Trends, challenges & evolution of security monitoring in the evolving digital landscape

Interview with **Adwait Joshi**, Director of Product Marketing for Azure Security, Microsoft

Society is becoming increasingly dependent on digitized processes and systems ([NCTV19]). This trend is also apparent within organizations. As the world continues on its digitization revolution, cybersecurity should be, if it isn't already, a core business requirement in order to protect critical business processes, assets and data from cyberattacks. And, unless your security monitoring strategy has been adapted in-line with this trend, there is a good chance that such capabilities are slowly eroding or becoming fragmented.

We spoke to Adwait Joshi, Director of Product Marketing for Azure Security, Microsoft, to discuss current trends and issues in the security monitoring space, potential solutions and what the future holds.

Jacqueline Morrison
is a senior specialist within the Cyber team at KPMG.
morrison.jacquleline@kpmg.nl

Jeroen de Wit
is a senior manager within KPMG Cyber
dewit.jeroen@kpmg.nl

INTRODUCTION

Research ([Harv19]) shows that forty-four percent of organizations are expecting fundamental changes in their business models driven by digital disruption. Business IT operating models are also changing rapidly especially with the adoption of Cloud services. As cyber threats continue to evolve, security monitoring and incident response have become a pivotal component of a modern cybersecurity program.

The traditional approach to security monitoring is often no longer practical or sufficient in today's multi-cloud world, compounded by an ever-increasing skills shortage ([Morg19]). Organizations are moving parts of their infrastructure to different cloud vendors, where there are different dedicated security monitoring solutions, which require their own flavor of tuning and monitoring. This results in fragmented and siloed security monitoring and does not allow for correlation across an organization's environment. In addition, extra resources must be utilized to learn different security monitoring technologies as well as monitor these dispersed technologies. The major resource shortage is exacerbated by repetitive manual tasks utilizing precious time that could be better spent on more complex tasks.

A likely reason for this could be that traditional on-premise SIEM solutions are not well positioned to facilitate the Cloud migration journey many organizations find themselves in.

In this interview, we will discuss solutions for the issues described, including the option to deploy a SIEM in the cloud and leveraging SOAR products that are exploding in popularity because they automate much of the manual repetitive work SOC analysts are normally tasked with.

"There is a lot to learn and there is a lot to protect"

INTERVIEW WITH ADWAIT JOSHI, MICROSOFT

KPMG: What changes are you seeing in the IT world and how does this affect the current state of security monitoring solutions?

Adwait: Organizations are embracing cloud and hybrid cloud strategies. That means a combination of public clouds and private clouds, which has increased the demands on data gathering. With that there are a few things to keep in mind:

- From a security perspective, there is a lot more that needs to be processed, monitored and analyzed;
- The attack surface is growing because of these hybrid strategies, multiple clouds, your existing on-premise data center, new IoT devices and new user mobility solutions. So, all in all, the devices, the infrastructure and the cloud infrastructure are adding complexity which increases the attack surface. This is something that CISOs need to consider in order to ensure that they have an integrated solution or full view of their enterprise.

With this growing digital space and digital footprint, specifically from a security monitoring perspective, organizations need to understand how they can get an integrated view, how they can have a consolidated solution that it will help give them a view across their entire enterprise.

This is the trend we see from an industry line perspective, everything is becoming more distributed, public cloud usage has increased and ultimately that is also driving organizations to use public cloud as a security platform as well. Gone are the days when people used to ask questions about public cloud and security associated with it. Now, CISOs have realized the advantages and benefits that a public cloud can offer, especially related to the scale and volume of data that can be processed, and the speed that can be used to help improve their own efficiencies for their security operations. And so we see public cloud being used as a security platform.

KPMG: What trends do you see in SIEM or SOAR technology?

Adwait: The challenges we see are all related to the trends that I mentioned earlier. These trends have to do with growing attack surfaces as data volume grows.

