TransUnion

DevSecOps

The journey to secure business agility

APRIL 2021

In a world that moves at pace, everything in that world moves at varied pace regardless if we embrace it or not.

Porters five forces of competition relating to operating markets, highlights what an organisation should keep an eye on:

- Threat of new entrants, Supplier Bargaining power, Competition, Substitution and Customer bargaining power.

Organisations have always had to have a element of being proactive and when necessary reactive to market forces.

Agility in delivery team, security and sales agility and the combination as a whole are key factors to being proactive and / or reactive at pace to the movement in which markets change.

From the first inception of an agile approach,

“*the halving of waterfall by using V-model’s doing it earlier*”,

“*the more modern day Disciplined, Scaled and / or simply SCRUM agile approaches*”,

Doing it early or the modern world, shifting left is a fundamental ingredient of business agility.

Moving from an agile DevOps culture to an agile DevSecOps culture has some challenges where its a welcome ingredient to overall business agility.

Here is narrative of one said journey.

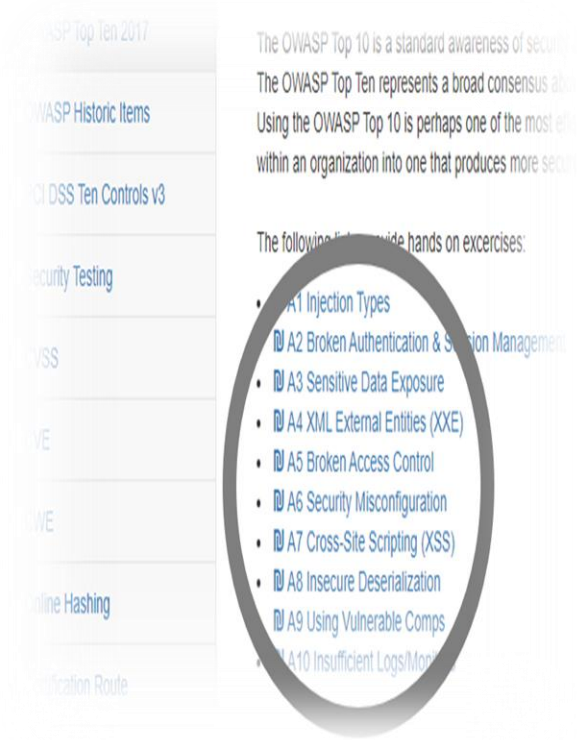
The organisation already has cloud, data centers, virtualized servers, software driven networks and so on…

Security requirements are captured through Epic's / Stories for products and services which teams deliver.

In the Epic / Stories monitoring is defined to capturing information that may help prevent a security incident using a Security Information Event Management System (SIEM).

The delivery teams are using Static Application Security Test Tools (SAST) in there CI/CD pipelines.

Vulnerabilities are fixed before releasing into test or production environments.



Penetration testing is carried out by the organisations trusted third party who do a good job.

All the evidence is captured and signed off by senior management.

External auditors for ISO 27001, SOX , PCI DSS sign off, the organisation is passing the requires security checks.

But hold on is there not a glaring gap in the delivery mechanism?

The gap, the point at which SAST skips straight into Penetration testing where vulnerabilities like bugs could exist in production environments.

A rallying shout out of “DevSecOps will solve the problem” is heard.

What we have to understand is using programming code to automate any process including testing, dynamic (DAST) / interactive (IAST) application security testing there are four key components:

- Action - the steps taken to get …
- Reaction - from solution …
- A set of expected results …
- A comparison of reaction to expected results giving a reported outcome …

Like DevOps we want to automate as much of DAST / IAST as possible when we go to DevSecOps.

We also have a need to fit the additional security objectives into using the same delivery teams without affecting delivery schedules.

What can we do there seems to be major effort, upskilling and cost involved?

At this point a lot relies on leadership and the ability to get stakeholder buy-in.

Try and find someone with the relevant skills within the delivery teams who has the passion / drive to deliver internal training to a level that allows Dev SecOps to happen.

Work with your security team / officer to define the scope of DAST / IAST within the delivery teams.

Keep in mind you will still want to use your third party penetration testers for BAU penetration testing.

Scope which types of controls you want to test for, OWASP Top Ten, PCI DSS Top Ten , SANs Top Twenty Five or combinations.

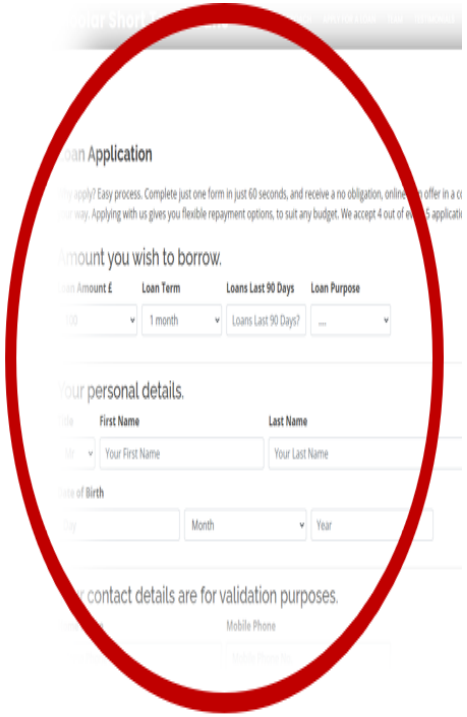
The training application is either find one which may have what you want at significant cost or build one.

