# THREAT HUNTING CAPABILITIES IN THE CLOUD

SHASHEEN BANDODKAR

ADELPHI UNIVERSITY

THREAT MODELLING- CSC 674-001

FALL 2019

ABSTRACT

Cloud computing is a new way of delivering computing resources, not traditional technology. Computing services range from data storage and processing to software, such as email handling, are now available instantly, commitment-free and on-demand. The main focus of this paper will be on how cloud economies of scale and flexibility are both a friend and foe from a security point of view. Massive concentrations of resources and data, present attractive targets to attackers but cloud-based defences can be more robust, scalable and cost-effective. The danger of cyberattacks is increasing day by day because of the growing number of cyber threats in new, advanced and complex technology. Any potentially-targeted company should be aware of these threats before they materialize in an actual attack. After all, it is much better to prevent a breach than to detect it and subsequently clean up the damage via consultants and lawyers. Security measures such as endpoint protection and firewalls are not enough to protect systems and their data from different types of cyber threats. Now the big challenge is how to collect the relevant data from the wide range of sources. For this reason, the amount of data that will need to be extracted and monitored and its retention window will be very significant. Another important requirement is the use of as much automation as possible. It is too hard to only manually browse the web looking for this content, let alone to manually correlate between different platforms and within large time windows. Cloud customers need assurances that providers are following sound security practices in mitigating the risks faced by both the customer and the provider (e.g., DDoS attacks). This is required to make good business decisions and to maintain or obtain security certifications.

## 1. INTRODUCTION

It is important to know the enemy and understand how an attack would be possible both internally and externally. Some external attacks include Phishing, malware, botnet, ransomware, etc and internal attacks include the lack of skill sets of the security professionals working in the enterprise. To understand how a cyberthreat or attack works we need to analyse a few things: -

1. It is important to be prepared and build a standard and document all the incident reports. When all the high authority officials at an enterprise understand the risks of a cyber-attack and the benefits involved, they will be much more likely to contribute, implement and add to the necessary plans to avoid a cyberthreat.
2. Once a plan has been documented it is important to test it and continue testing it. It is important to have test-driven developments.
3. Running simulations to keep testing the system is important as it helps see incidents, prepare for something unexpected and also helps in making improvements.
4. When a cyberattack is underway one needs to have the ability to make quick decisions and adapt to the continuous changing information. Incidents occur out of nowhere and are rarely fully formed. It is important to put data to work, and some of the key components for the incident response platforms is the central hub to process, track and resolve incidents and try to integrate

with security technologies such as SIEM.

After these four steps, one of the most important things is to orchestrate this across people and process this effectively and improve the ability through the technology at the enterprise.

Threat hunting is an early-stage component of threat detection which focuses on identifying threats at the earliest possible phase of an attack or compromise. Threat detection as a broader term refers to the full set of processes focused on discovering and identifying threats, whether before, during, or after a compromise has occurred. It is important to formulate a hypothesis about a threat, for example, say attackers are exfiltrating your proprietary research data, or that they have successfully launched Phishing attacks against one or more employees and have compromised their endpoints. (eSecurity Planet, 2019).

## 2. BACKGROUND

Threat Hunting in the cloud can be confirmed, following an anomalous behaviour. It is important to know when and where this attack occurred or occurs to confirm whether this attack was an actual and active attack. This includes a combination of detection of these threats and hunting them down which includes identifying and detecting gaps in the cloud.

Firstly, it is important to build trust in the cloud and this is by providing security services. Large cloud providers can offer a standardized open interface to manage security service providers. This creates a more open and readily available market for such services. A cloud provider needs to have the ability to dynamically reallocate resources for filtering, traffic shaping, authentication, encryption, etc to create resilience for defensive measures against threats and attacks. The cloud can also provide pay-per-use forensic images of virtual machines which can be accessible without taking the infrastructure offline which leads to less down-time. It also allows cost-effective storage.

