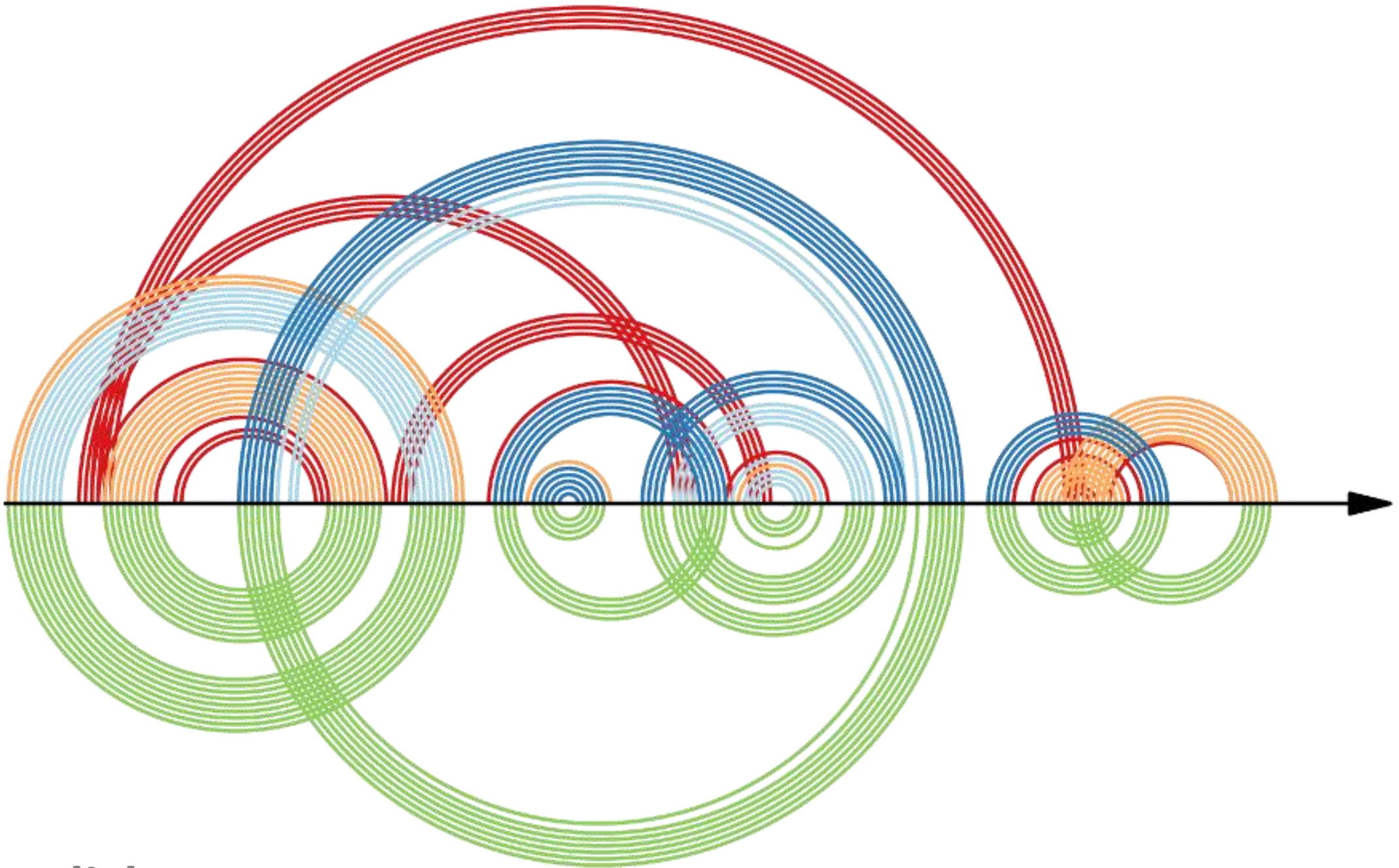
The time to check security must fit within the time to complete the work.

Stop Building Castles



@jwgoerlich

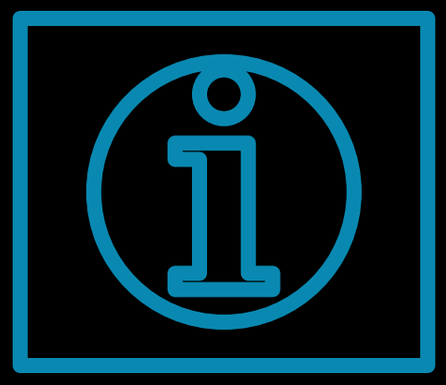
Think Feedback Loops



@jwgoerlich

Create a culture of quality and security one line of code at a time.

Cyber Security Street Smarts



@jwgoerlich

Software Composition Analysis (SCA)

