IBM Security

“My Super Power is Artificial Intelligence!”

Michele M. Sullivan
Global Application Security Segment Leader
Msulliv@us.ibm.com

IBM

August 6, 2018

“Security has and will always be about understanding, managing, and mitigating the risk to an organization’s most critical assets.” - **Dr. Eric Cole, SANS Institute**

- According to Ponemon Institute's "2017 Cost of Data Breach Study" sponsored by IBM, the average cost of a data breach is $3.62 million. Further, by adopting business continuity management practices, organizations are able to reduce the total cost of a breach by 16.2% and identify and contain a data breach 78 days faster
- IBM’s Application Security Testing solutions provide preemptive protection for mobile and web-based applications. They secure apps from malicious vulnerabilities and help organizations to remediate potential attacks in the future. The best application security defense strategy is designing and building secure applications
- There are different techniques, both automated and manual, used to test applications for unknown vulnerabilities.
  - **Dynamic Application Security Testing** (DAST)
  - **Static Application Security Testing** (SAST)
  - **Interactive Application Security Testing** (IAST)
  - **Application Pen Testing**

IBM Application Security

Application security testing solutions provide preemptive protection for mobile & web-based applications

Business Value

- Provides clear visibility across the application development infrastructure
- Helps identify and prioritize applications based on their business impact
- Assesses applications for vulnerabilities
- Places vulnerabilities in context to determine their risk levels
- Mitigates risk by correcting vulnerabilities or implementing necessary fixes

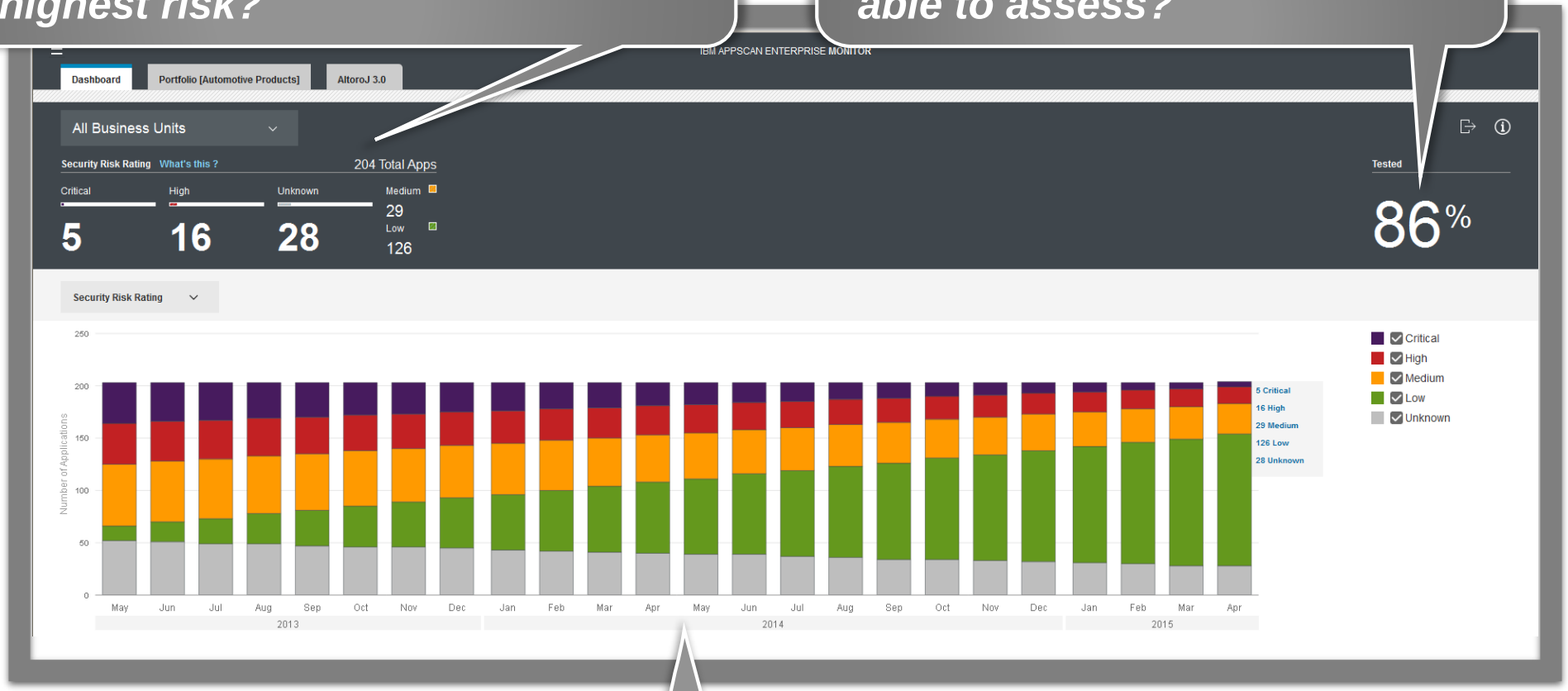
Highlights

- Improves application security program management
- Assesses software code, web and mobile applications for vulnerabilities
- Automates correlation of static, dynamic and interactive application security testing results
- Uses a single console for managing application testing, reporting and policies
- With cognitive capabilities, delivers deeper and faster scan coverage of applications and eliminate false positives Integrations

Integrated Application Security Management Dashboard

What is the current state of application security? Which applications present the highest risk?