With benefits there are also many risks that are associated with cloud computing. In using cloud infrastructures, the client necessarily cedes control to the Cloud Provider (CP) on a number of issues which may affect security. It can be difficult for a user or customer to migrate from one cloud provider to another or migrate data and services because there is very little to offer in terms of tools, procedures or standard data, formats or services interfaces that could guarantee data, application and service portability.

Cloud computing does significant potential to improve security and resilience. This includes all kinds of defensive measures such as filtering, patch management, hardening of virtual machine instances and hypervisors, human resources and their management and vetting, hardware and software redundancy, strong authentication, efficient role-based access control, and federated identity management solutions. Cloud computing is a distributed architecture which means that more data is in a transit stage, this basically means that data must be transferred in order to synchronise multiple distributed machines between cloud infrastructures. Moreover, secure connections such as a VPN is used more often in data centres and not always practiced or implemented on the cloud. Five reasons why security professionals need the cloud.

1. Malware analysis: Malware analysis can be risky however a completely isolated network and sandbox system are needed to prevent the malware from accidentally moving into the production network. A simple mistake in a configuration or a shortcut used for convenience could lead a companywide outbreak. Another risk to take into consideration is the potential for the sandboxed malware to beacon back to the attacker's infrastructure. This will leave a trail for that attacker to follow back to a potentially compromised network. The attacker can then check for already infected machines or try to slightly adjust the attack method, based on the (partially) failed first attempt. The use of a third-party cloud platform is the perfect solution for all these issues.

2. Penetration testing: Penetration testing comes in many flavors, but quite often the tests are conducted from a system outside the target's network, simulating an external attacker. Security companies specialized in penetration testing could have their own infrastructure setup, but they could also benefit from the use of cloud platforms. The flexibility and relatively low on-demand costs have made this option very accessible. There is another

difference, however. If the penetration tester uses the security company's infrastructure, the attack usually originates from a known IP that can be (temporarily) suppressed or blocked by the target company as a response to the test. For a more thorough test or a red team exercise, however, this might not create a realistic scenario, because attackers quite often leverage cloud platforms for their attack. Companies are simply too risk-averse to block an entire IP range or subnet from for instance Amazon or Azure, potentially taking down legitimate services, leaving an opening that is often exploited by more sophisticated attackers.

3. Secure Storage: One of the most important roles any security professional has is to ensure the availability and integrity of security logs. Not only are these logs critical from an operational perspective (reporting, analysis, threat hunting, correlation), most companies also need to adhere to compliance regulations around the retention of this data. When it comes to cost per Gigabyte and redundancy options, cloud solutions tick all the boxes. Being based off-site storage, data is also much more secure in case an attacker tries to hide his tracks by directly targeting the logs.

4. Proof of concepts: A cloud environment is a perfect platform to build and test systems without affecting the company's production environment. Security professionals in the architecture or design areas or even attempting to troubleshoot an issue with for instance a firewall cluster can quickly set up an environment to proof whether a specific outcome can be achieved. Virtual machines and appliances and virtual networks avoid delays and costs associated with sourcing the required hardware and software, and once the proof of concept is completed, the environment can simply be reset or removed.

5. Virtual labs: Cloud technologies, however, have made virtualization even more flexible without the need for any on-premises hardware. Cloud solutions also significantly enhance accessibility to the platform. A security professional has access to the lab from anywhere and only needs an internet connection. For this same reason, vendors and specialized training providers offer training via a cloud model these days, greatly enhancing the accessibility of their offerings while reducing the requirements for the customer. There simply is no way around it; the cloud is here to stay and has become invaluable to any security professional.

## 3. DISCUSSION

So, the question begs as to what is needed to start threat hunting. Firstly, it is important to ensure that the organization is actually ready to threat hunt. One should have a fairly mature security setup capable of ingesting multiple sources of information and storing it in a way that lets you access it. A basic set up should include automated blocking and monitoring tools such as firewalls, antivirus, endpoint management, network packet capture, and security information and event management (SIEM). One will also need access to threat intelligence resources so you can look up IP addresses, malware hashes, indicators of compromise (IOCs) and more.

