CAT-AND-MOUSE

Rani Osnat discusses *10 of the cloud security trends that organisations are likely to face in the continually evolving cyber security landscape*

As anyone involved with cyber security knows, it is a constant game of high stakes cat-and-mouse. Every year new attacks emerge, while new security solutions are created, and old security fixes are upgraded. Threat actors constantly append new methods to the old ones, using them as part of their ever-growing toolbox. With this in mind, below are some of the top trends organisations should expect to see over the next 12 months and beyond, in terms of new attack vectors in cloud native environments.

An increase in attacks that bypass agentless security solutions. Many organisations have been adopting agentless security models that utilise volume scanning to identify vulnerabilities and misconfigurations. Some have been using these solutions to detect threats in runtime as well. But agentless solutions don't detect certain attacks such as memory-resident malware. Threat actors are already using such evasion techniques in more than half of attacks, and are highly likely to continue this trend and append new techniques that bypass agentless solutions to their arsenal. Vendors will need to adopt supporting agent solutions in order to detect and block these runtime attacks going forward.

New severe vulnerabilities will be weaponised even faster. Recently, there's been an increase in the number of severe zero-day vulnerabilities. Some have been conducted through Remote Code Execution (RCE), including log4shell, Confluence, Zimbra and Zabbix among others. Over the past year, large botnets (such as Kinsing, Mirai, Dreambus, etc.) were able to quickly append these new vulnerabilities on top of their existing infrastructure, effectively both decreasing the time it takes to weaponise new zero days and increasing the reach of these new attacks. This trend is expected to not only continue, but even increase in the coming months. Consequently, vendors will face the challenge of rapidly updating threat intelligence feeds and solutions accordingly.

As threats to the software supply chain escalate, CISOs will be compelled to develop and deploy better strategies

Attackers shift left – a new generation of attacks. Attackers often invest significant time and resources to detect new vulnerabilities in applications and the infrastructure on which it runs. Meanwhile, security practitioners utilise a range of solutions in various locations throughout their development lifecycle to detect and mitigate vulnerabilities including source code management security solutions, container image scanning, CI/CD security tools and runtime controls. Simultaneously, threat actors are now aggressively innovating and adopting new or emerging technologies themselves. It's expected that these threat actors will adopt similar approaches to improve and even optimise their campaigns. Attackers will begin to leverage offensive security tools such as code scanning to detect security issues in a victim's code and development infrastructure, especially if they're developing open-source software.

More creative attempts to bypass eBPF-based solutions. Over the past couple of years, there's been discussions about the advantages of eBPF-based technology for runtime protection, leading to wider adoption of agent-based solution technology. We've seen methods that seek to bypass eBPF technology and believe threat actors will continue to look for more creative ways to circumvent these solutions and avoid detection. Strong up-to-date security research that analyses campaigns will soon be able to detect threats, update the agents and block such bypass attempts.

A darker side of BPF. With the expanding adoption of eBPF technology, there's been exponential growth in the use of BPF and eBPF malware in the wild. In particular, state-sponsored threat actors have been using this technology to bypass security solutions and avoid detection. In fact, several new eBPF based rootkits have emerged on GitHub as proofs of concept. Expect to see an increase in such publications over the coming months. As eBPF-based technology is further adopted, it can also help to detect these elusive threats. Additionally, threat actors will likely use these open-source proof of concept tools to launch attacks in the wild, requiring advanced security solutions that have the capability to detect them.

The skills gap will widen further. With most organisations now leveraging cloud native architectures for the bulk of their digital transformation initiatives, the lack of knowledgeable staff to support the growing number of production applications running on these platforms is widening. Although more and more operations and security resources are being trained (or cross-trained) in Kubernetes, CI/CD pipeline automation and Infrastructure as Code (IaC), it simply isn't keeping up.

As a result, in order to bring production ready resources on board faster, both time-to-hire and overall compensation to fill these positions is expected to increase by more than 15 percent in the next 12 months.

Providers of professional services will emerge as winners. One way organisations are likely to address the growing skills gap is by relying more on partner-delivered services. Procurement models are shifting, with many customers buying technology solutions directly through cloud providers. This is also an opportunity for resellers and distribution partners to get creative in the ways they bring value to customers.