How many of the applications in our portfolio have we been able to assess?



Is our application security posture improving?

Application Security Deployment Solutions

On-Premise

Custom program

- Scalable
- Customizable
- Comprehensive

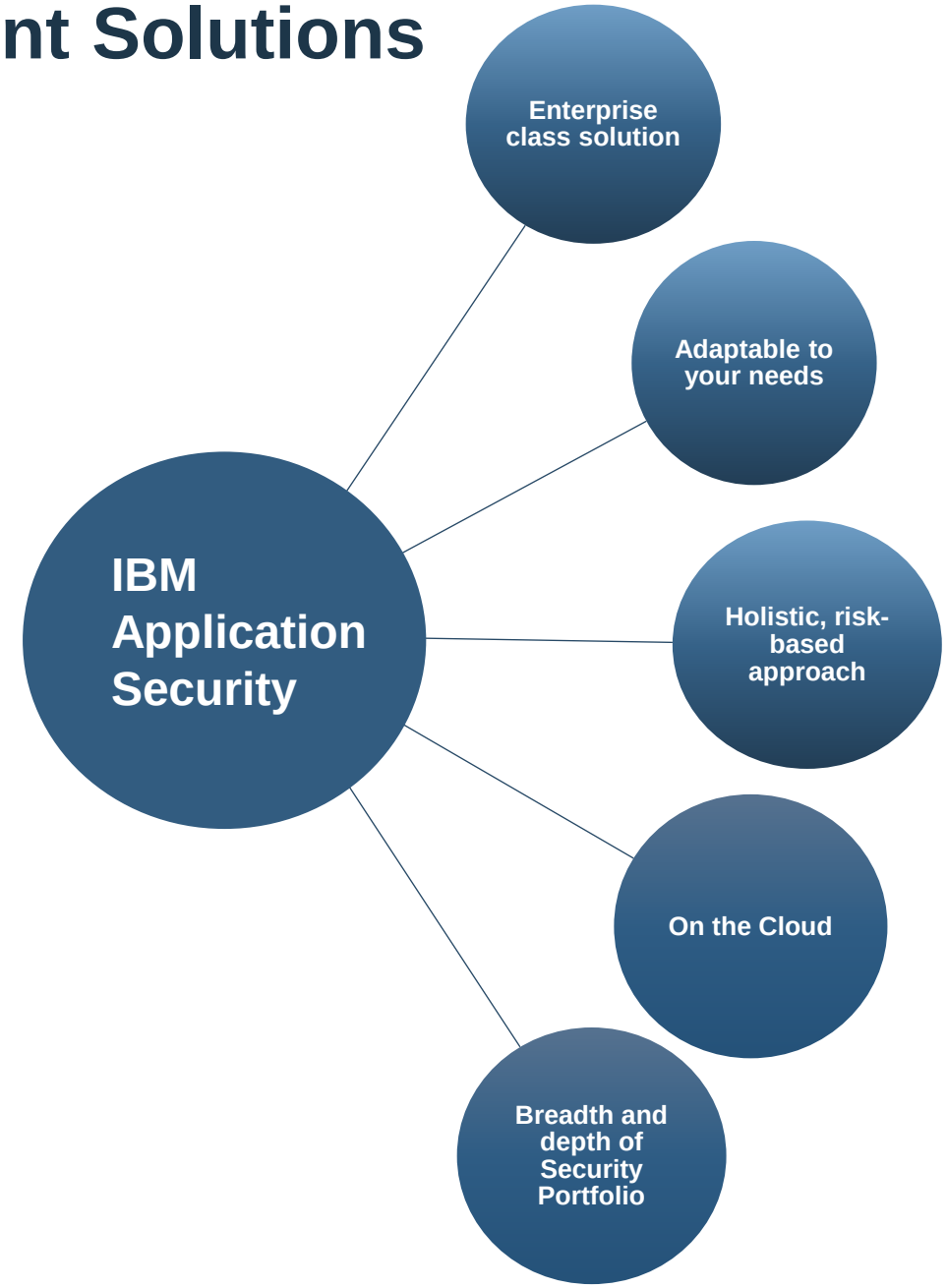
IBM Security AppScan

SaaS

Testing focus

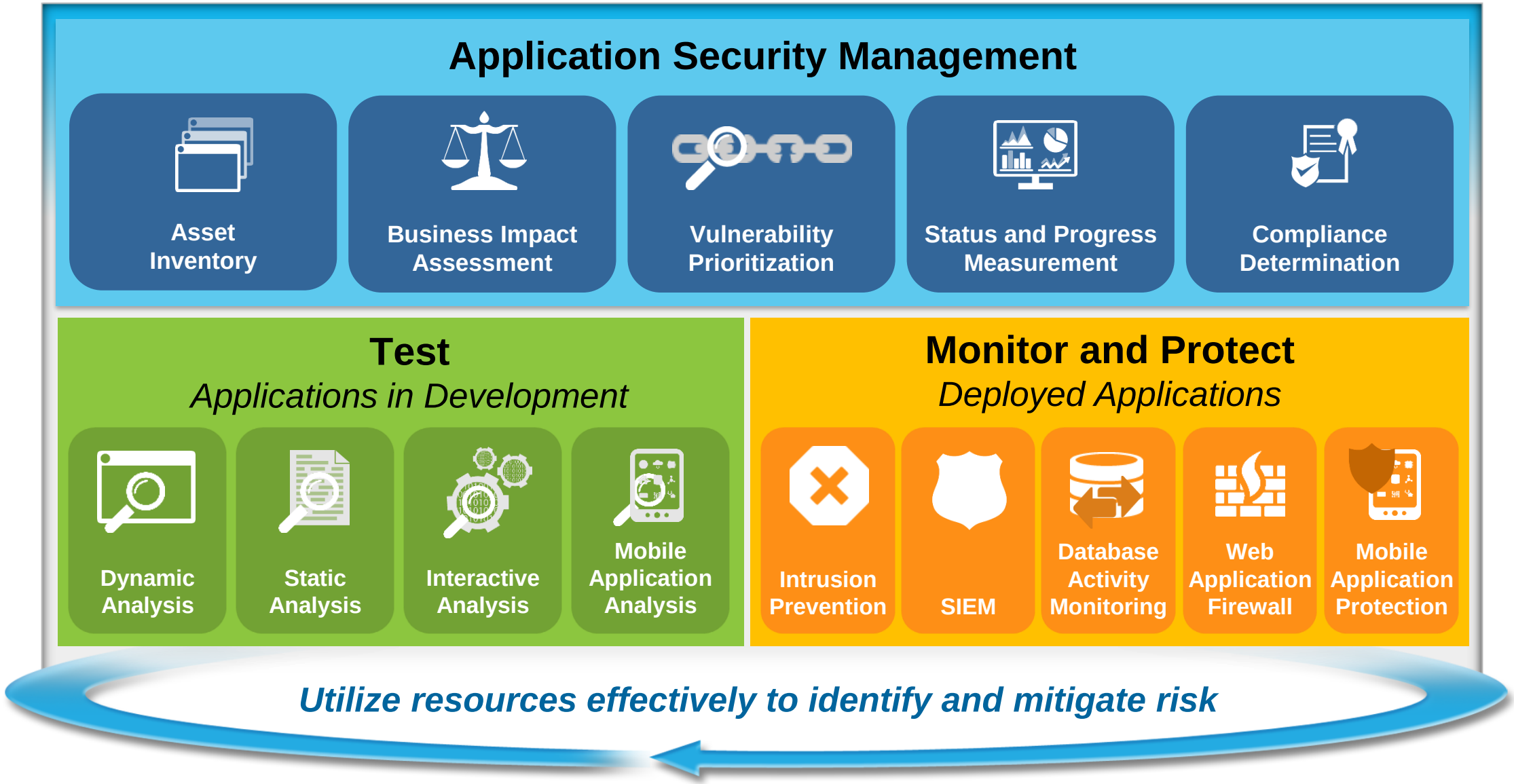
- Simple
- Self-Service
- Quick results

IBM Application Security on Cloud

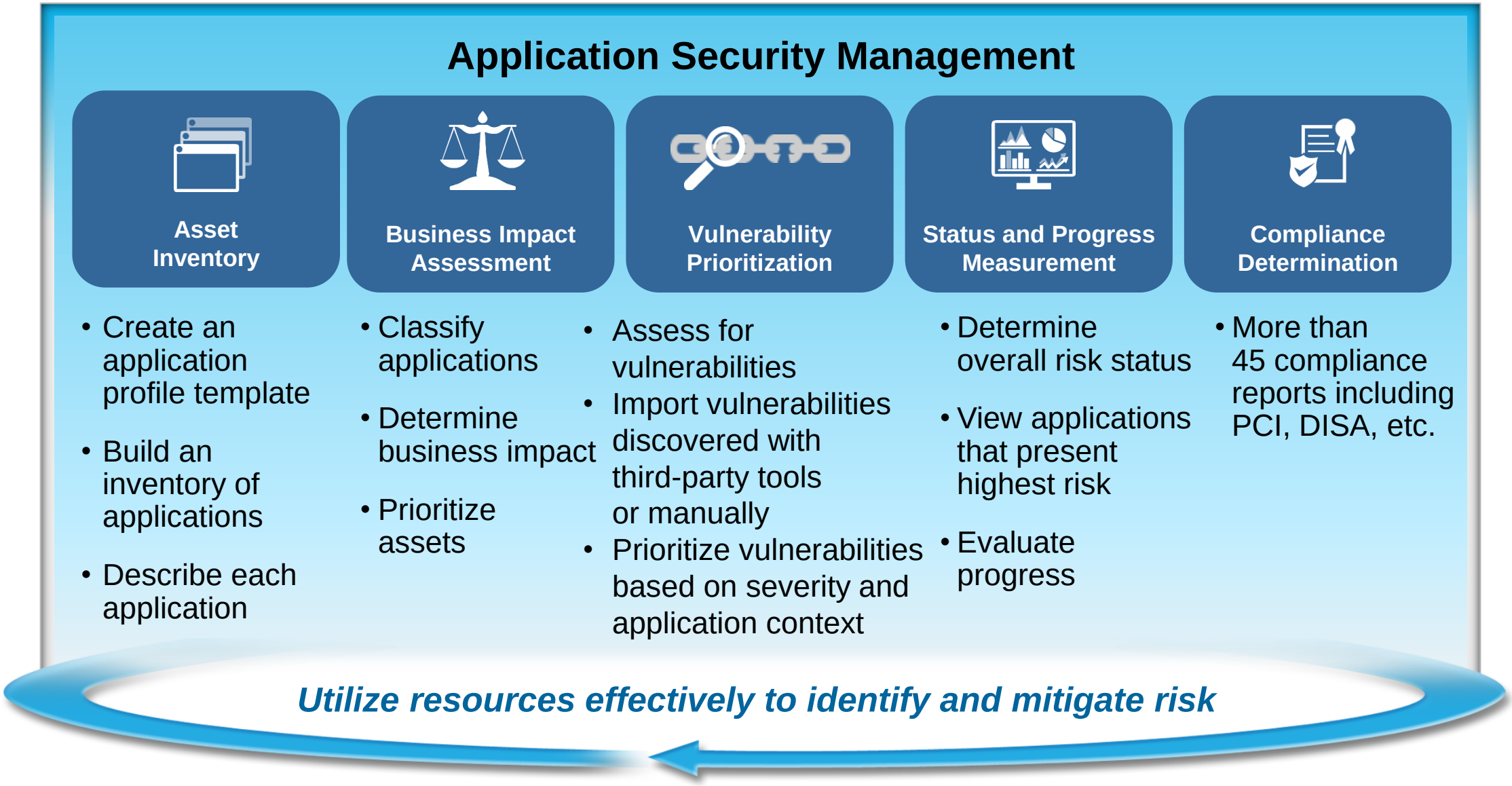


Application Security Risk Management Framework

IBM Application Security Framework



Risk-based Approach to Application Security Management



IBM Application Security on Cloud

Application Security on Cloud Overview

Application Security Management

Use a single console for managing application risk, test results, reporting and policies

Dynamic
Identify vulnerabilities in running applications

Static
Deeper analysis of application code

Mobile
Interactive testing of a Mobile binary

Open Source
Identify unique vulnerabilities introduced by open source packages

Intelligent Code Analytics
Deep analysis of APIs and frameworks

Intelligent Finding Analytics
Improves speed & accuracy of application code analysis

GDPR
Map vulnerabilities to GDPR articles and generate compliance report

Identify and remediate high-priority vulnerabilities

IBM Application Security on Cloud

Simple

Easy as 1-2-3

Fast

Fully-Automated Solution

Comprehensive

Based on AppScan engines

Safe

Meets IBM Security standards

#CoverYourApps

IBM Application Security on Cloud

Easy as 1, 2, 3!

Does my application contain security vulnerabilities?

