SOGETILABS

THE 4 FOCUS AREAS OF DEVSECOPS

DevOps will make systems more secure. In opposite to what many think, adopting DevOps, with its fast release cadence, will result in hardened systems which are fully compliant with security guidelines and which can stand the modern hackers.

SUMMARY.

Teams must follow, must inject, secure guidelines and practices in their way of working. This way of working needs to be highly automated, supported by machine learning and role playing.

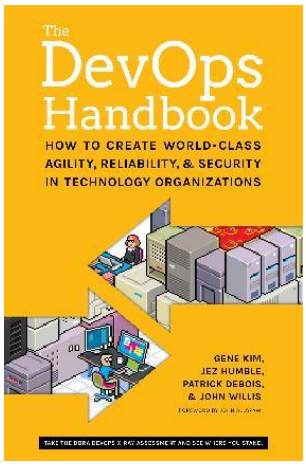
Fast, flexible, innovative, cheap, compliant and secure are the common requirements the business has on systems. In the past these requirements where a tradeoff from each other. Fast, flexible and innovative never went hand in hand with compliant and secure. With the current set of development practices, tool and platform capabilities these tradeoffs are gone, teams which follow a Secure DevOps way of working (DevSecOps) will deliver and run secure systems.

For a secure system DevOps teams and the connected business need to focus on the areas of:

Automation, Machine learning, Platform and Culture.

Automation will help on fast reliable and repeatable provisioning and validation of systems. Machine learning is the new kid on the block and will help analyze and understand the behavior of the system. Platforms are appearing in many flavors with many capabilities, many already with security baked in. Culture eats automation, platform capabilities and machine learning for breakfast, without the proper mindset of the whole company all the countermeasures won't help a thing.

As the DevOps Handbook mentions in chapter 22:



The bad guys are already delivering malicious code continuously. Security can respond faster by working within the DevOps patterns.

The DevOps paradigm shift may give security pros the opportunity to finally bake security into IT processes rather than add it on as an afterthought.

AUTOMATION

When the whole team and business is comfortable to release as often as they want, multiple times a day whenever a feature or patch is ready, will make a system more secure.

*Opinions expressed in this paper reflect the author's views and not the position of the Sogeti Group

Automation is key to make a team capable of releasing as often as they want. Automate the provisioning of the system from start to finish with validation between every step. Automation will give the team the ability to quickly push a security patch when a breach is detected.

Too often companies are in the news about system hacks via unpatched breaches. For example the Equifax Breach where the hackers used a vulnerability, Apache Struts CVE-2017-5638, that was found months before.

Equifax said that it was aware of the vulnerability two months earlier and worked to patch the bug then. https://www.nytimes.com/2017/09/14/business/equifax-hack-what-we-know.html

Automated provisioning is one part of the game, validating the work is the other part. Every activity executed during the creation and provision process of a system requires validation.

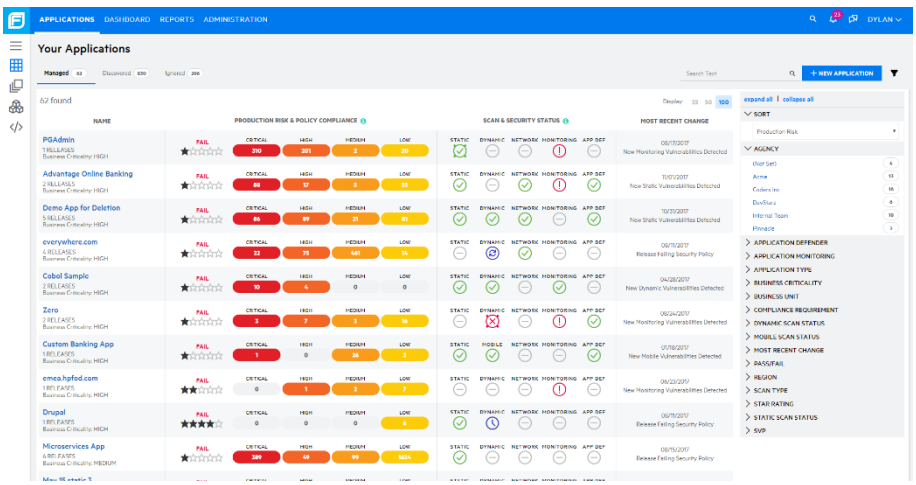
Coding activities requires unit testing with a good coverage, executed every time during the build. Not only the handmade code needs to be validated also the used packages. Packages and framework components are almost all opensource. Knowing if these opensource components have vulnerabilities requires specific tools which scan the used package every time the automated build runs. Sonatype, Whitesource, Flexera and other tool vendors offers these capabilities.