And so the challenges are:

1. The complexity to manage solutions and get a consolidated view across the enterprise is growing rapidly. Having traditional strategies of on-premise software solutions that are or are not connected and having individual point solutions for different clouds, CISOs

'Yesterday'

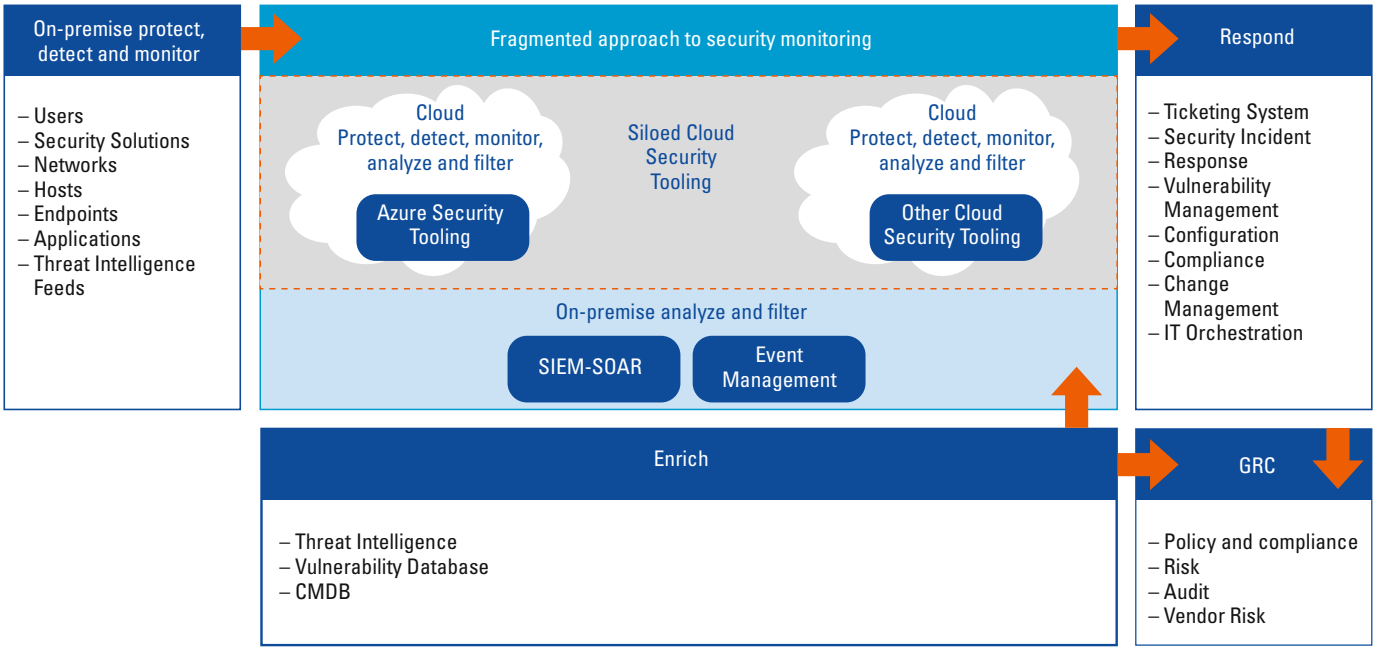

Figure 1. Yesterday's view of siloed security monitoring which does not allow for correlation across an organization's environment.

What is "SIEM"?
Primarily a detection mechanism, a Security Information & Event Management tool ingests events and data flows from multiple sources such as networking devices, endpoints, active directory and security tooling (e.g. EDR, IDS), as well as data to enrich events and alerts like asset databases and Threat Intelligence feeds. This data is then used to identify non-compliance, for example and real time security incidents such as an attacker performing malicious actions on a workstation.

What is "SOAR"?
A Security Orchestration Automation and Response tool enhances detection capabilities and contextualization of incidents, as well as accelerating incident response. Security Operations Analysts are often stretched resources and SOAR aims to relieve this by tactically enhancing and streamlining workflows where human interaction is not needed, freeing up valuable time to focus on tasks that require more critical thinking. For example, a typical phishing alert could take an analyst an average of 15 minutes to investigate. A SOAR tool could automatically analyze the email, place the attachment in a sandbox and return all of that information to the analyst for review.

Another strength of SOAR is that it allows integration of multi-vendor tooling which generally does not directly interface with each other, bringing them together in an automated way. Being able to work across a multi-vendor security tooling ecosystem is important for organizations to avoid single vendor dependence, and is also very valuable for MSSPs who work with different organization tool sets.