1 → 2 → 3

Enter URL / Upload Application

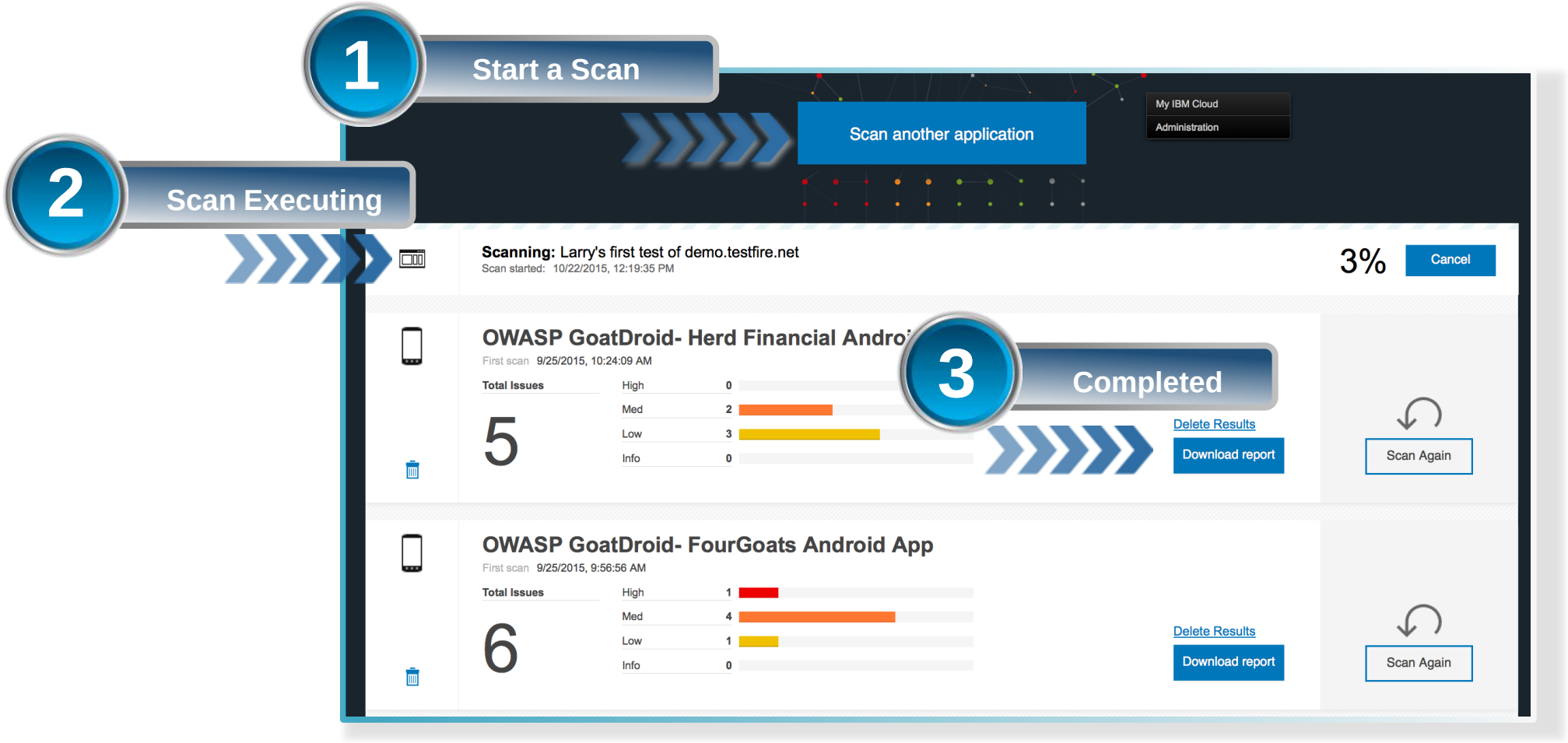
Scan application

Review Report

Simple

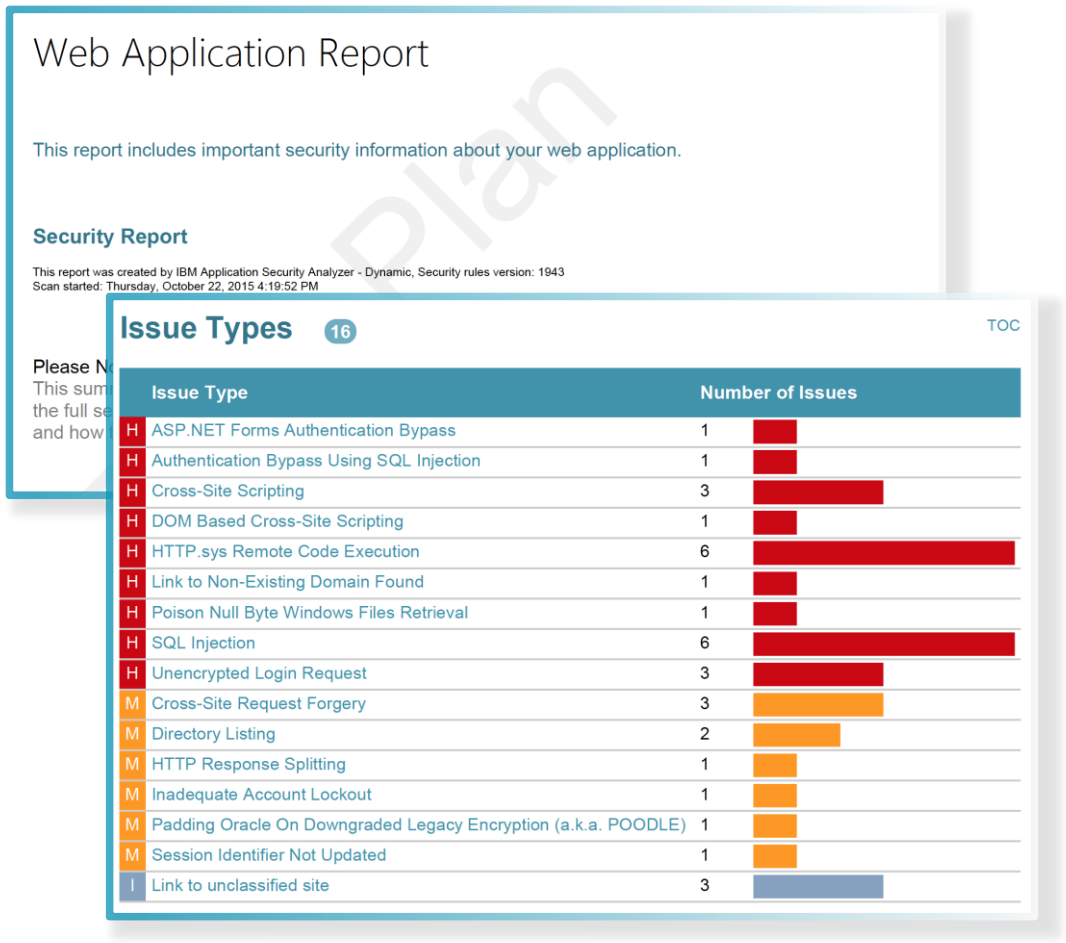
Application Security on Cloud

List of Running & Completed Scans



Results based on Industry-Leading AppScan Engines

Security Issues & PCI compliance report examples



Web Application Report

This report includes important security information about your web application.

Security Report

This report was created by IBM Application Security Analyzer - Dynamic, Security rules version: 1943
Scan started: Thursday, October 22, 2015 4:19:52 PM

Please N
This sum
the full s
and how

Issue Types 16 TOC

	Issue Type	Number of Issues
H	ASP.NET Forms Authentication Bypass	1
H	Authentication Bypass Using SQL Injection	1
H	Cross-Site Scripting	3
H	DOM Based Cross-Site Scripting	1
H	HTTP.sys Remote Code Execution	6
H	Link to Non-Existing Domain Found	1
H	Poison Null Byte Windows Files Retrieval	1
H	SQL Injection	6
H	Unencrypted Login Request	3
M	Cross-Site Request Forgery	3
M	Directory Listing	2
M	HTTP Response Splitting	1
M	Inadequate Account Lockout	1
M	Padding Oracle On Downgraded Legacy Encryption (a.k.a. POODLE)	1
M	Session Identifier Not Updated	1
I	Link to unclassified site	3

Regulations

The Payment Card Industry Data Security Standard (PCI) Version 3.0

Summary

The Payment Card
data security and
baseline of technic

PCI DSS comprise
additional controls
Additionally, legisla
information or othe
laws, government

The PCI DSS secu
environment. The
process, or transm

"System compone
components includ
authentication serv
example, name re

Virtualization comp
applications/deskto

Network compone
appliances, and ot

Server types includ
Protocol (NTP), an

Applications includ
applications. Any

Violated Section

Issues detected across 26/32 sections of the regulation:

Sections	Number of Issues
Requirement 2 - Do not use vendor-supplied defaults for system passwords and other security parameters.	4
Requirement 2.1 - Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.)	3
Requirement 2.2.2 - Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	5
Requirement 2.2.4 - Configure system security parameters to prevent misuse.	5
Requirement 2.2.5 - Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems.	6
Requirement 2.3 - Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web based management and other non console administrative access.	3
Requirement 2.6 - This section applies to web applications that are used by hosting providers for hosting purposes – Hosting providers must protect each entity's hosted environment and data.	21
Requirement 4 - Encrypt transmission of cardholder data across open, public networks.	3
Requirement 4.1 - Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. Examples of open, public networks include but are not limited to: • The Internet • Wireless technologies, including 802.11 and Bluetooth • Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA) • General Packet Radio Service (GPRS). • Satellite communications.	3
Requirement 6 - Develop and maintain secure systems and applications.	32