The golden rule of automation that every used artifact should be under version control doesn't count for secrets. Secrets never ever should be stored in a Git repository, even if they are development and test secrets, still they easily can be used to track the path to the production environment. An example is explained in this blogpost.

The GitHub extension that ships with Visual Studio 2015 exposed my source code to a public repository which allowed Bitcoin miners to spend $6,500 on my AWS account. https://www.humankode.com/security/how-a-bug-in-visual-studio-2015-exposed-my-source-code-on-github-and-cost-me-6500-in-a-few-hours

Nowadays there are tools and build steps that can be executed every build run which validates if the code has secrets of any kind. An example is the free CredScan from Microsoft

Automated vulnerability scanning is an important part and a benefit DevOps brings to system development next to automated provisioning. OWASP Zed Attack Proxy Project and Micro focus Fortify are vulnerability scanners which must be integrated in the automated release pipeline of systems.



*Opinions expressed in this paper reflect the author's views and not the position of the Sogeti Group

Automation is often the main DevSecOps focus area. The fast delivery next to the automated validation helps secure systems. Automation is also the area where many tool vendors are entering the DevSecOps market, helping mature this area for teams.

MACHINE LEARNING

Knowing the default behavior of the system is a must to know when it is hacked and behaves different. Too often companies don't know they are hacked and only face it when their data is set public. Even hackers are missing they are hacked.

It's the summer of 2014. A hacker from the Dutch intelligence agency AIVD has penetrated the computer network of a university building next to the Red Square in Moscow, oblivious to the implications. One year later, from the AIVD headquarters in Zoetermeer, he and his colleagues witness Russian hackers launching an attack on the Democratic Party in the United States. https://www.volkskrant.nl/tech/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~a4561913/

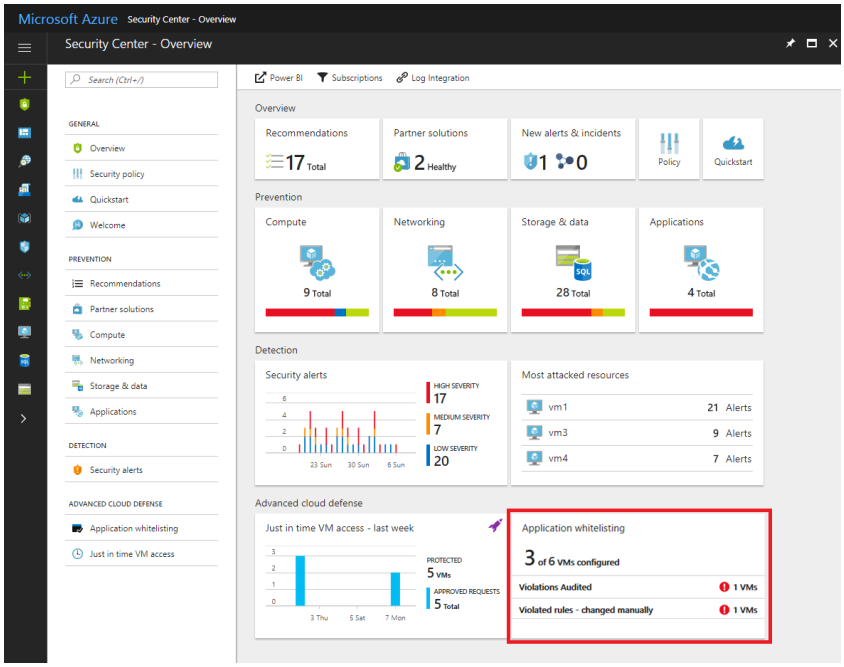
Capturing log data, monitoring the whole system, its components and business functionality is a starting point. There are great log tools available which can monitor from traditional systems till large services-based systems and everything in between.