@jwgoerlich

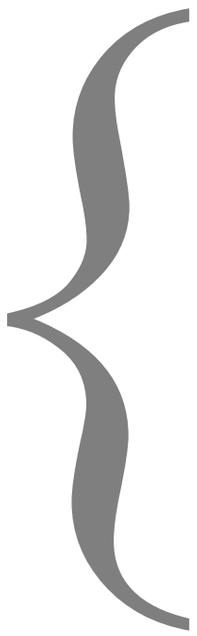
Thousands

Millions

@jwgoerlich

Heartbleed Vulnerability

@jwgoerlich



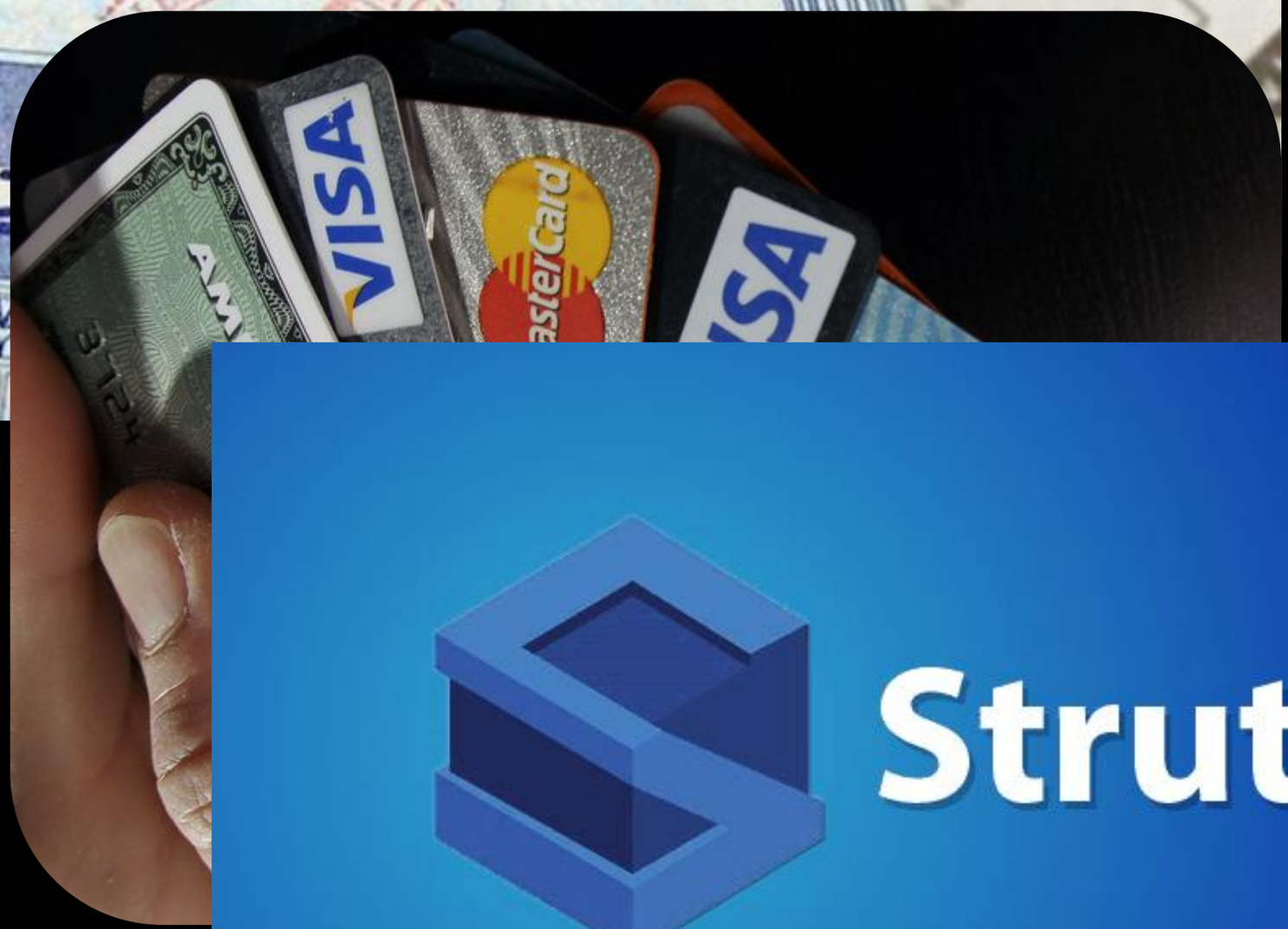
```
if (1 + 2 + payload + 16 > s->s3-
>rrec.length) return 0;

/* silently discard per RFC 6520
sec. 4 */
```

Since Heartbleed, how many vulnerabilities has OpenSSL had?

96


123.1250
-19.60 -13.73%
121.00
OPEN
124.00
HIGH
123.02
1
EFX


SOCIAL SECURITY

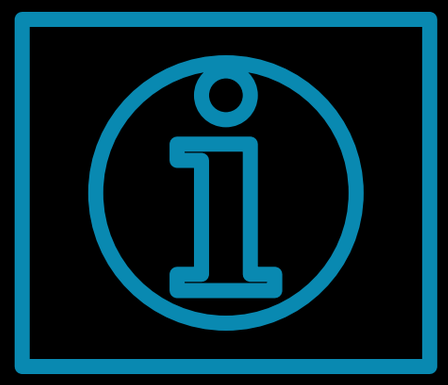

VISA
MasterCard
VISA

Struts 2
APACHE
SOFTWARE FOUNDATION

@jwgoerlich

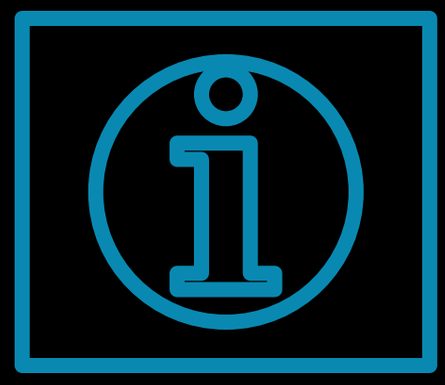
A software composition inventory is essential in defense.

Survey the Land



Track and report on vulnerabilities in third-party libraries and code.

