



When **your SDLC is Nimble and Safe**  
We are **happy**

# About The founder



## Francesco Cipollone NSC42



Founder – NSC42 LTD –

Nimble Security Consultancy (42 is the answer to the fundamental question of the universe (hitchhiker guide to the galaxy)

I have been in CISO and consulted with many organization. I was unhappy with the status quo and the fact that the cloud was an unknown and securing it seemed even more obscure art.

My mantra is people first technology, having an offering that combined the people aspect, and the technology was key to me

I want to empower organization to have clear visibility on their cloud environment and apply data driven and risk-based decision on what to fix.

we have been serving several organization helping them securing their application security journey like HSBC



@FrankSec42



Fracipo Linkein



Email



Website



Articles

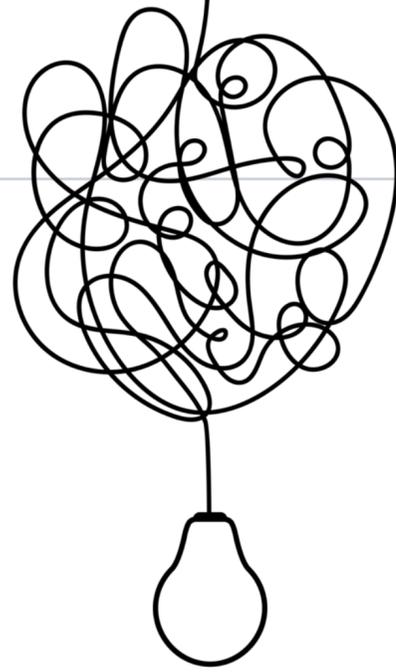


NSC42 LinkedIn



**People and technology, this should be the norm  
Visibility and data driven/risk-based decision is the modern security**

# Our Solution



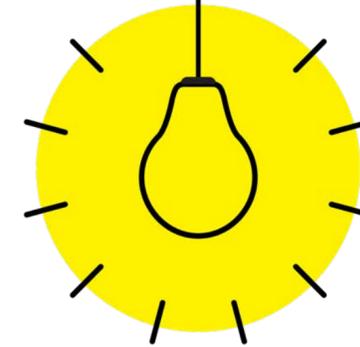
Lack Of Skills

What do I do where?

Too many tools to fix the same problem

Not enough skilled expertise

Trust & Clarity



On Demand Consultants

Maturity Model with progression

Clear set of tools to address your problems

Coaching, Training and consultancy

# Application Security Challenges

## Skills and consultancy

Application security is complex and no one solution fits all. In order to execute and solve problem skilled developers are required

## Maturity Measurement

A maturity model that shows a roadmap to evolution and enable you to assess where you are on your SDLC

## Consistency of assessment

Ad-hoc inconsistent assessment leaves holes and measuring progress is challenging

## Visibility and data driven security remediation

What issue to fix first? Which one will make me more vulnerable? answering those questions is key

## Auditability and Standards

Standard don't mean your application is secure. To have secure SDLC you need several pragmatic steps

1

2

3

4

5

Are your application secure??

The common theme around all those breaches are

1. **Bugs in code**
2. **Open source libraries**
3. **API without proper access control**
4. **Exposed applications over the web without assessment**
5. **Unknown vulnerable applications**

# Application Security Solution offered

## Skills and consultancy

Application security is complex and no one solution fits all. In order to execute and solve problem skilled developers are required

## Maturity Measurement

A maturity model that shows a roadmap to evolution and enable you to assess where you are on your SDLC

## Consistency of assessment

Ad-hoc inconsistent assessment leaves holes and measuring progress is challenging

## Visibility and data driven security remediation

What issue to fix first? Which one will make me more vulnerable? answering those questions is key

## Auditability and Standards

Standard don't mean your application is secure. To have secure SDLC you need several pragmatic steps

1

### On Demand Appsec Consultants

Appsec Consultant available every month to demystify findings

2

### Evolution & Maturity

Maturity Model and framework that enables to measure the evolution

3

### Consistent Assessment

Maturity Matrix, Progression towards higher maturity, Program of work

4

### Visualization of Vulnerabilities

Across the SDLC measurement of vulnerabilities and visualization with pragmatic reports

5

### Auditability & Standards

Compliant and providing a consistent report enable to keep auditor happy

# Breaches in Number - appsec

Adversaries don't need many vulnerabilities - ONE is enough.