The log capturing, and visualization tools are expanding their capabilities with Machine Learning, with a reason. The huge number of small chunks of log data are a rich set of information. With Machine learning applied on this set of data systems can get more secure.

For cloud providers it is already a common capability in their products. Microsoft which positions his Azure Cloud offering as the Intelligent Cloud, has machine learning in many offerings. For example, Azure Active Directory Identity protection uses it to identify compromised identities:

Discovering compromised identities is no easy task. Identity Protection uses adaptive machine learning algorithms and heuristics to detect anomalies and risk events that may indicate that an identity has been compromised.https://blog.route443.eu/2016/03/10/azure-active-directory-identity-protection-2/

Azure Security Center uses machine learning to understand the behavior of the applications in your subscription to understand if they are candidates for hacks.



https://azure.microsoft.com/en-us/blog/how-azure-security-center-uses-machine-learning-to-enable-adaptive-application-control/

Making systems for monitoring, configuring the environment for monitoring and creating the machine learning algorithms to secure the system are a main task of DevOps teams and shouldn't be an afterthought.

Connecting machine learning techniques to automation for self-healing (self-defending) systems when an attack takes place is a near future scenario, we're not there yet. It won't be good when an algorithm mistake results in system failures, like with automatic stock trading systems where an algorithm mistake results in spontaneous price drop.

PLATFORM CAPABILITIES

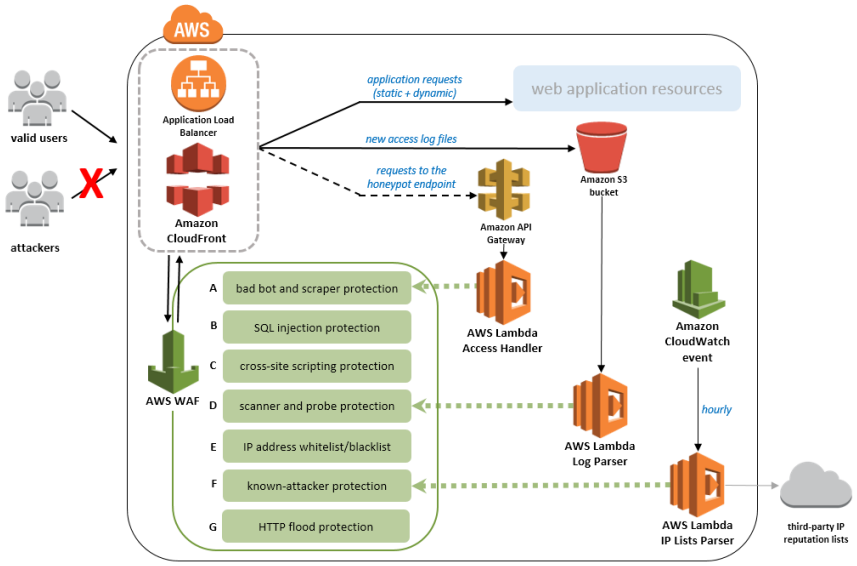
A platform comes in many forms. When talking Cloud, the platform exists of IaaS, containers, PaaS, Serverless and SaaS. Each platform has different features and capabilities which makes the platform valuable for business systems. Also, every platform flavor has its specific security characteristics and needs for protection.

From a security perspective IaaS surrounded with traditional networks for security can be of a good security level. There is a lot of experiences how to configure this kind of environments. Compared with cloud native systems like PaaS and Serverless where 'no network' is the default.