Survey the Land



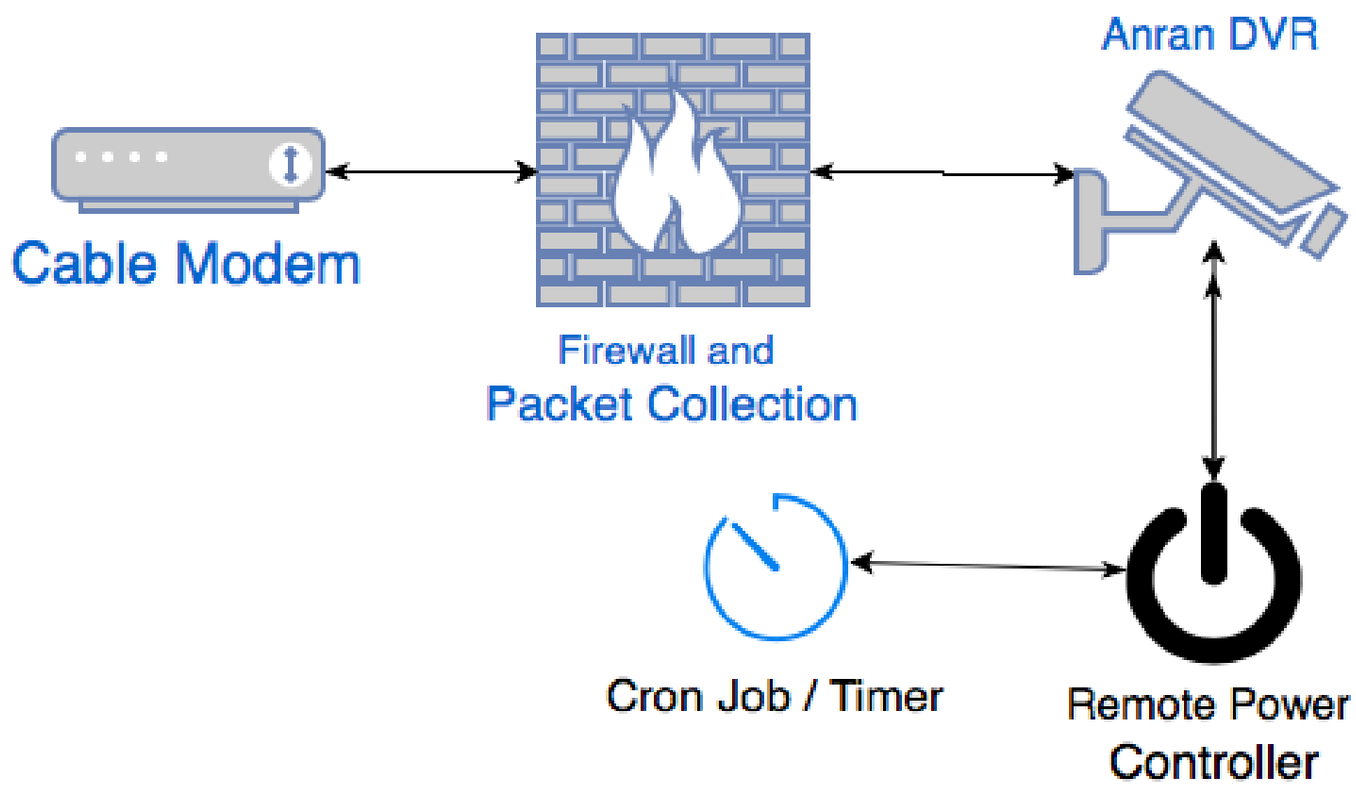
Dynamic Application Security Testing (DAST)

Interactive Application Security Testing (IAST)

The criminal and the curious constantly scan the Internet for the targets of opportunity.

In 2004, a Windows XP computer connected to the Internet was compromised within 20-minutes.

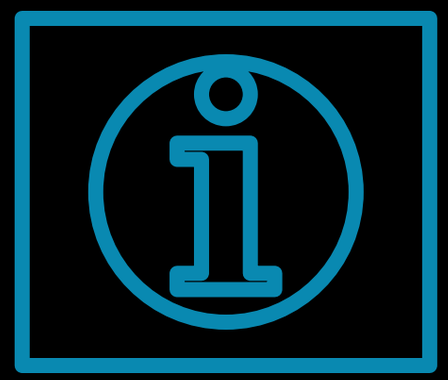
In 2017, a DVR connected to the Internet was compromised every 2-minutes.




MARVEL
AVENGERS
AGE OF ULTRON
@jwgoerlich

Constantly scan our equipment for vulnerabilities. Track and report on any exploitable action.

Survey the Land



Runtime Application Self-Protection (RASP)

Web Application Firewall (WAF)

@jwgoerlich

Be Rugged. Fix Defects.

Vulnerabilities are inevitable

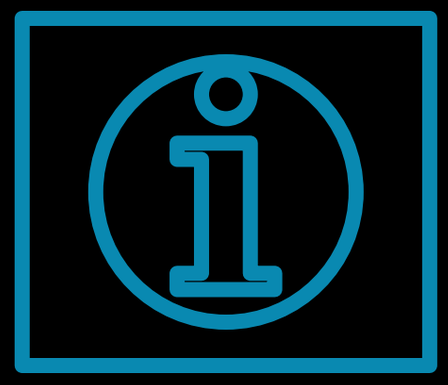
SOFTWARE AND PATCH MANAGEMENT

STRUTS

@jwgoerlich

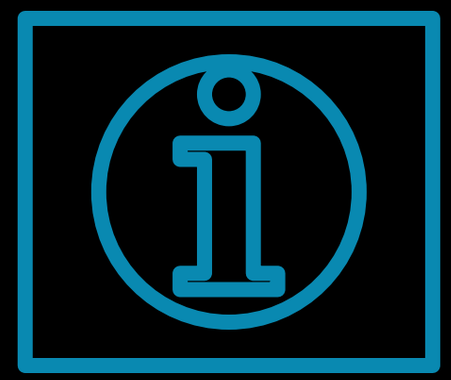
We can’t wait for the permanent fix (patching). Deploy tools that provide immediate risk reduction without slowing us down.