Is your business equipped with the right tools to react fast enough?

Av Cost of data Breach

**3.03 m**

Every

**36 minutes**

A new security vulnerability is identified

It takes

**150-180 days**

To fix a vulnerability

N. Of Vuln per year

**1400 vuln**

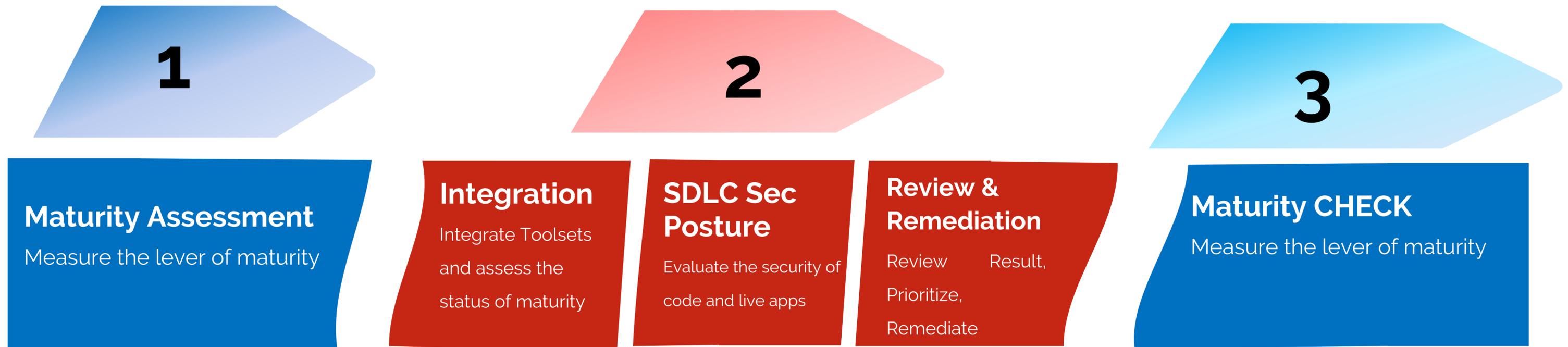
As disclosed vulnerabilities

It takes

**3-15 days**

To exploit a vulnerability

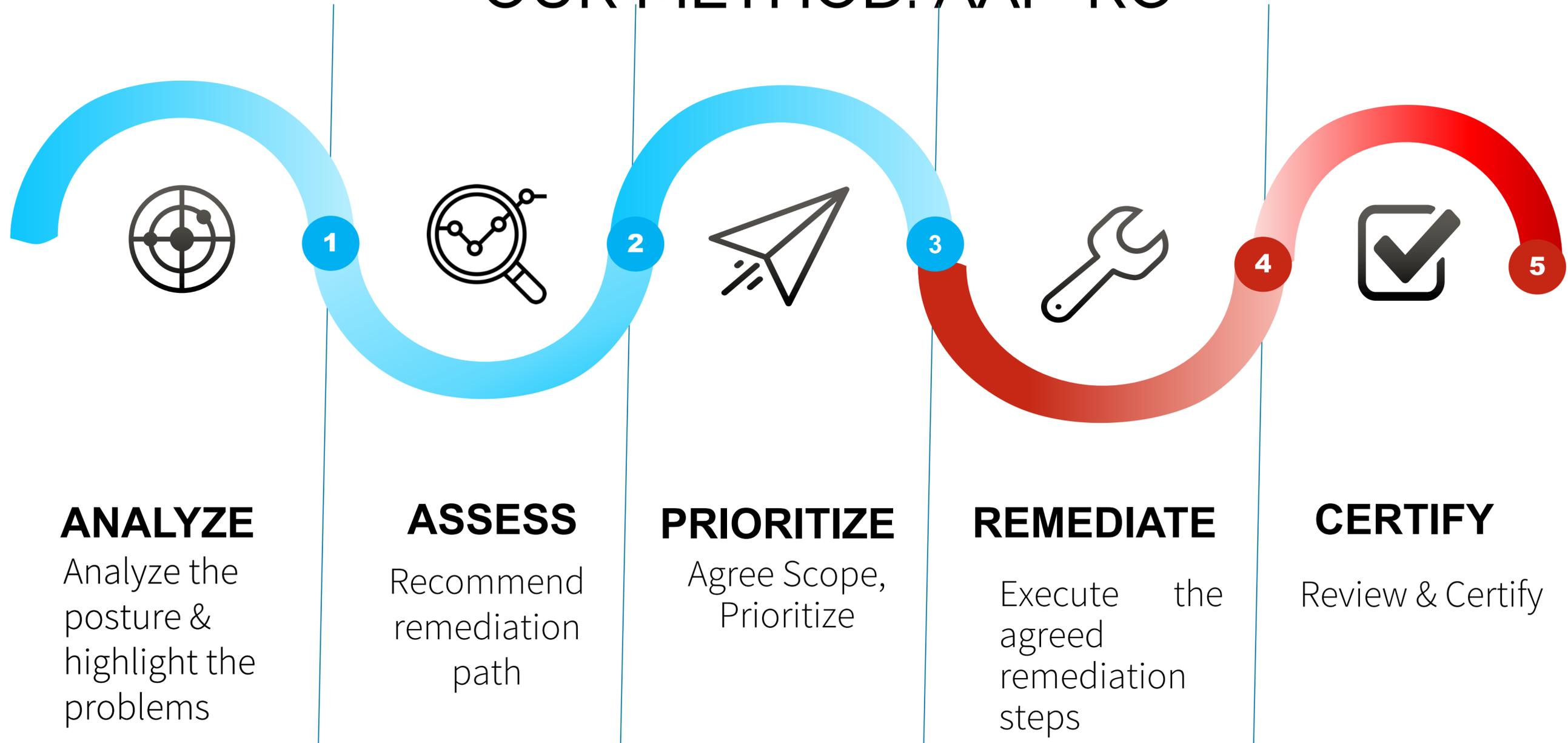