Cloud native systems require a different kind of security via authentication, encryption and other technologies. For example, when making the connection between an Azure WebApp and a SQL PaaS database a connecting string with username and password over https isn't enough. This communication can better be secured via Azure Active Directory authentication or with certificates and an Azure KeyVault. It is more secure but also require more effort to accomplish, the platform requires it.

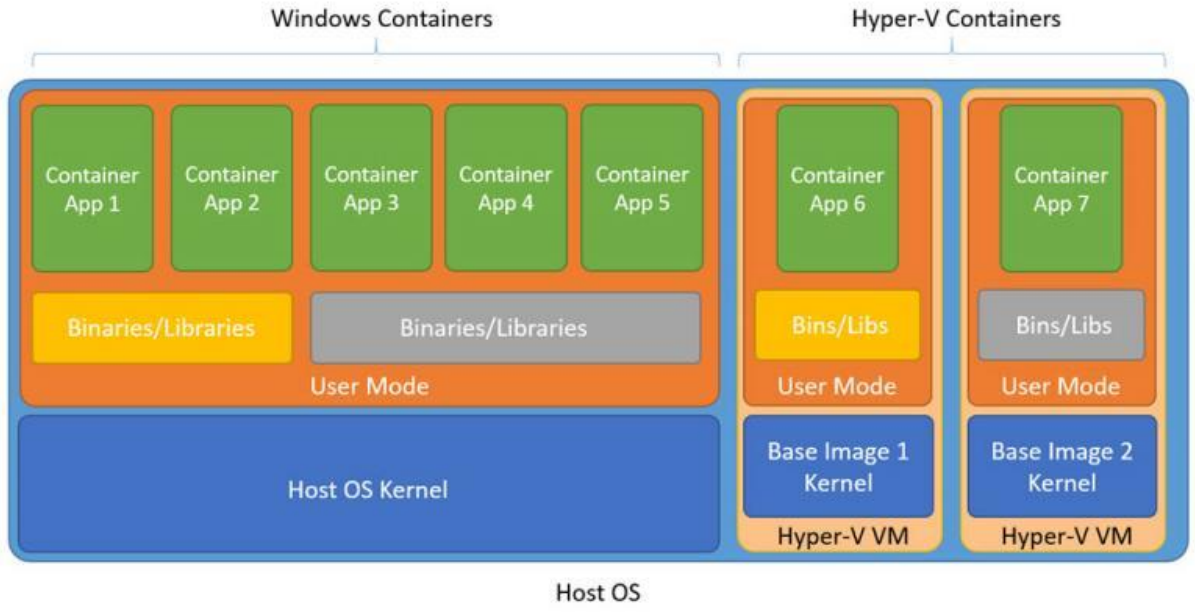
*Opinions expressed in this paper reflect the author's views and not the position of the Sogeti Group

Platforms also offers capabilities easy to configure and which makes use of the experience of the platform provider to protect the platform.



AWS WAF rules configuration is a set of default capabilities to protected web applications against attacks to exploit a vulnerability, take control of a server or DDOS attacks.

Other platform types like container technology also have their own tradeoff with security. Containers are easy shareable over different stages, by sharing the hypervisor of the container host. The smaller the container size the easier to distribute, while memory overloads can cause data to be leaked to other instances. Windows Hyper-V container have their kernel level isolation which solves this security problem, the tradeoff is that the containers are significantly bigger.