Stop Building Castles



Constantly monitor user behavior and note ways applications are misused and abused.

Survey the Land



DevOps Development Lifecycle

Security Review: Design Review
Security Review: Code Review
Static Application Security Testing (SAST)
Dynamic Application Security Testing (DAST)
Interactive Application Security Testing (IAST)
Software Composition Analysis (SCA)
Change Monitoring
File Integrity Monitoring (FIM)
Infrastructure Vulnerability Management
Runtime Application Self-Protection (RASP)
Web Application Firewall (WAF)

Penetration Testing

@jwgoerlich

Automate them!

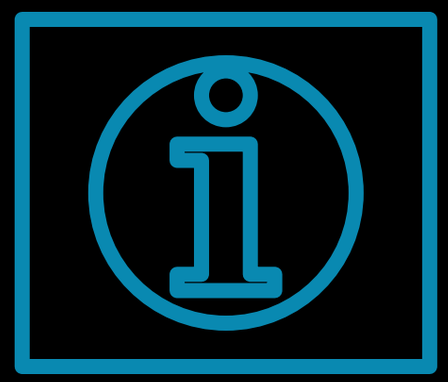
39% of DevOps have automated security controls in place

58% of mature DevOps have automated security controls

Organizations have a finite capacity for change. Never ask them to take on more change than they can handle.

Don’t slow work down to create security. Phase in controls at the rate of change.

Stop Building Castles

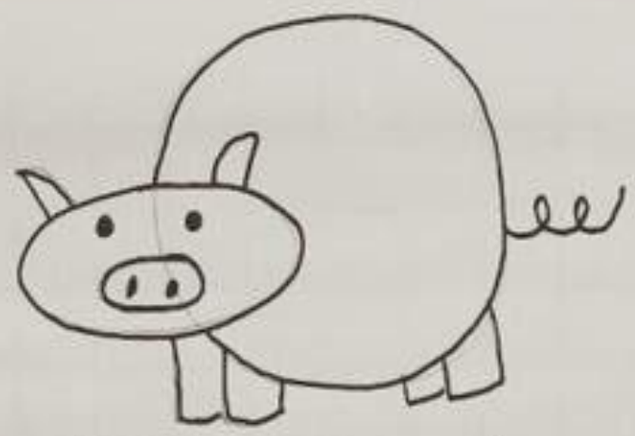


@jwgoerlich

@jwgoerlich

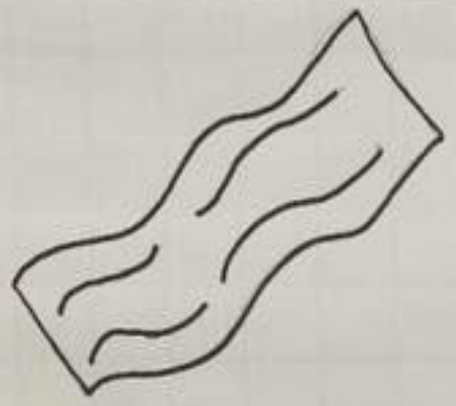
Cloud service models

Private Cloud (On-Premise)
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)