# Methodology simple and nimble as 123



# A validated methodology across our services

Your Protection is Our Success

## OUR METHOD: AAP-RC



# Our Partners

## WEB APP TESTING



## OPEN SOURCE/LIBRARIES



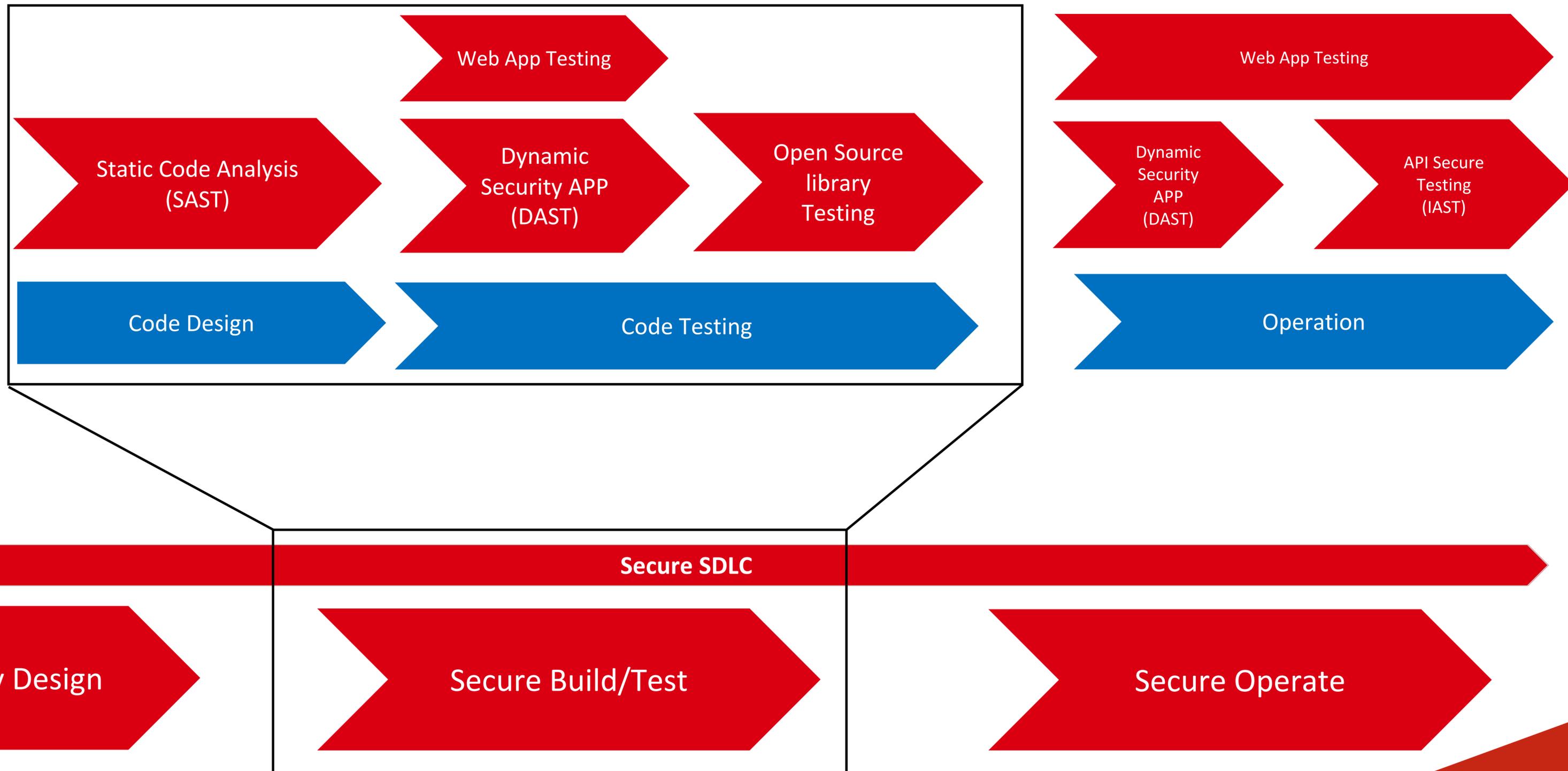
## STATIC CODE ANALYSIS



## ENVIRONMENT



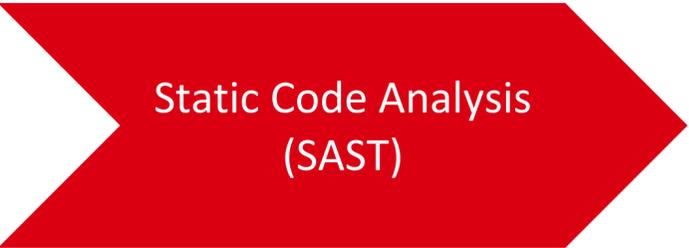
# Shift Left - Meaning



# Partner Network



CHECKMARX



# WEB APP – APPLICATION SECURITY OFFERING -

FEATURES	Bronze	Silver	Gold	Platinum
<b>Security Expert –Per Year</b>	2-5 days	12-25 days (1-2 ppl)	28-56 days (2-3 ppl)	63-100 days (5 ppl)
<b>Web Applications (FQDN)</b>	5-10	20-35	50-75	100+
<b>Assess – Tools &amp; report *</b>	Report	Portal + continuous testing	Portal + continuous testing	Portal + Continuous testing
<b>Monthly Report</b>	1 per website	1 per web + Low False Pos.	1 per web + 1 Custom	1 per web + 4 Custom
<b>Annual Audit &amp; Review</b>	✘	✘	✓	✓
<b>Remediation**</b>	✘	✘	✘	✓