SIEM vs SOAR
A SIEM is focused on ingestion of data and detection mechanisms (finding the needle in the haystack), while SOAR is mostly focused on enriching the data and automating repeatable tasks related to the response of the incidents generated from the SIEM. While there are more and more standalone SOAR solutions, vendors are adding SOAR-like features to their SIEM, with some vendors launching solutions that fully encompass both SIEM and SOAR.

'Tomorrow'

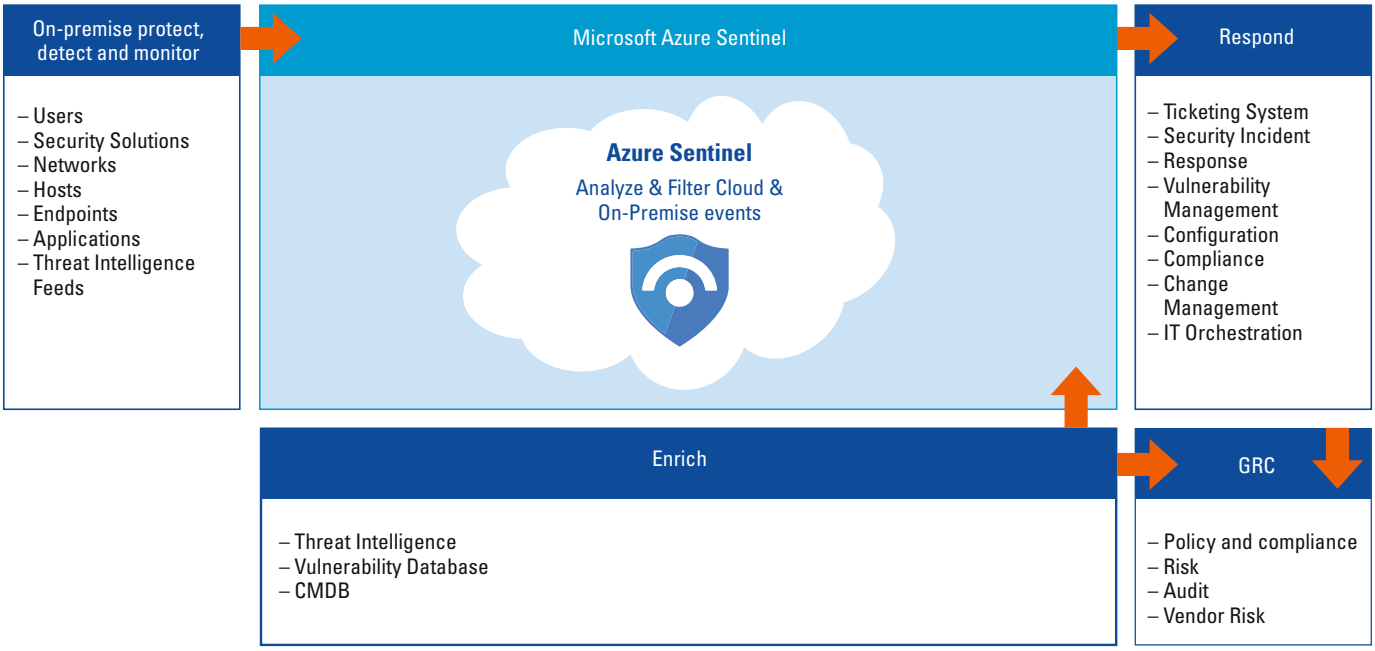

Figure 2. Tomorrow's view of security monitoring where visibility and correlation across an entire organization, including on-premise and multiple cloud environments, is possible.

are telling us that that is not working well, and it is costly to set up and maintain individual solutions.

2. Security analysts are inundated with the volume of alerts that they see. As a result, their efficiency is going down. They are not able to prioritize the threats because of false positives and large volumes of alerts. There are multiple reports that state that more than 40-50% of alerts are not processed because of the volume ([ESG20]). So how can we help improve that efficiency, how can we help empower SecOps team to quickly act and understand what is the high priority attack, high priority threat?
3. Lack of security expertise because there are so many different solutions and attack surfaces, there is a lot to learn and there is a lot to protect. On the other hand, we do not have enough security resources in the market. Reports show that by 2021 there will be 3-4 million roles for security ([Morg19]).