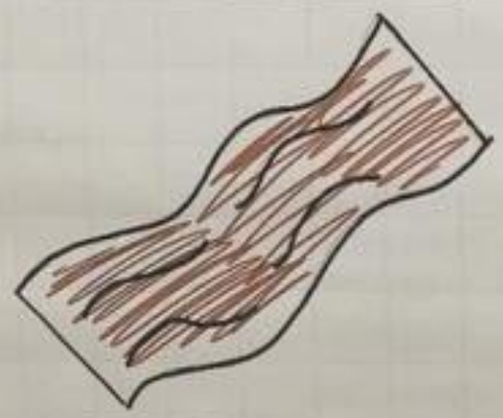
ON-PREM

Do it all



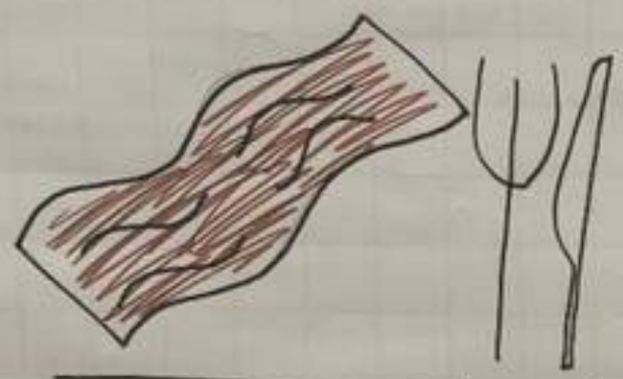
IaaS

Cook it, Serve it, Enjoy



PaaS

Serve it, Enjoy



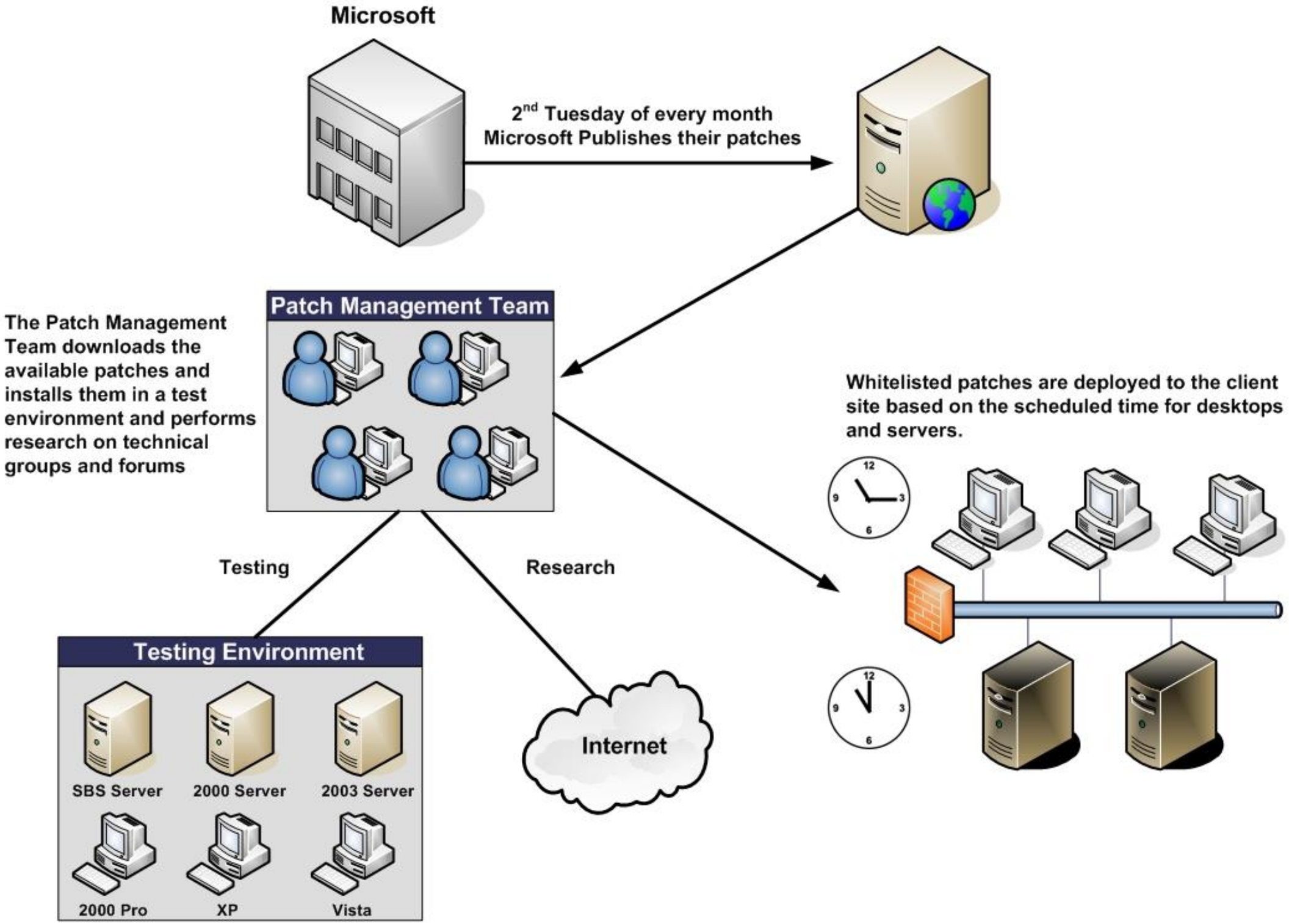
SaaS

Enjoy

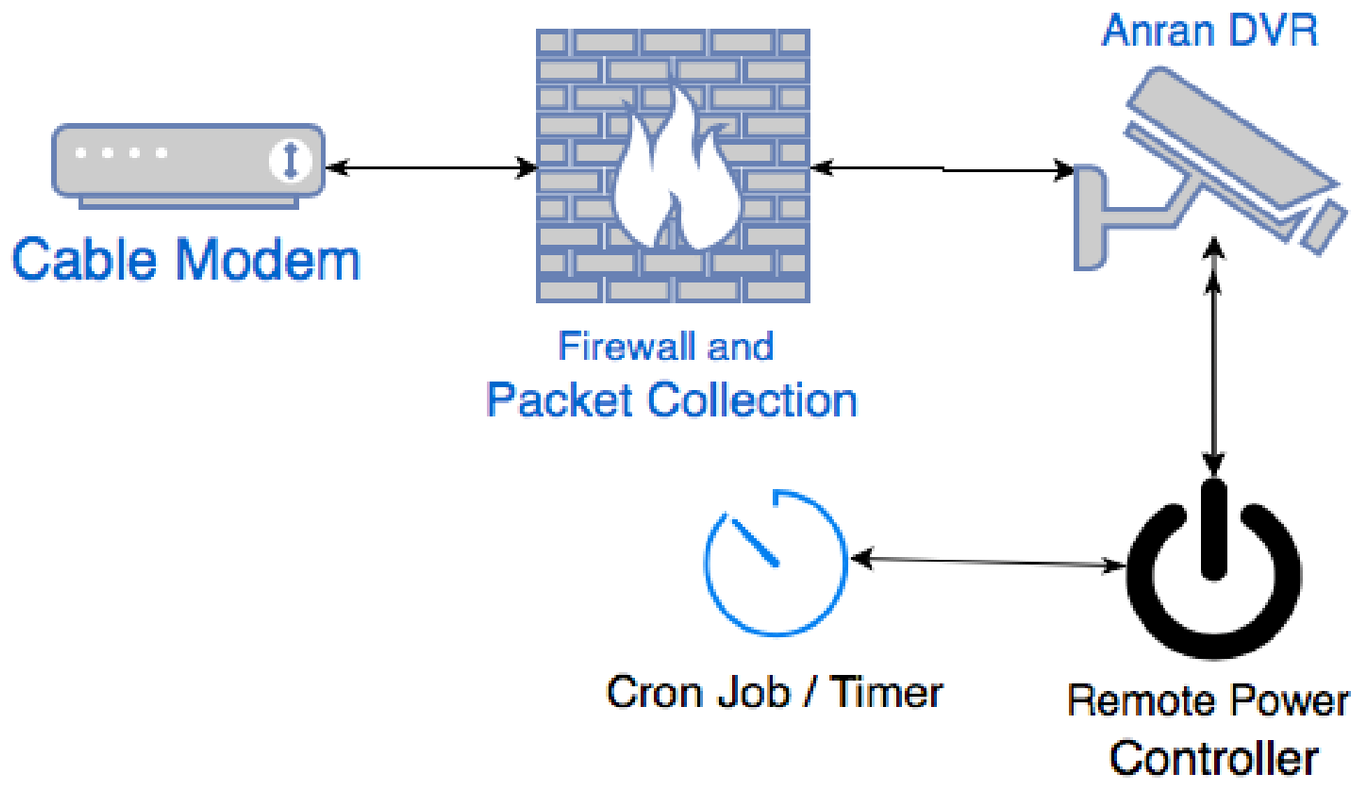
@jwgoerlich

So for classic IT …

90% of companies get attacked with 3-year old vulnerabilities.


Microsoft
2nd Tuesday of every month
Microsoft Publishes their patches
Patch Management Team
The Patch Management Team downloads the available patches and installs them in a test environment and performs research on technical groups and forums
Whitelisted patches are deployed to the client site based on the scheduled time for desktops and servers.
Testing
Research
Testing Environment
SBS Server
2000 Server
2003 Server
2000 Pro
XP
Vista
Internet

In 2017, a DVR connected to the Internet was compromised every 2-minutes and logged into using default credentials.