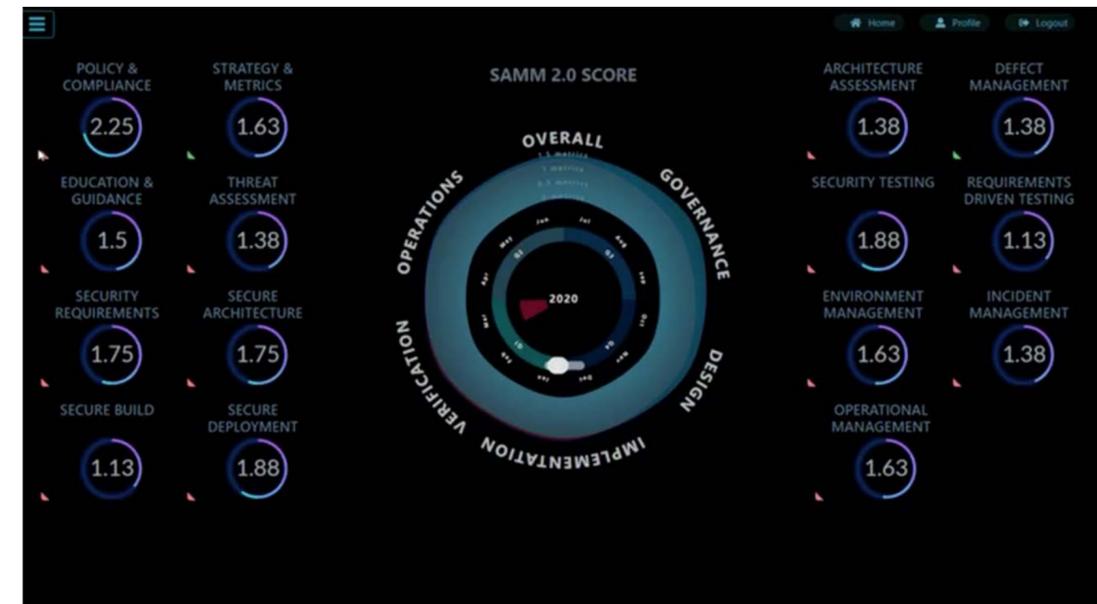
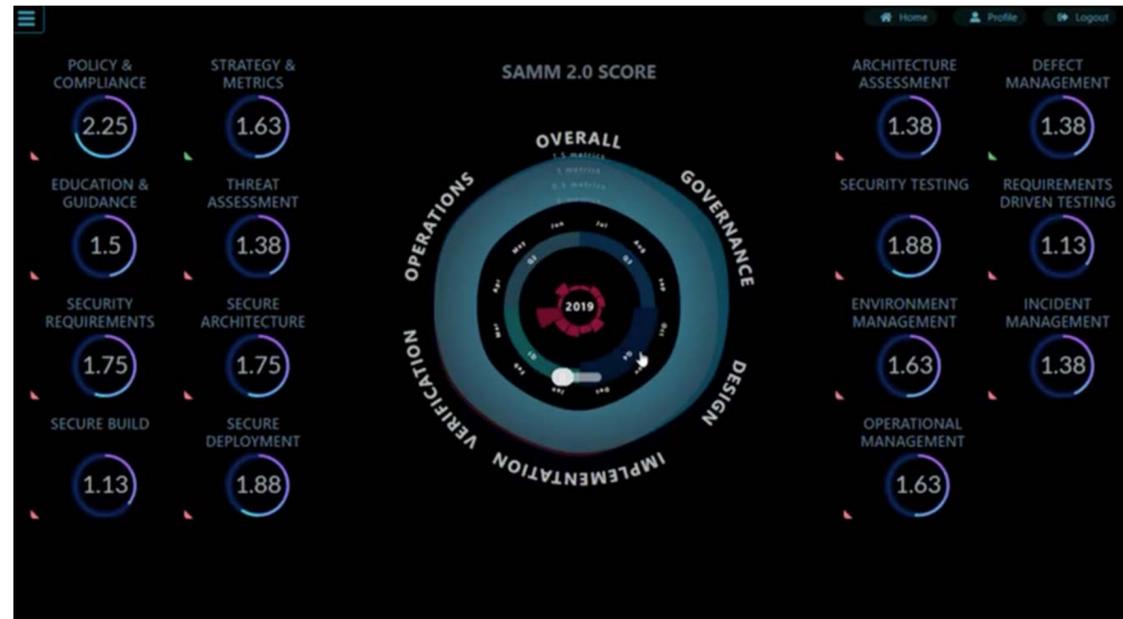
\* Offering based on the enterprise