It’s a minefield when looking at training applications that provide hand-ons training and meet the organisations needs.

Given delivery teams have expertise in automation, train delivery teams to do security testing manually so they understand what and how to test.

This will then naturally drive tests to be automated (DAST / IAST) given the teams expertise.

Time for a quick demo of a training application…



The training is complete, delivery teams adopt adding DAST / IAST to there automation frameworks. DAST / IAST is now incorporated into CI/CD pipelines.

Over time vulnerabilities are fixed in a layered approach much in the way application bugs are handed.

Visibility of residual vulnerabilities allows the third party penetration testers to target application adding additional value and further reduce risk.

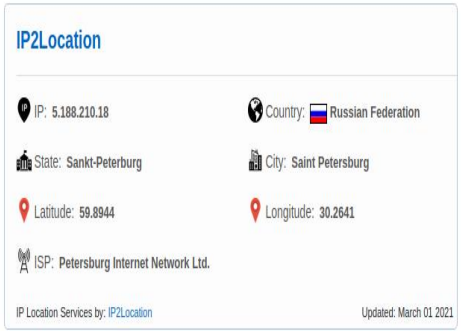
The organisations has reduced it security risk profile and strengthened its overarching security posture.

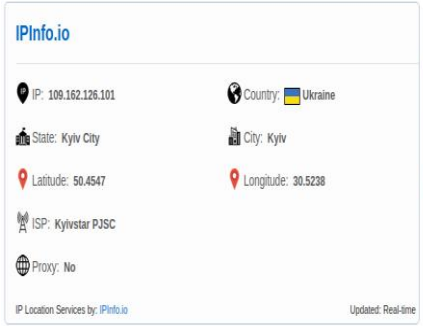
As the pub landlord would say “Job done game over.”

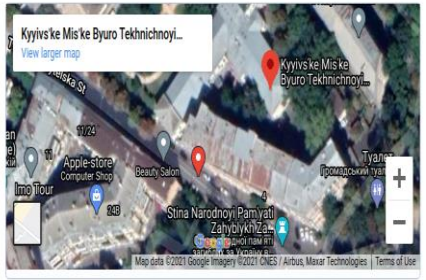
Very much the opposite, the journey of protecting products and services is as continuous one of offensive and defensive measures to counter the threat of attack.

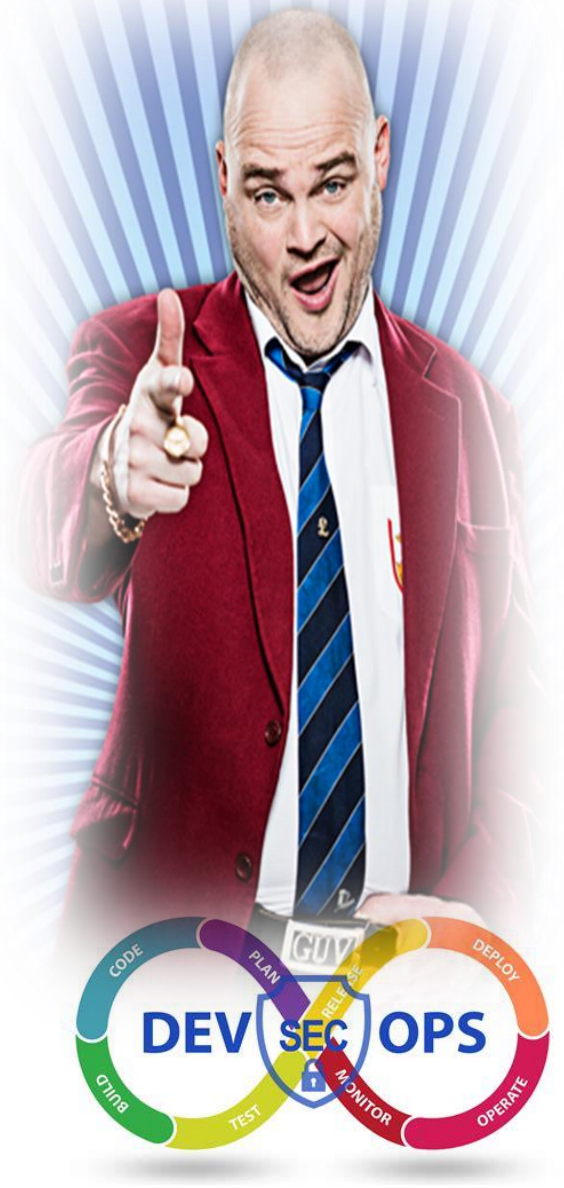
Real World Honey Pot capture traced to Russia and the Ukriane.

id	nameentry	bere	emailentry	cribe	nmsen	textareaentry	assessment	date	ipaddress
77	PetrHog		petrosom11@rambler.ru		Эло...	Лекарстве...	hacking event	Frid...	109.162.126.101
78	zaorAdaws		menhandbop1386@mix-mail.online...		стр...	<a ...	hacking event	Frid...	5.188.210.18
79	Damianbeack		2ewgaig6u1b1@gmail.com		Tell ...	Guys just ...	hacking event	Sun...	46.8.34.33









DevSecOps and continuous improvement go hand in hand.

In ending the presentation here are a few key continuous improvement tips:

- Be proactive and vigilant…
- Learn from reported security events…
- Never settle for the pub landlords “Job done game over.”…
- Measure improvement and socialise the success…