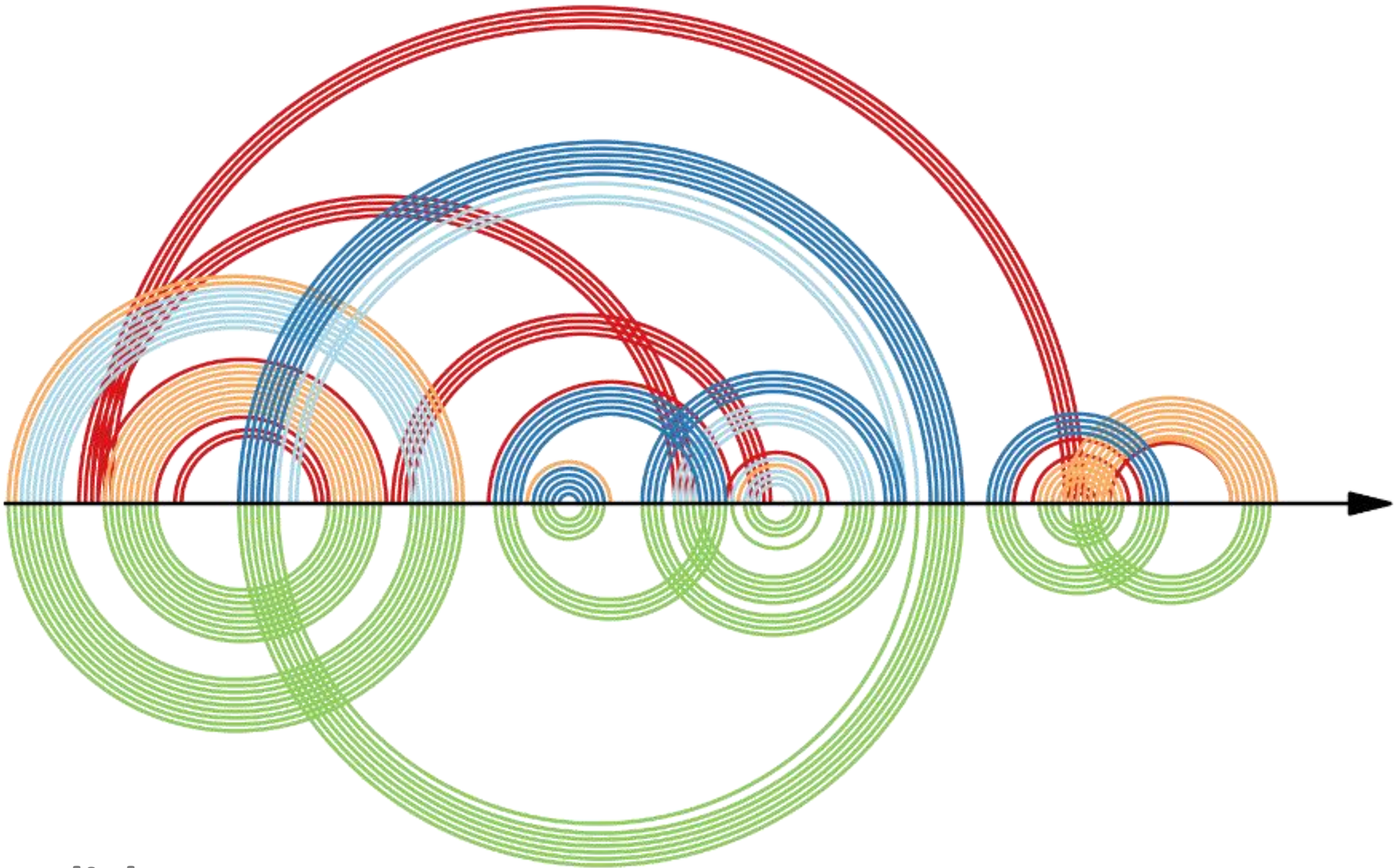
EQUIFAX®

Username: admin | Password: admin

Infrastructure Vulnerability Management

@jwgoerlich

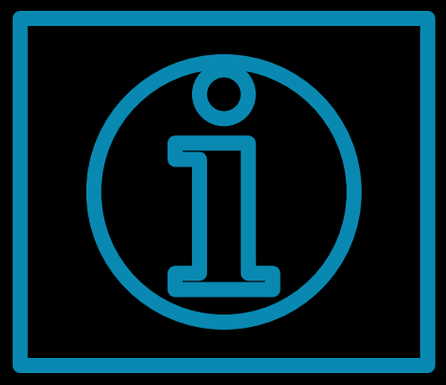
Think Feedback Loops



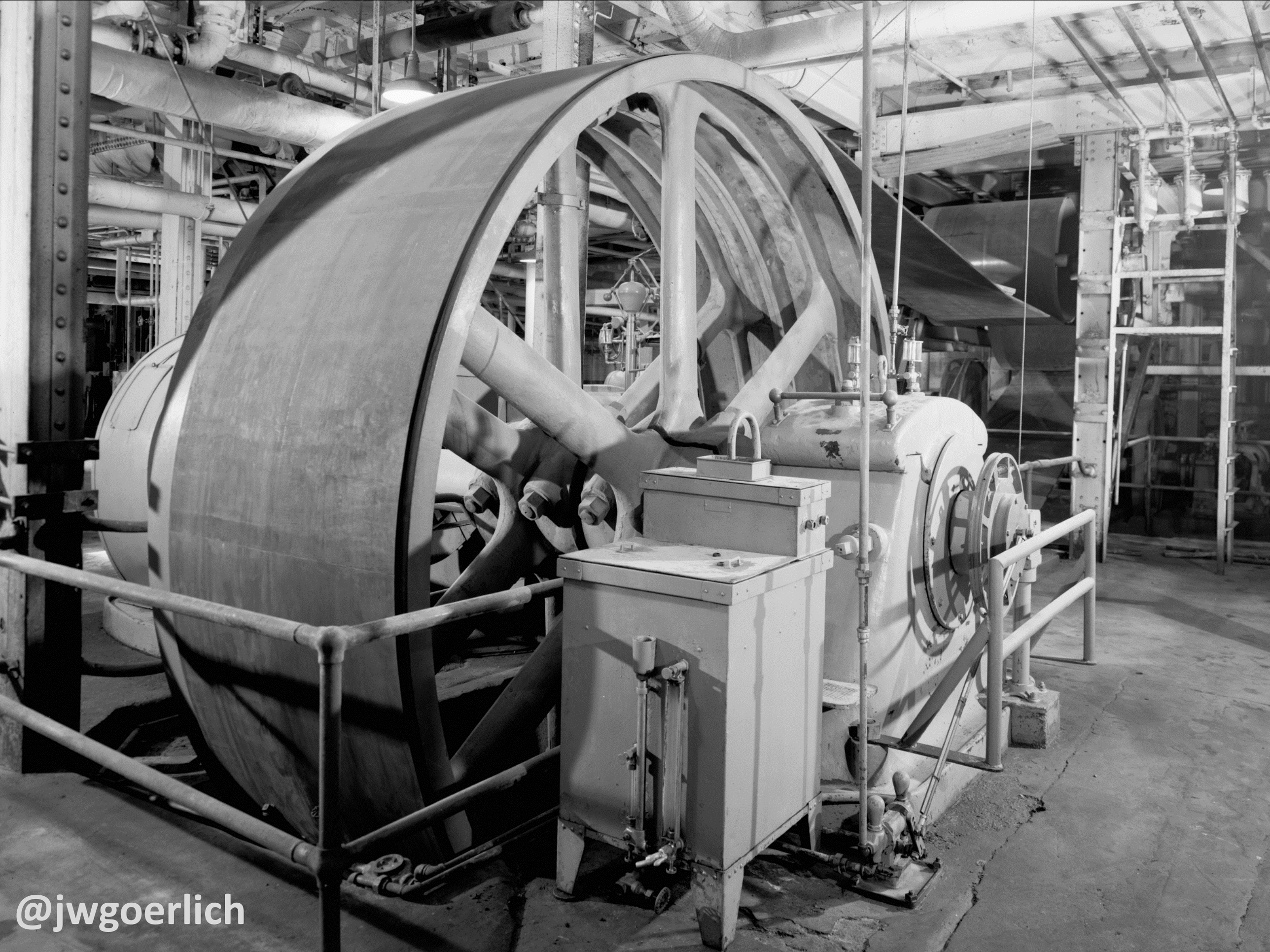
@jwgoerlich

Create a culture of quality and security one change at a time.