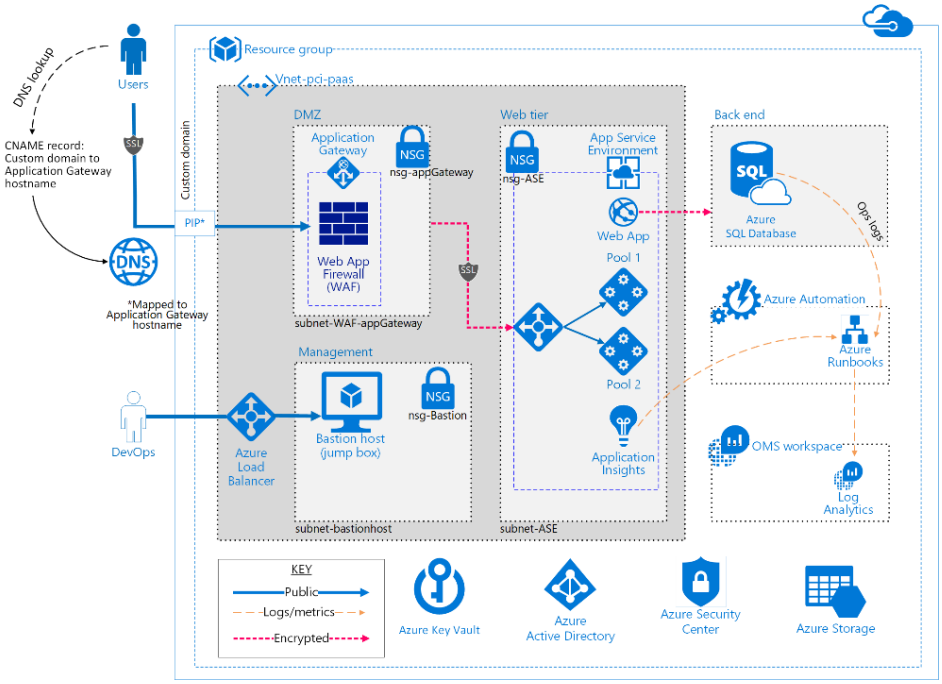


Companies adopting platforms need to think about these tradeoffs when selecting the platform for their infrastructure, on-premise or in the Cloud.

*Opinions expressed in this paper reflect the author's views and not the position of the Sogeti Group

THE COMPLIANT PLATFORM.

To make the selected Cloud platform compliant with regulations, this platform needs to be configured, and consume resource from the platform in a specific way. For example, Microsoft has built several reference architectures on Azure for specific compliances.



Azure Blueprint Automation: Financial Services Blueprint for Regulated Workloads.

CLOUD COE AND THE SERVICE CATALOG.

Companies will need such a compliant platform on top of the cloud platform with additional capabilities and configuration to be compliant to the company security rules. The Cloud Center of Excellence (or any other name) will be set in place for business units to maximize the usages and speed on delivering business value by using the cloud while staying compliant.

"A Cloud Center of Excellence (CCoE) is a cross-functional team of people responsible for developing and managing the cloud strategy, governance, and best practices that the rest of the organization can leverage to transform the business using the cloud. The CCoE leads the organization as a whole in cloud adoption, migration, and operations. It may also be called a Cloud Competency Center, Cloud Capability Center, or Cloud Knowledge Center. " — https://cloudcheckr.com/document/cloud-management-report/