\*\* Remediation Pricing Depends on the # of agreed Findings to fix

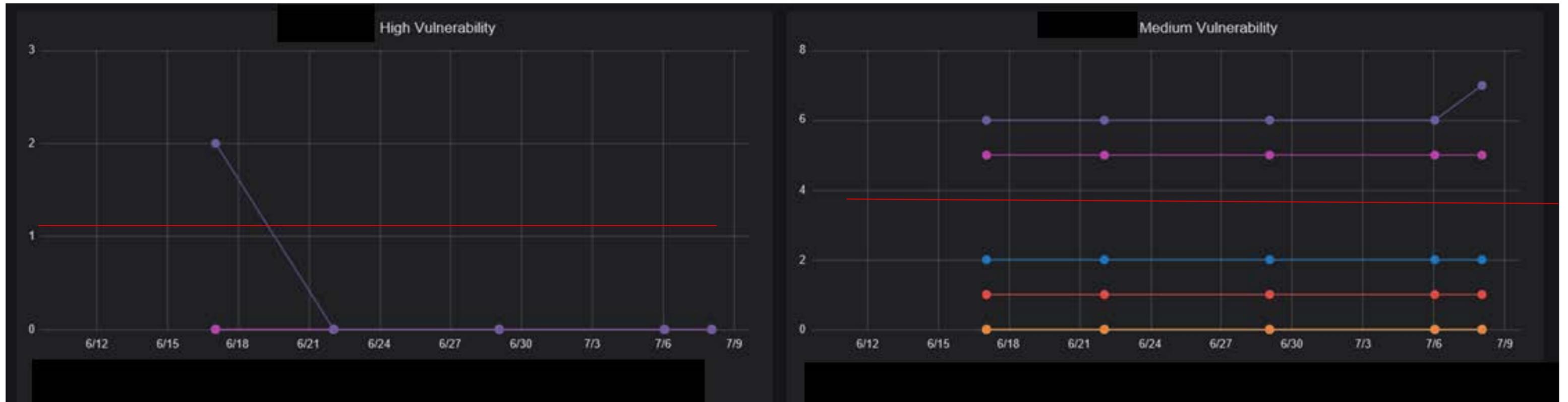
# Maturity Model Pillars



# Maturity Model Visualization



# Simple, Nimble Application Dashboards





# Fix the problem with technology – Where do you look

What do you look to assess? Where do you look

**Nexus IQ Server** Lifecycle 1.18.0-SNAPSHOT

Dashboard / Newest Risk

**VIEWING**

- 2 APPLICATIONS OF 3 (67%)
- 12 POLICIES OF 14 (86%)
- 31 COMPONENTS OF 42 (74%)

**NON-PROPRIETARY COMPONENT MATCH RESULTS**

- Exact Match 27 (87%)
- Similar Match 3 (10%)
- Unknown 1 (3%)

**RISK**

THREAT AGE	POLICY	APPLICATION	COMPONENT	BUILD	STAGE	RELEASE	OPERATE
7	7h Security-Medium	A Pristine Application	tomcat: catalina : 5.5.15	7h			
3	7h Security-Low	A Pristine Application	tomcat: catalina : 5.5.15	7h			
9	1d Security-High	A Test Scan	org.mortbay.jetty:jetty: 6.1.15	1d			

**Organization Alerts** View All

Policy	Libraries				Security	
Violations	New Versions	Multiple Versions	Multiple Licenses	Rejected In Use	Per-Library Alerts	Per-Vulnerability Alerts
112	323	13	64	0	91	539