Compliance on Cloud: For consumers to get the information from the cloud provider is sometimes difficult due to high competition in market and security concerns, information such as

1. Physical Address of the data centres.

2. Certain Internal Procedures.

3. Security Defences.

Finally, the tool that allows you to bring together the disparate data sets and slice and dice them in a way that reveals insights with the least possible effort. Threat hunting can involve a massive amount of information, so while it is a human-led effort, you'll certainly need some computer assistance to make the task more manageable. Once all the tools are in place and working together, you will also need a team with enough people to manage the technology and data.

Why should one hunt for threats? While threat hunting it is important to have a proactive approach instead of a reactive approach, what this means is that a threat hunter must actively search for threats and bugs within the system. A reactive approach to this could have a very negative approach as, by the time you react to a threat, a user's system could already be compromised and could be very little or next to nothing he could do in order to regain control over the systems or the data that could be stolen or exploited.

A proactive approach could lead to catching a new or completely unknown threat. This gives a threat hunter an added bonus of exploring new unknown territories that could be harmful to the systems and also avert the danger and create a risk management plan against such a threat.

This is an example of threat hunting capabilities in the cloud environment, when basic security hygiene is implemented, the threat hunting team needs to start evaluating infrastructure for any threats and undetected breaches. Each infrastructure features moving parts, multiple operating systems, networking tools, and custom applications. Security teams need to know which threats to look for, how to prioritize them, and where to start hunting and then you add the nuances of doing this in a cloud environment. Threat hunting is all about proactive analysis of data to detect the anomalous behavior that is undetectable by the security products. As the threat hunting team's analytics become more sophisticated, it may begin developing a set of repeatable analytics, enrichments or data gathering steps. If it's repeatable and articulate, it can be automated.

If we summarize, these are some top potential threats of cloud computing that must be thought about instead of moving to the cloud blindly. The Cloud Security Alliance identifies following potential risks:

1. Abuse and Nefarious Use of Cloud Computing: Cloud providers offer their customers the illusion of unlimited computing, network, and storage capacity. There are registration processes where anyone with a valid credit card can register and immediately begin using cloud services. By abusing the relative anonymity behind these registration and usage models, spammers, malicious code authors, and other criminals have been able to conduct their activities with relative impunity. Cloud computing providers are actively being targeted, partially because their relatively weak registration systems facilitate anonymity, and providers' fraud detection capabilities are limited.

2. Insecure Interfaces and APIs: Cloud computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. The security and availability of general cloud services is dependent upon the security of these basic APIs. Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability and accountability. Examples: Anonymous access and/or reusable tokens or passwords, clear-text authentication or transmission of content, inflexible access controls or improper authorizations, limited monitoring and logging capabilities, unknown service or API dependencies.

3. Malicious Insiders: This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure. The impact that malicious insiders can have on an organization is considerable, given their level of access and ability to infiltrate organizations and assets. Brand damage, financial impact, and productivity losses are just some of the ways a malicious insider can affect an operation.

4. Shared Technology Issues: Often, the underlying components that make up this infrastructure (e.g., CPU caches, GPUs, etc.) were not designed to offer strong isolation properties for a multi-tenant architecture. To address this gap, a virtualization hypervisor mediates access between guest operating systems and the physical compute resources. Attackers may focus on how to affect the operations of other cloud customers, and how to gain unauthorized access to data.

5. Data Loss or Leakage: There are many ways to compromise data. Unlinking a record from a larger context may render it unrecoverable, as can storage on unreliable media. Loss of an encoding key may result in effective destruction. There is damage to one's brand and reputation, a loss could significantly impact employee, partner, and customer morale and trust.

6. Account or Service Hijacking: If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. With stolen credentials, attackers can often access critical areas of deployed cloud computing services, allowing them to compromise the confidentiality, integrity and availability of those services.

7. Unknown Risk Profile: Information about who is sharing your infrastructure may be pertinent, in addition to network intrusion logs, redirection attempts and/or successes, and other logs. When adopting a cloud service, the features and functionality may be well advertised, but what about details or compliance of the internal security procedures, configuration hardening, patching, auditing, and logging?