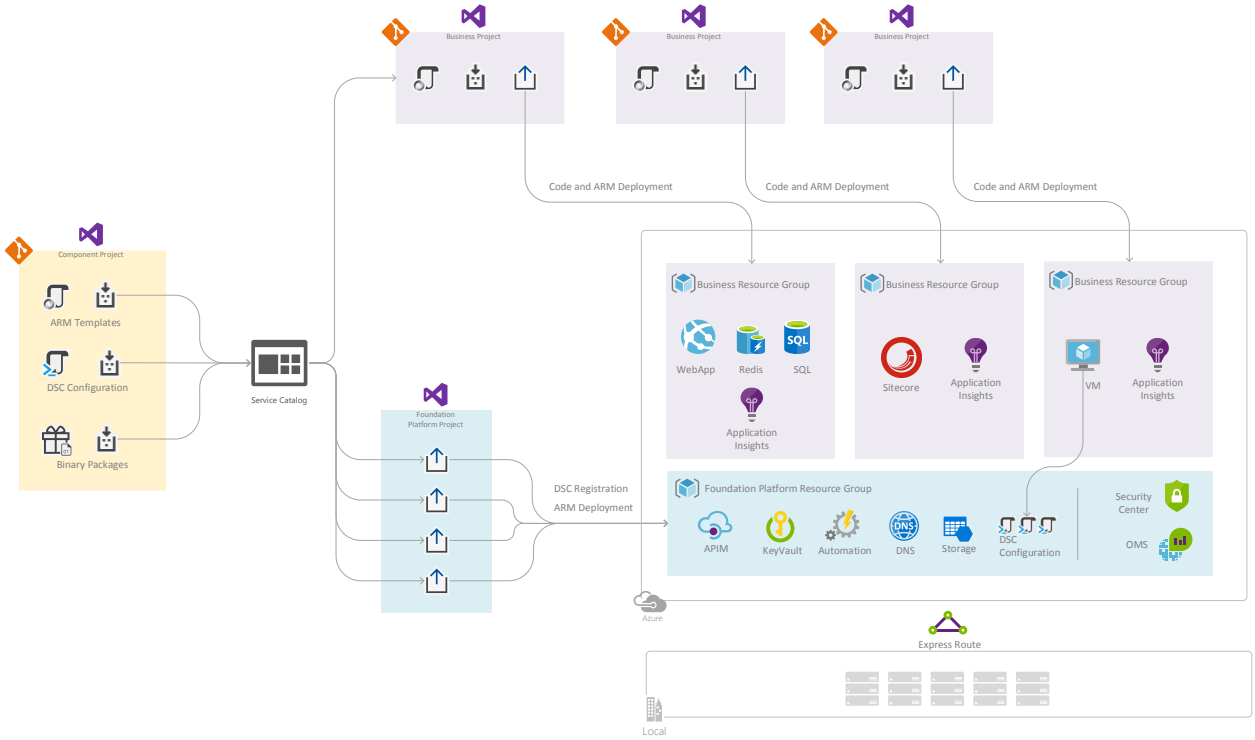
Cloud technology adoption combined with a focus on value delivery and feedback will bring the goal of a flexible, cheap, innovative and secure business closer. The combination of these two are a catalysator for change.

The Cloud CoE is a service and practice center with deep and width knowledge on cloud platforms, design, delivery and run of cloud systems. The breadth and combination of development and operational knowledge makes the Cloud CoE an accelerator for businesses innovation.

Automation, templates, practices, solutions and services supports organizations in the adoption of cloud. The Cloud CoE must make an Service Catalog available for business units with these artifacts.

*Opinions expressed in this paper reflect the author's views and not the position of the Sogeti Group

An implementation of a Service Catalog, Platform and Business projects are in the image below. In yellow the Service Catalog team with artifacts ready for use by the business teams (purple) and the platform team (blue) which uses the same service catalog artifacts to build and release the compliant platform.



With the out of the box ready solutions and automation scripts in the Service Catalog, teams can start to focus on business functionality immediately. Setup and organizational practices will make sure systems are ready for operations with the feedback loop back to the business ready to use.

AWS has a Service Catalog service which tracks the lifecycle of the products in the service catalog and provides access to the catalog.

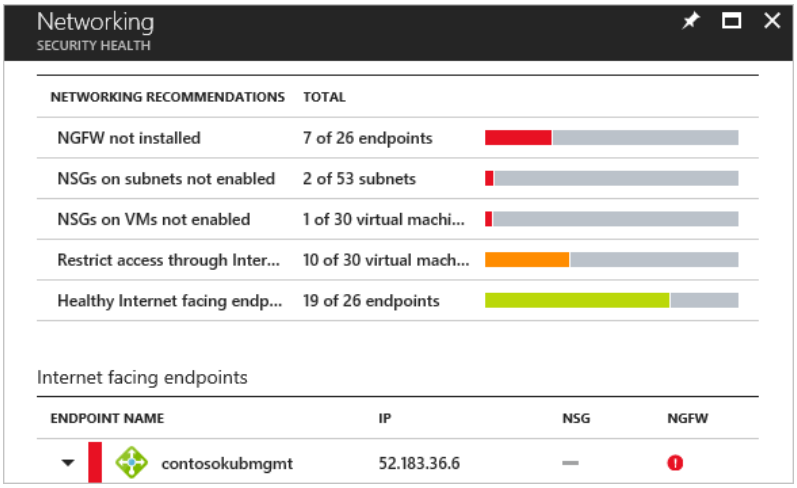
CONTINUOUS PLATFORM COMPLIANCY.