58 31 2 225 273 41

Scans History

Full Scan Incremental Scan

5 1:49:05 PM

**Top 10 Products (22)** View All

Product	Projects	Libraries	Vulnerable Libraries		Licenses
Struts	29	127	High: 8	Medium: 2	18
NewProj	5	24	High: 5	Medium: 4	14
CRM_Prod	4	81	High: 10	Medium: 1	19
KSA	3	42	High: 8	Medium: 1	8
Demo Product	2	328	High: 13	Medium: 13	31
My Product	2	36	High: 2	Medium: 3	9
Jenkins Test	2	10	No Vulnerabilities		1
ERP-1.0_Repo	1	318	High: 12	Medium: 13	29
ERP-1.0_Build	1	318	High: 12	Medium: 13	29
EUA_2019	1	39	High: 8	Medium: 1	9

**SecurityCenter** Dashboard Analysis Scans Reporting Assets Workflow Users

XenServer Status

XenServer - Audit Vulnerabilities by CoS3 Category

Category	Passed	Failed
Device Information	15	11
Application Information	1	0
Secure Configs	6	11
Vulnerability Assessments	1	0
Ports & Protocols	1	4
Plugins	2	0
Monitoring & Logs	2	1

XenServer - Compliance Summary

XenServer - IP Summary

IP Address	Score	Total	Vulnerabilities
192.168.1.81	219	47	31 5 11

**SAST Vulnerabilities Status**

Full Scan Results >

- 616 High (13 Solved)
- 834 Med (141 Solved)
- 2824 Low (1582 Solved)

**SAST progress status**

Previous Solved Recurrent

616 834 2824

13 141 1582

© 2016 Checkmarx

**Open So**

1 No Known Vulnerabilities

1 Vulnerable & Outdated

Total 2 Libraries

View Analysis Results >

**OWASP Top 10 - Web Informational Vulnerabilities**

Plugin ID	Name	Family	Severity	Total
1442	Web Server Detection	Web Servers (Passive)	Info	3711
1724	Microsoft IIS Server Detection	Web Servers (Passive)	Info	406
10107	HTTP Server Type and Version	Web Servers	Info	238
24280	HyperText Transfer Protocol (HTTP) Information	Web Servers	Info	234
4667	Persistent Cookie Utilization	Web Servers (Passive)	Info	214

**OWASP Top 10 - Web App Result Indicator**

Injection	Overflow
SQL	Error Handling
CGI Generic	XSS
High Web Vuls	Critical Web Vuls

