Vince's 3 i's of Monitoring in the Cloud

Cloud Security Posture Management (CSPM) is a popular topic of conversation. Go to any event or expo and you'll see the growing number of solutions, and with organisations moving to the cloud at a staggering rate, this is set to continue. If you need a CSPM … and you do need a CSPM solution if you are in the cloud, not all the tools you see may match your needs. For me, when considering a CSPM solution I have a number of requirements. 47 to be exact. Here, we are going to talk about 3 of the most important.

## Inventory

Simple things first … you can't protect what you can't see, so inventory is hugely important to Cyber Security. Typical on premise, agent-based solutions can only guarantee to report on assets that are able to make contact. However, the tooling could never be held responsible for assets that were poorly configured or failed to register with the platform.

Having been faced with the issue of unknown unknowns in the past, I had to create an application to combine data from numerous, agent-based systems to allow me to identify gaps in our coverage.

Now, with so many organisations moving to the cloud at speed, these issues will only intensify, especially when you include the potential need for multiple Cloud Service Providers (CSPs).

So, it is imperative to know what you have to protect, but if we are using cloud correctly, we start to move away from the traditional VM-based estate. If you ever talk to me about cloud I quickly start ranting about the benefits of the cloud and the new abilities it gives us. No longer are we tied to building and configuring VMs. Applications can now be built using cloud native resources such as serverless functions, blob storage, and other managed services. So, now we must think about the health of these new types of resources, some of which, due to the ephemeral nature of the cloud, may only live for short periods of time.

## Intelligence

Next is intelligence. You cannot use the internet without hearing reports of new vulnerabilities, zero-days, and breaches. Whether it's organised crime, nation states, or script kiddies, threat actors are constantly knocking on our door trying to find the smallest crack in our defences.

Attack vectors are constantly evolving and we, as cyber professionals, need to keep up-to-date with the ever-changing landscape.

The global pandemic changed many things, and cyber security activities were no exception. Historically time-to-exploit of a new vulnerability was months. More recently I've seen this come down to weeks or even days.

Vulnerability data sources are freely available, from NVD, to GCHQ, and even security vendors reporting the findings of their own research. However, collecting, triaging, and interpreting all this information can be very time consuming and overwhelming. But, I can't understate the importance of data. Having this information allows us to identify the issues in our estate by being pro-active in our response and minimising our risks.

## Insights

Finally, insights. Risks without context are meaningless. If you remember only one thing from this presentation … risks without context are meaningless!

All CSPs provide the ability to view known vulnerabilities associated with a resource, however this normally highlights issues in isolation. CSPs also allow you to compare your assets against defined policies, but again this evaluation is on a resource-by-resource basis. Knowing that a VM is missing an OS patch and is outside policy is useful, but how serious an issue is it …. Really.

What we need is to be able to look at the bigger picture, not quite the 35,000 feet view, but certainly something larger than individual assets. Being able to view issues on assets and see how those assets are related to other resources across our resource group or subscription is hugely important.

If we follow basic cloud security we will have applied layers of protection, but the constant stream of new vulnerabilities and exploits means we must continuously evaluate the potential impact of a successful attack. Data sources, again can help, but the advice provided is not tailored to our environment, assets, or configurations.

Understanding a vulnerability within the context of our environment can quickly elevate the severity of an issue and demand a response to avoid exploitation.

An unpatched server may not raise an alarm, but let us play the "what if" game. A bit of threat modelling. What if the patch addresses an elevation of privilege vulnerability? And what if that server has a public IP address and open ports that expose it to the internet. And what if the server has poor SSH authentication and is connected to other servers within an application. Could a successful attacker start to move laterally through our estate?

Without context the possible risk and impact of vulnerabilities may never be realised.

## Summary

So as I mentioned, I actually have 47 requirements for a Cloud Security Posture Management solution, but these are a few of the ones I MUST have. I'd advise you to keep them in mind when considering a tool to monitor you cloud instance.