Monitoring the platform, the service catalog and the business projects during their lifecycle on compliancy on security frameworks such as NIST, CIS/SANS 20 or ISO 27001 is a daunting task.

Cloud platforms are taking care that they are compliant on many frameworks, making it possible to inherit some of the compliance to the business projects, service catalog and company platform. Still continuous monitoring is required.

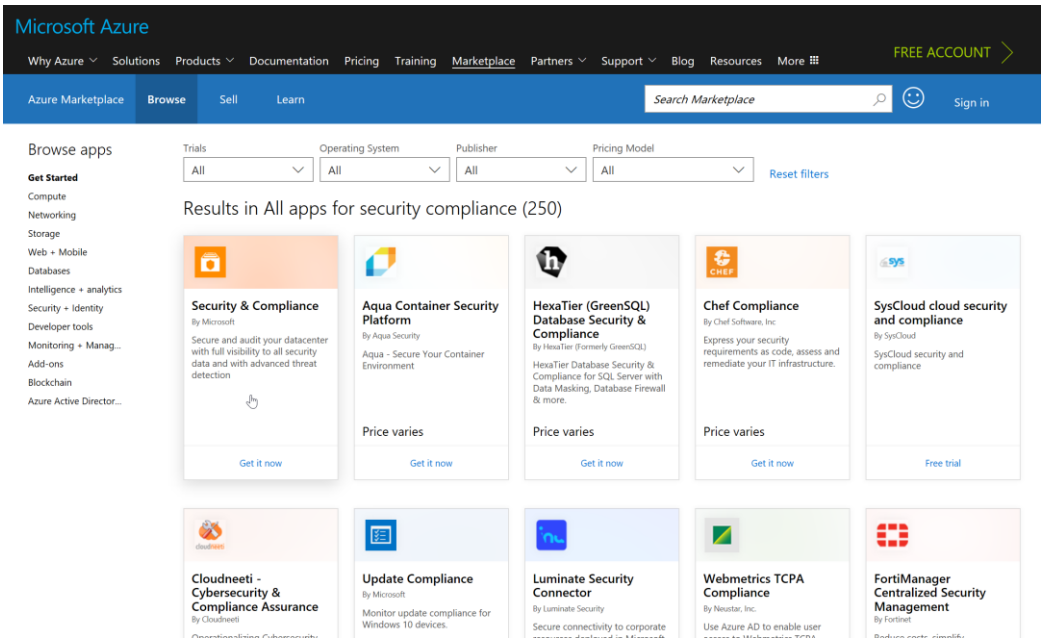
Azure Security Center monitors the platform continuous on threats and vulnerabilities. Policies can be configured to ensure compliancy with security frameworks.

*Opinions expressed in this paper reflect the author's views and not the position of the Sogeti Group