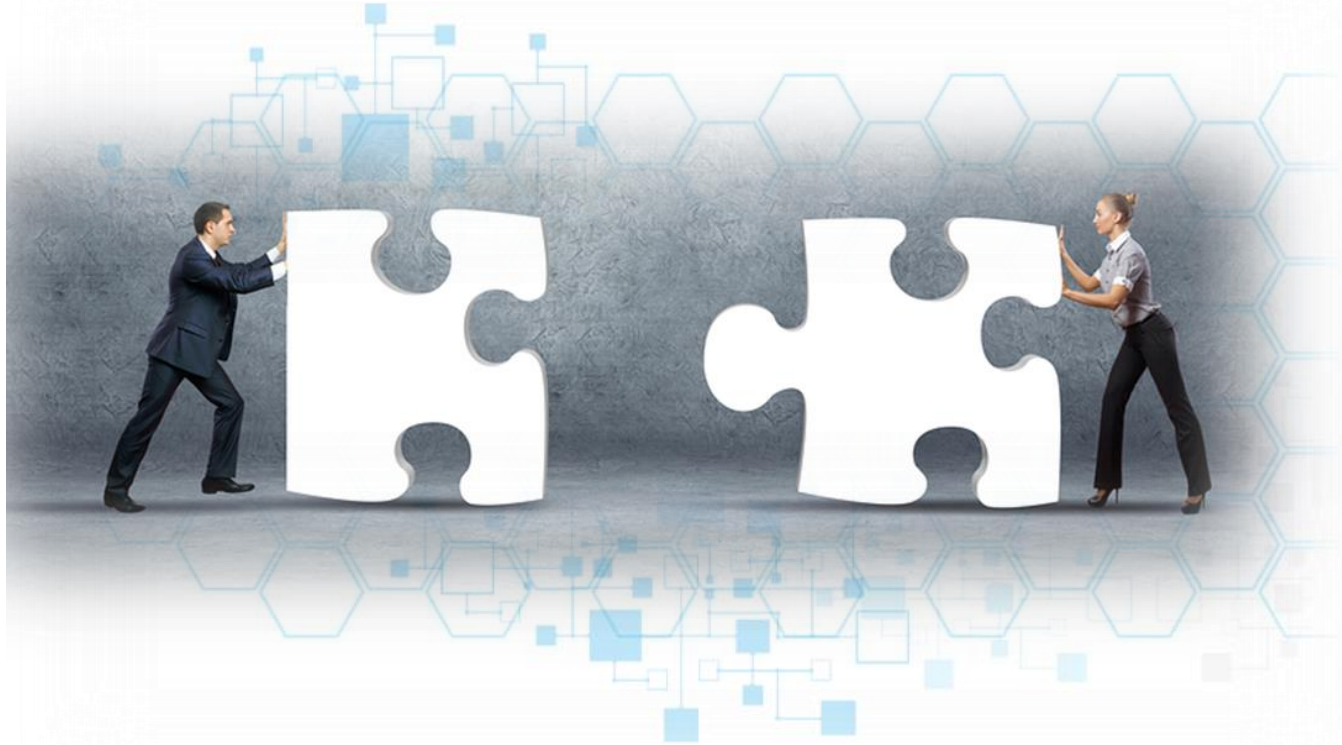
Register, test and generate results… *Quickly!*

- Convenient registration
  for immediate access to service
- Minimal to no set-up time
  for your environment
- Launch security scans 24 x 7 x 365
- Superior results without requiring
  “behind the scenes” experts

Fast

Quickly Plug into Your Application Lifecycle

Streamlined Incorporation into Existing DevOps / Continuous Integration Frameworks



- UrbanCode, Maven, Bamboo, Jenkins plug-ins available
- IDE Visual Studio, Eclipse, IntelliJ
- Extend your environment with robust REST API

One-Stop Shop for Application Security Testing

Analyze all app types:

- Web apps
- Mobile apps
- Desktop apps

Run all tests:

- DAST
- SAST
- IAST
- Open Source

Comprehensive

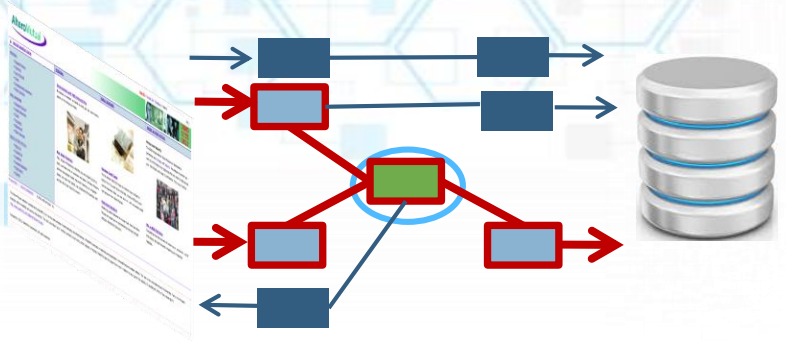
Applying Cognitive Computing to security vulnerability analysis

*Machine learning with Intelligent Findings Analytics**

Scan results

Learned results

- 98.91% accurate in eliminating false positives
- Minimize “unlikely attack scenarios”
- Provide fix group recommendations that resolve multiple vulnerabilities



- Built on Watson Machine Learning
- Trained by IBM Security Experts
- Fully automated review of scan findings

* Patents pending

Intelligent Findings Analytics: Real-World Results

- 90-99% average reduction to security analyst workload
  - Equal or exceeds human experts
- Returns results in seconds rather than hours or days required for manual reviews
- Seamless integration into existing development workflow

Real-World Applications	Scan Findings	IFA Vulnerabilities	Fix Groups
Application 1	12k	1k	35
Application 2	247k	1.2k	103
Application 3	746k	483	42