**OWASP Top 10 - Web Events**

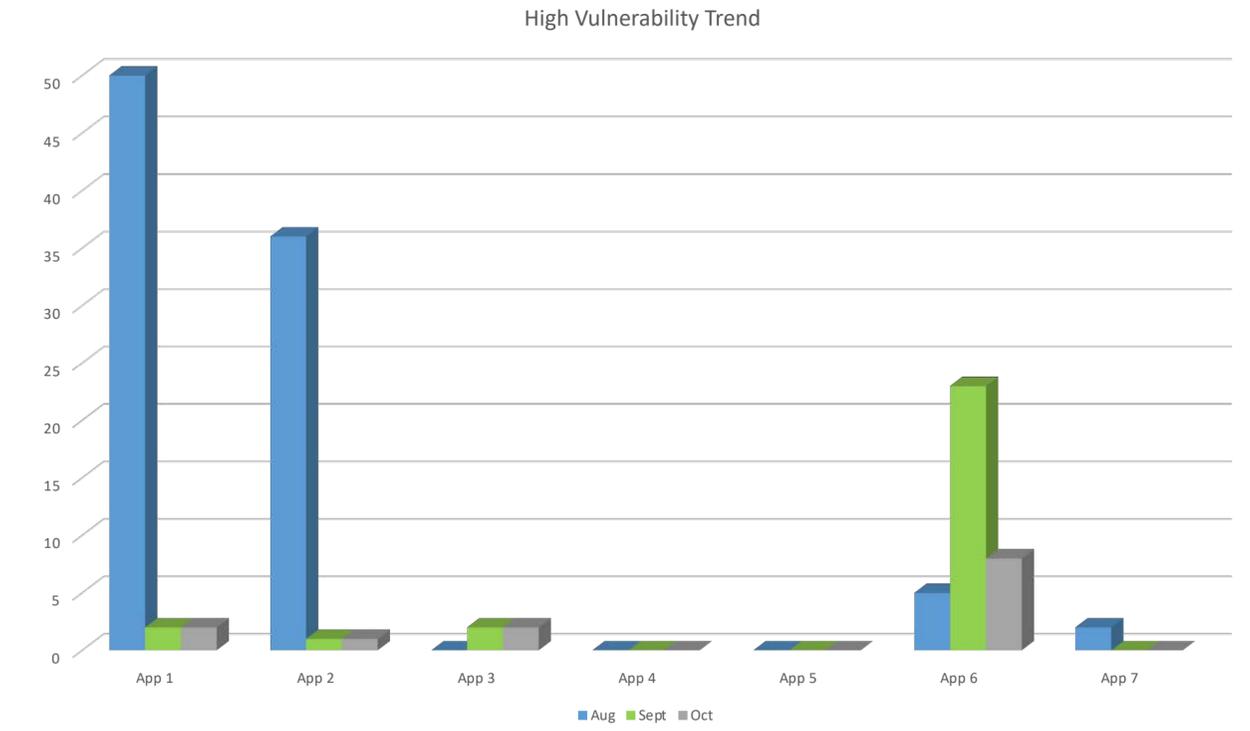
Web Intrusion	Web Threatlist
Web Stats	Long Term Web Error Activity
NMM Detected Web Error	NMM Detected Web Access
Apache Web Error	Apache Web Access
IIS Web Error	IIS Web Access

**OWASP Top 10 - SQL Events and Vulnerabilities**

Suspicious SQL User Database Dump	Suspicious SQL Command Detection
SQL Injection Vulnerability Detected	Suspicious SQL Query Detected
SQL Intrusion	Database Stats
SQL Error	SQL Login Failure

# Program Results

Vulnerability Level	Aug	Sept
High	93	05
Medium	221	141
Top Fixes	<p>Overall 94% Reduction</p> <p>Overall 46% Reduction</p>	



2<sup>nd</sup> Level SQL Injection

**19**

Stored Cross Site Scripting

**15**

Dead Code

**46**

Not Exploitable

**15**

# Customer Journey – Cloud Security Assessments

Initial Assessment

Unknown Security Posture

Initial Call

Size of Assessment

Base Assessment, Cloud Assessment Walkthrough

**Bronze**

Service Tier

**Silver/Gold/Plat**

**Silver/Gold/Plat**

**Bronze**

Assessment & Sizing

Agree On toolset

Recommend Service Days

**Silver/Gold/Plat**

**MSSP**

**AD-HOC**

Agree on services to be secured

Onboard Client on the security analysis Platform

Agree on the remediation (project work)

**Managed Services**

# Our Other Services

We believe in an all rounded set of services built on the need of our clients over the years and recognized by the Cloud Security Alliance.

What differentiates our company from other consultancies is that we do what we love and are customer focused.

Our company goes the extra mile in order to deliver solutions that are fit for purpose, effective and cost-effective for your organization's risks appetite.

We offer a range of products within cybersecurity.



**VCISO/INTERIM CISO**



**CYBER SECURITY STRATEGY**



**CYBER SECURITY CONSULTANCY**



**CLOUD SECURITY**



**TRAINING/COACHING & EDUCATION**



**APPSEC/DEVSECOPS CONSULTANCY**

# Contacts

# NSC42

WHEN YOU ARE CYBERSAFE WE ARE CYBERHAPPY

**Thank you**  
**Get in touch:**



<https://www.linkedin.com/company/nsc42-limited>



[Communications@nsc42.co.uk](mailto:Communications@nsc42.co.uk)



[www.nsc42.co.uk](http://www.nsc42.co.uk)