Going into more detail regarding the trends of SIEM and SOAR technology, we see that more and more cloud solutions/technologies are being embraced because of the data requirements. Most vendors are now migrating their solutions to the cloud because of these requirements. For Microsoft, it was natural from the beginning to design a cloud native solution with Azure Sentinel. We decided to build it completely in the Azure platform and that gives us the ability to process data quickly without our customers having to think about how to scale their infrastructure or how to set up and maintain their infrastructure. We see that even traditional vendors are now offering some cloud services.

Furthermore, we see more and more usage of machine learning. We have built-in machine learning models that are trained in observing data that consists of more than 8 trillion signals every day. Based on that all those insights, we also train our own machine learning models. With Azure Sentinel, we use those models in such a way that security analysts don't have to do anything extra. They can use those models within the product to gain knowledge, get quick insights and prioritize billions of signals. Making better and more use of machine learning therefore helps to empower and improve the efficiency and effectiveness of the security analysts.

All technologies, automation, orchestration and the traditional value of SIEM are coming together. Besides SIEM and SOAR, the User and Entity Behavior Analytics aspects are also being integrated and combined into these solutions. CISOs are looking for this type of combined approach to help make their SOC more efficient. They can have integrated, more cohesive solutions that give these capabilities.

KPMG: You mentioned a lack of security expertise as one of the challenges. Is this something you also see as

not being completely resolved but eased into by freeing up resources to use machine learning and AI?

Adwait: It's not the full solution, machine learning will not solve the situation of lack of expertise. That is a partnership between the security organizations and security vendors helping each other to create more training and certificates, which will again create more opportunities for people to learn. This is a long-term effort for the industry. On the other hand, machine learning and AI are there to help make your existing security more efficient and drive your business. It is important to understand what business results AI is driving. Microsoft uses AI internally, and the insights that we have are provided in Azure Sentinel. We want to save time cost for our clients by providing built-in machine learning models.

Apart from machine learning and AI trends, I also see another trend in increased usage of automation and orchestration within SecOps. Security analysts and even CISOs want to have automation and orchestration in place for effective incident response.

KPMG: What is in your view the unique thing about Azure Sentinel compared to more traditional SIEM and SOAR solutions?

Adwait: Azure Sentinel is a cloud native solution. Created on a proven public cloud platform. That helps us integrate Azure Sentinel with all other Azure services such as log analytics. There are also logic apps that provide you with automated playbooks. You can also make your own playbooks for incident response or develop playbooks to integrate with your existing solutions like ServiceNow or your firewalls. That is the benefit we can offer with public cloud. The other benefit with public cloud is that it does not require a setup or maintenance, and it scales dynamically to help address your needs. When data requirements are growing and the analysis grows automatically, Azure Sentinel grows and changes with you.

The other differentiator is the unique threat intelligence and built-in machine learning models that we provide. Microsoft processes more than 8 trillion threat signals per day. Imagine the insights we draw from them. They are all distributed in the services we offer. We provide robust threat intelligence, robust insights built by diverse signals. All the detection and hunting rules we provide are all based our own experiences and what we run inside Microsoft. Our security operators and our security analysts are always working on these queries. We provide our expertise to the customers and we provide our own security analysts, which is very efficient for our customers. With the built-in machine learning that we have in Azure Sentinel, we have seen the alert fatigue go down more than 90%. Reducing false positives, to just pinpoint prioritized alerts is the efficiency that we help drive with these built-in models.

> "Machine learning will not solve the lack of expertise"

Internal security analysts working within Microsoft SOC; we offer all of that expertise to our customers. We leverage all the activities that they are performing with their analysis and insights to constantly improve our detection and response capabilities. Combined with our open community that is available on GitHub where our partners, our customers are also contributing, not just with machine learning models but also with detection rules, threat hunting rules or even playbooks. We offer more than Microsoft security experts; we offer a community that helps improve your security operations.