AppScan applies Cognitive capabilities to application security testing

AppScan Cognitive Application Security Advisor

- **Intelligent Code Analytics**

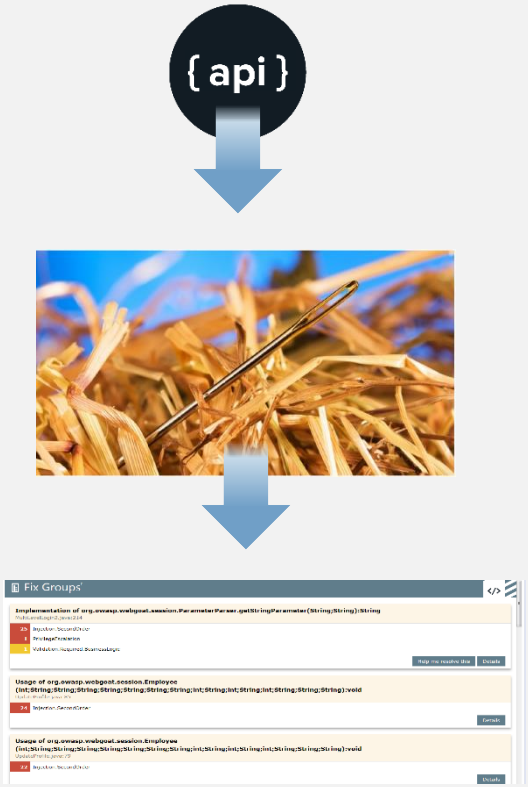
  Expands analysis coverage and eliminates **false negatives** by generating Security Rules for ANY framework used by an application during trace analysis.

- **Intelligent Findings Analytics**

  Reduces **false positives** by up to 99% & eliminates lengthy manual review processes by provides fully-automated review of Application Security Testing findings.

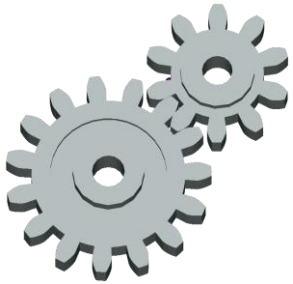
- **Simple Fix Group recommendations**

  Provides fix recommendations that help development teams resolve multiple vulnerabilities with a single code fix.



No Other solution on the market can improve scan times, depth of scan & quality with cognitive capabilities

Keys to successfully integrating Security into DevOps



Automation

Integration into existing Development tooling/processes

Speed

Roundtrip analysis (Submit & Retrieve Scan Results)

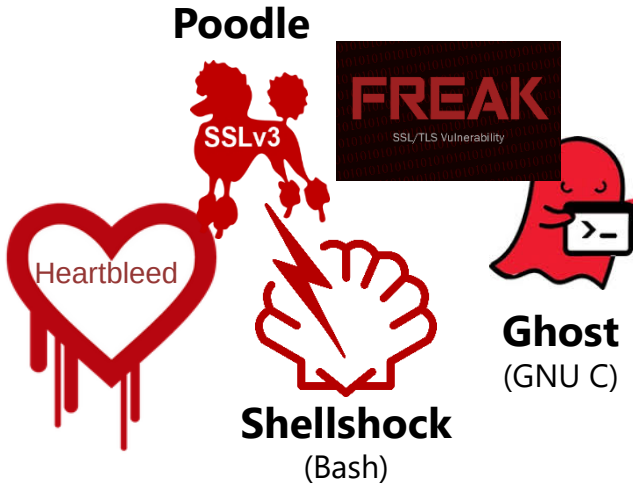
Coverage

Breadth and Depth of analysis of your Application Inventory

IBM Open Source Analyzer

Forrester: *How To Leverage DevOps Trends To Strengthen Applications Dec. 2016*

"Approximately 80% to 90% of the code in modern applications is from open source components, and open source components that are at least two years old have three times the number of vulnerabilities. Even when developers are diligent about using newer third-party libraries, these libraries often use other libraries of their own, resulting in latent vulnerabilities that expose themselves at a later date.



ASoC Open Source Analyzer

- Builds a manifest of an application usage of Open Source
- Checks for Open Source vulnerabilities
- Industry leading DB of over 180k vulnerabilities
- Remediation instructions on OSS version to upgrade to
- Integrated into application vulnerability testing

Comprehensive Application Security Collateral

Fuel the AppSec Discussion!

- **IBM Security AppScan Customer Trial:** Link to Trial
- Application Security Customer Brochure
- **Gartner Analyst Report:** IBM Maintains Leadership Position in 2018 Gartner Magic Quadrant for Application Security Testing
- **E-Guide:** Mitigate Business Risk Strategically With Application Security Management
- **Forrester Total Economic Impact Study (IBM AppScan Source Client):** Forrester TEI Reveals Triple Digit ROI for IBM AppSec Testing Solution
- **Ponemon 2017 “State of Mobile and IoT Security” Study:** Link to Study

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

IBM