THIS MARKET DEMANDS THAT WE STAY AHEAD OF ATTACKERS AND ANY NEW TECHNOLOGIES ADOPTED

Timing will align with the growing appetite from customers for managed solutions and those partners who have built strategic relationships with vendors to provide advisory and professional services will win market share. This will shake up the traditional channel model for security products, leading to greater consolidation and fewer partners doubling down on individual vendors. That said, following in the footsteps of firms like Fishtech and The Herjavec Group, it wouldn't be a surprise to see additional M&A events in this space in the coming months.

Consolidation of tools for multi-cloud and cross-business use cases. Another way to address the skills gap is by maximising productivity of existing resources. As organisations move from separate pockets of cloud native development within their various business units to an environment where the architecture team is defining cross-company tooling, the point solutions across different cloud stacks and dev teams will rationalise.

With economic constraints increasing over the next 12-18 months, there will be even more pressure for CISOs to quantify the value of their toolsets and increase ROI on their security spend. Moving forward we can expect to see a shift in demand towards solutions that offer a broad set of cloud native security capabilities – particularly those that can be embedded into developer workflows – and a greater focus on measuring and reporting on the value they provide. With companies typically managing more than 75 tools, organisations will reduce the number of separate products in use for cloud native application protection by more than 20 percent this year on average, putting pressure on smaller point product providers.

Extending DevOps with GitOps. Another current hot trend in cloud native deployments is taking DevOps principles and applying them to infrastructure with the primary approach being GitOps. If this isn't already gaining traction within your organisation's teams, it most certainly will be at

some point soon. GitOps use cases will span beyond continuous delivery (eg ArgoCD) to infrastructure, with the main tool being Crossplane. GitOps is making changes to any resource more observable through version control and thus, more secure.

We'll see more cloud native projects implementing GitOps tools such as Crossplane and ArgoCD, going from proof-of-concept use cases to large scale adoption across end-user companies. With GitOps becoming more mainstream, more resources are going to be defined as code in a structured way, allowing for higher scan coverage with security scanners.

SBOM will move front and centre. Shifting further left in the supply chain, the attention of

ATTACKERS WILL USE SECURITY TOOLS SUCH AS CODE SCANNING TO DETECT SECURITY ISSUES

nearly every CISO will be on the Software Bill of Materials, or SBOM, this year. New tools, languages, and frameworks that support rapid development at scale are being targeted by malicious actors who understand the catastrophic impact that attacks on the software supply chain can have. As threats to the software supply chain escalate, and with government regulations in the form of executive orders (EO 14028) mandating proper action to be taken, CISOs will be compelled to develop and deploy better strategies to secure this area of significant weakness. Going forward, expect to see fewer sophisticated attacks like SolarWinds and more attacks like those targeting Log4J, Spring4Shell, and OpenSSL which are widely used across code and production. These attacks will have a much larger potential blast radius, allowing hackers to impact (and potentially penetrate) many more organisations.

To demonstrate the level of commitment to the executive order, it is highly likely that several companies found to be out of compliance with the order will find themselves facing fines or lose business with the government. While simply generating SBOMs is already becoming easily accessible today, the processes and tools around handling, signing and managing SBOMs, as well as applications of SBOMs in different use cases, will become more sophisticated and prevalent.

With so much change in the world of cloud native security, the old saying: "May you live in interesting times" comes to mind. This market demands that we stay ahead of the attackers, the technologies being adopted and the cultural/organisational changes that come along with these changes.

While many of the key predictions above are troubling, the good news is that leading cybersecurity companies are not only monitoring growing trends, but they are constantly developing sophisticated new technology and tactics to help organisations everywhere stay one step ahead in the ongoing game of high stakes cat-and-mouse. Whether you're a senior executive, security researcher, engineer or practitioner, taking these forecasts into account will help you to formulate, procure and implement a cyber security programme that helps protect your employees, customers and stakeholders as effectively as possible throughout 2023 and beyond ●

Rani Osnat is SVP Strategy at Aqua Security

One way organisations are likely to address the growing skills gap is by relying more on partner-delivered services