Cyber Security Street Smarts



@jwgoerlich


@jwgoerlich

@jwgoerlich

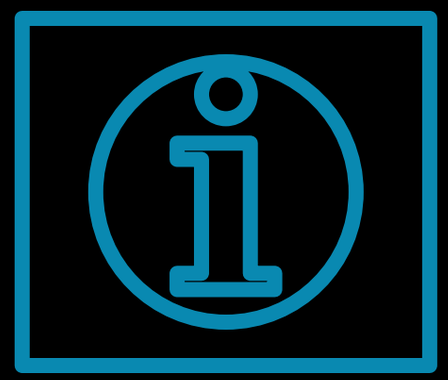
CIOs think there are
30-40 Cloud Apps

Employees actually use
928 Cloud Apps

Know what we have.

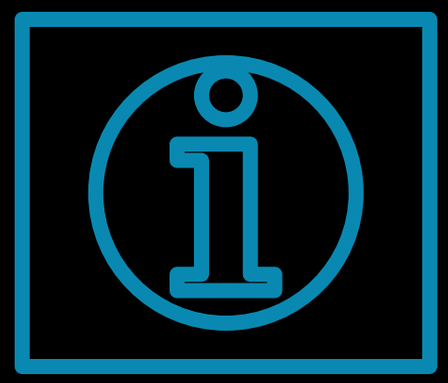
Know what it means.