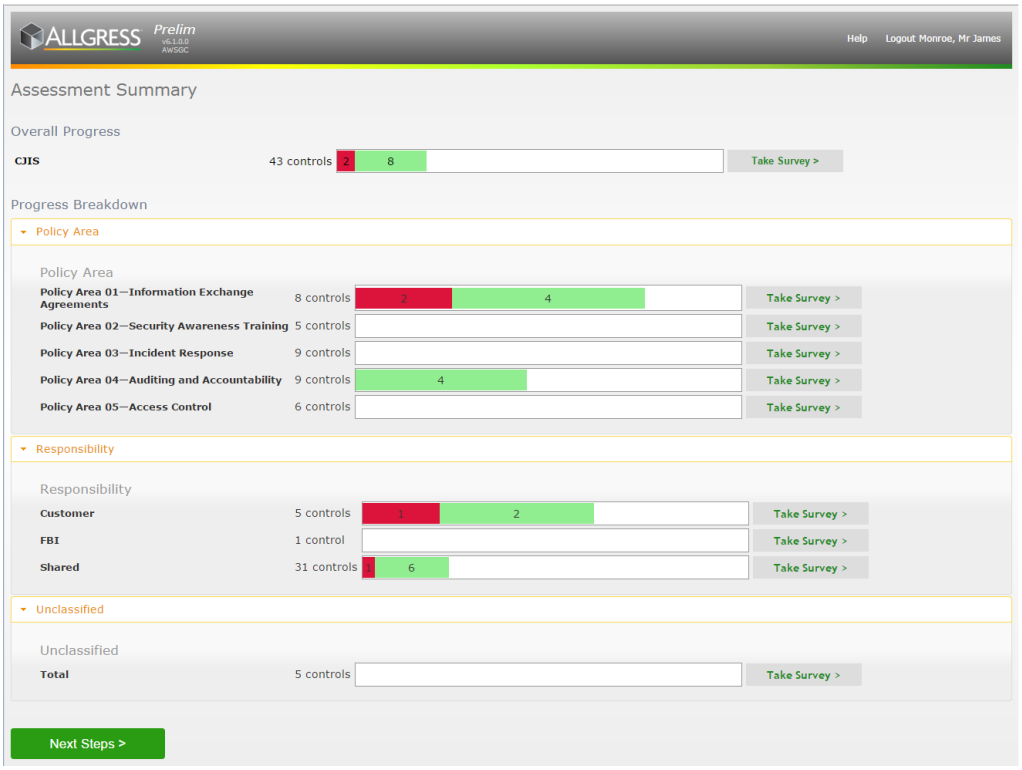
Multiple vendors are offering additional capabilities on top of these security policies with auditing and compliancy management. In the platform marketplaces these offerings can be found.

Azure Marketplace on Security and Compliance:



AWS partnering with Allgress https://aws.amazon.com/config/partners/allgress/

*Opinions expressed in this paper reflect the author's views and not the position of the Sogeti Group



Platforms and tools help to stay compliant with security frameworks, they are supportive and reduce the complexity to be compliant.

CULTURE

Just opt-in for a cloud subscription, automated the delivery, setup the compliant platform configuration and learn from the system behavior isn't enough for a secure platform. Getting a real secure environment requires a combined mindset from all the organization, its people, its processes, the whole cultural mindset of the organization should be secure. Cloud technologies with a DevOps way of working offer powerful capabilities to make business systems secure. But, to get the most out of these efforts a clear and structured secure way of working is required.

The question "*What is the weakest point in my organization?*" results in interesting answers. From admin passwords on shares and production data for test runs on less secure environments till old habits.

Having the whole organization focusing on security is challenging, there are many roadblocks. Secure DevOps Practices like automation, feedback loops from operations will help teams to clear many of these barriers, but there are more practices to adopt.

We believe that boards and senior business leaders should be asking the technology team a different question—namely, "Are we ready to respond to a cyberattack?" *https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/playing-war-games-to-prepare-for-a-cyberattack*

Cyber Security War Games is a practice companies are starting to adopt. One team tries to hack the system and the other team reacts to it.

*Opinions expressed in this paper reflect the author's views and not the position of the Sogeti Group

These games have a twofold benefit, they train teams in fast responding to intrusions. The alerts, log information will be added, and Machine Learning algorithms will be tuned to make the team more responsive to hacks. The other benefit is obvious, finding holes internally before the bad guys do.

An exercise which makes the whole company secure aware, is to do an internal phishing exercise and publish the shocking results.

CLOSING

Security should be baked in the whole company. DevSecOps with practices like automation, machine learning, platform and culture should be adopted by the whole organization. Still be aware hackers move fast, they think different. Be as fast as the hackers, know when you are hacked and responsive to these hacks will make you win the security war. Because:

You just have to accept it. The hackers are going to get in. The question is, what are you going to do once they are in? *http://www.trustedsoftwarealliance.com/2016/03/10/security-war-games-with-sam-guckenheimer-at-rugged-devops-rsac-2016/*