Integration with your existing tools. More than 200-250 apps that you can integrate, and you can create playbooks to automate your incidence response. We also work with many solutions that customers might already have. Many customers today might have invested in existing solutions, but may not be able to fully switch to the Microsoft Ecosystem. We can work with that! For example, we can integrate Azure Sentinel with ServiceNow. Manage and monitor the incident with Azure and use the ticketing system of ServiceNow.

KPMG: What kind of journey do you see clients taking for example that already have a SIEM solution, such as Splunk, and would like to move to Azure Sentinel? Do you have any thought on how that would work?

Adwait: There are many scenarios, and each situation is different. There are organizations that really want to switch/migrate to Sentinel. One case is where we are working with customers who are in the process of migrat-

ing from their existing solution to Azure Sentinel. It is one approach that customers are taking for whatever reason. Then there are many other organizations that are thinking of it as side by side. As they grow their footprint in the cloud, they want to have a cloud solution. They are embracing Sentinel to get all their data from the cloud, and then their existing solution, which is on-premise, is used to collect on-premise data, connecting these two solutions.

KPMG: In this hybrid situation, is there something that works well for clients or do you think there is a need to move only to cloud?

Adwait: Good point! Our discussions were mostly about this strategy as part of the journey and not as the end strategy. We see more and more customers embracing cloud technology. This is therefore part of the journey to get the benefits of the cloud, but because of their existing investments (especially for large mature organizations), they may not be able to switch all their instances at once. So, moving to the cloud and Azure Sentinel is a gradual process.

KPMG: What are the challenges you see with customers that are now implementing Azure Sentinel, is there something that you see that is often difficult for this journey?

Adwait: Something that all customers need to think of is understanding the data sources they want to collect data from. They must have a strategy to connect those data sources to Azure Sentinel, especially if they have an existing on-premise solution. Then they have to think of a strategy on how they are going to connect all that data in the cloud, data normalization, what is the critical data you want to send into the cloud. A strategy should be put in place before you start configuring Azure Sentinel.

CONCLUSION

With organizations increasingly embracing cloud and hybrid cloud strategies it is harder to have a consolidated view across an organization. Alerts are increasing, and in different locations, and compounding the issue turns out to be a lack of expertise in some organizations. SOAR solutions available in products such as Microsoft's Azure Sentinel can help alleviate some of this pressure by automating repetitive tasks, freeing up precious resources to be spent on tasks that require more deep thinking. Machine learning and User Entity and Behavior Analytics can also help to make a SOC more efficient if implemented well. These tools in combination with organizations and vendors working together to upskill resources will help to tackle these complex challenges in the long term.

References

[ESG19] ESG (2019). Security Analytics and Operations: Industry Trends in the Era of Cloud Computing.

[Harv19] Harvey Nash / KPMG (2019). *A changing perspective.*

[Morg19] Morgan, E. (2019, 24 October). Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021. Retrieved from: https://cybersecurityventures.com/jobs/

[NCTV19] NCTV (2019). *Cybersecuritybeeld Nederland.*

About the interviewee and authors

Adwait Joshi is Director of Product Marketing for Azure Security at Microsoft. Adwait has 20+ years of experience in the field of technology, including in the areas of product engineering, networking and security.

Jacqueline Morrison is a senior specialist within the Cyber team at KPMG NL focused on Security Operations. During her career in Cyber Security spanning over a decade she has helped organizations assess, design and implement their Security Operations function from a strategic and procedural level, as well as leading teams to build detection and response services, including during high pressure incident scenarios. She also has extensive hands-on technical experience including working in roles as a SOC analyst and the engineering and configuration of security tooling (e.g. SIEM, IDS/IPS, Endpoint Protection).

Jeroen de Wit is an experienced senior manager within KPMG Cyber with a primary focus on Security Operations, for which he is the Dutch lead within KPMG and co-leading the Global Core SecOps SME team. He is the co-author of KPMG's Global SecOps framework. Besides SecOps he possesses a wide experience in a variety of Information Security related engagements including penetration testing, network and infrastructure security design and review, (web) application and protocol security, as well as the Cyber Defense organizations', procedures' and technologies' design, implementation and review. Jeroen has been involved with the implementation of Security Operations capability and selection of technological solutions as well as managed security service providers for numerous clients.