Survey the Land



Culture is built one conversation at a time. Use this time well.

Cyber Security Street Smarts



@jwgoerlich

“Through 2020, 95 percent of cloud security failures will be the customer's fault.”

Gartner®

@jwgoerlich

On-Premise and IaaS

CIS Critical Security Controls (CSC)
CSA Cloud Controls Matrix (CCM)

Center for Internet Security®

cloud
CSA security
alliance®

@jwgoerlich

IaaS and PaaS

Vendor Reference Architecture
Vendor Security Controls

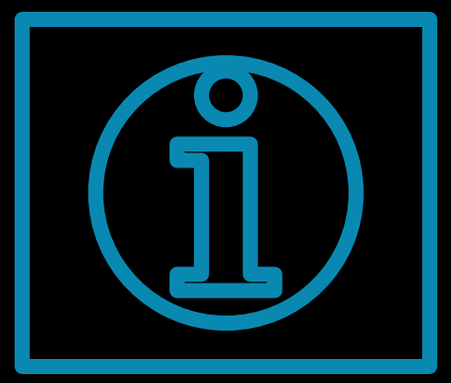
SaaS

Ours? See above.

Theirs? Vendor risk management.

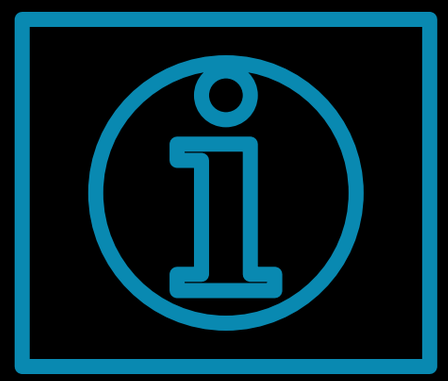
Use control frameworks to get a quick insight into industry standards.

Standards and Practices



Start with the controls that provide visibility of risks and detection of threats.

Survey the Land



@jwgoerlich

Interview to Assess the Maturity

0.0 – Not performed or documented. Get a cape.
0.5 – Partially performed or documented. Wear the cape.
1.0 – Fully performed. Fly!

Interviews

Make it seem like …

@jwgoerlich

Interviews

But behind the scene

@jwgoerlich

Technical Validation

Existence – does the technical control exist as describe?

Effectiveness – will the technical control stop the attack?

Circumventable – can the technical control be bypassed?

Operational – is the control monitored, backed by people and process?

“We have this category that Equifax calls unhandled malware, which traditional security approaches haven't been very helpful. Putting in FireEye has really helped us detect this unhandled malware, then gives us the capability to take action to stay secure.

-- Tony Spinelli, SVP and CSO, Equifax”

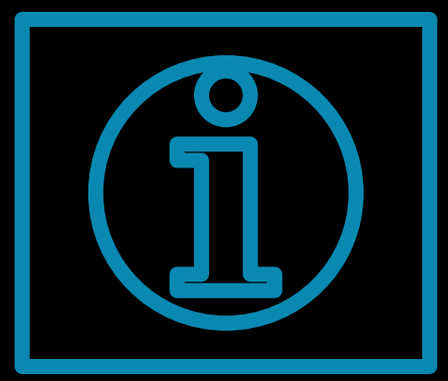
We can never attest to security.

@jwgoerlich

@jwgoerlich

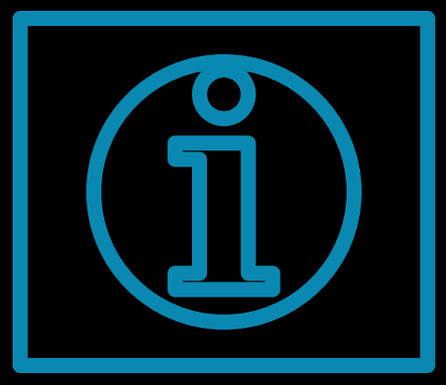
We can attest a strong set of detection and prevention at the point we last checked.

Position of Strength



Automate setting controls.
Automate auditing controls.

Stop Building Castles

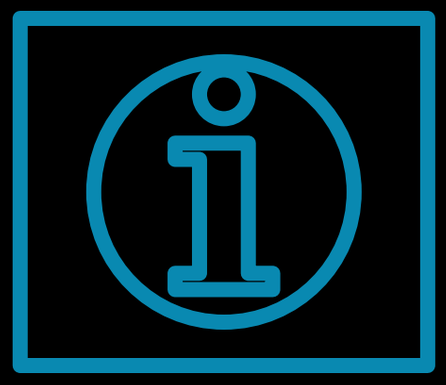


@jwgoerlich

Organizations have a finite capacity for change. Never ask them to take on more change than they can handle.

Phase in cloud security controls at the rate of change.

Stop Building Castles



@jwgoerlich

Securing without Slowing

Cyber Security Teams

DevOps and IT Engineering

@jwgoerlich

Stop Building Castles

Create Flexible and Fast Defenses

@jwgoerlich

Survey the Land Often

Focus on Visibility, Knowledge, Intuition

@jwgoerlich

Standards and Practices

Leverage Proven Defenses and Controls

@jwgoerlich

Position of Strength

Create and Assert a Defensive Core

@jwgoerlich

Create Street Smarts

Create a Culture of Cyber Security

@jwgoerlich

Principles

Stop building castles
Survey the land first and often
Leverage standards and practices
Defend from a position of strength
Create cyber security street smarts

Thank you

J Wolfgang Goerlich
wolf@jwgoerlich.com
https://jwgoerlich.com
www.youtube.com/user/jwgoerlich