Focussing the attention more towards the amount of visibility that can be gained inside a cloud, this is essentially a tricky aspect of it. For a larger organisation being the cloud provider, it may be easier for them to convince their clients for gaining visibility of their data and providing essential security measures to make it more secure inside the cloud but for a smaller organisation that might not be the case. There may be users who do not wish to subscribe to the necessary or cautionary measures provided from the cloud providers side, in this case a third party could be brought in and a legal contract could be signed. In this way a user or client gets what he wants, but an argument can also be made as to what if the third-party service provider gets compromised. Additional complexity is introduced because organizations seldom have a single-cloud strategy. Therefore, threat hunting solutions must "talk" to multiple clouds. The ability to capture, normalize, and enrich data across environments is a core requirement of an effective threat hunting platform. One major concern security teams have is losing visibility and detection capabilities when their organization moves to a cloud. While this might have been true in the early days of cloud services, these days providers are announcing new threat detection features and offerings almost every month. These new services open up the possibility of adjusting traditional network- and host-based monitoring to support intrusion detection in the cloud.

An added question to such a problem would also be to determine the level of access a cloud provider or a third-party service would or should have over a particular client's or user data. There can be no definite answer or solution to a question like this yet, what we could portray or resolve through this situation is that such a matter is basically based on a very key aspect which is "Trust" especially in a small-to-medium enterprise. Some clients will let you gain access to critical information and then there are some who would not but in security terms it's a continuum with a lot of grey in between. After all, security is very rarely a selling point for the clients.

Cloud services have mushroomed in the past couple of years and are becoming widely used by a large number of people and companies. There are many benefits when a company chooses to implement the existing or new service/application in the cloud, which is why the traditional way of building applications is no longer being widely adopted. There are many applications and systems, which companies can move to the cloud, compared to privately owned internal networks.

MITRE is a federally-funded research and development centre (FFRDC) for the U.S. government. As part of its duties as an FFRDC, it performs research and development in a variety of different fields, including cybersecurity. For example through a recently published article about the threat hunting capabilities in a cloud environment of automation, once attackers gain access to the web application VM, they will want to use the MITRE ATT&CK tactic called Discover to find other services of interest, such as an accessible Amazon S3 bucket with the command List Buckets. In AWS, the case study looks at the web application which has access to Amazon S3 buckets for configuration. The IAM role does not allow listing of buckets. Automated systems likely already know the resources they need to interact with, so listing potential names is unnecessary. From the Amazon EC2 instance, listing buckets results in an error. This is where AWS Cloud Trail comes in. It gathers and allows an analysis of Amazon Web Services (AWS) API requests. AWS CloudTrail, using the Amazon EC2 ID as the username, looks at the List Buckets as an indicator. There is an Access Denied error code. Each event like this has a unique event ID and data table which a threat hunting team can then filter, carve, and format.

For securing passwords, one could use the framework to gain knowledge about the attacks that have occurred in the past depending on the service model, we're given a certain amount of access to the service managed by the service provider. In any case, we usually have a number

of passwords that we have to remember in order to access the cloud services. Since the services running in the cloud are most often accessible from anywhere in the world, an attacker knowing the password could log in and use our service, whatever it may be.

Best security practices while choosing a password inside a cloud would be to use:

First time passwords: a service provider has to choose a password when setting the services up for the customer. This happens when the process of setting up everything doesn't ask the customer for a password that will be set during the installation phase. In such cases, the service provider has to set the password to a unique value for each customer, but the customer's duty is to change it after the first use.

Shared passwords: when setting the password, we have to ensure we don't use the same password for other services as well. Setting the same password for two cloud services means that if one cloud service is hacked, and if the attacker is able to get the password, we will be able to use the second cloud service, because he already knows the password. There are times when cloud services don't store passwords securely in the database, but store them unencrypted or as MD5 hashes, which can easily be compromised. To keep secure, we should choose a different password for every service that we're using, so even if the attacker gets our password or password hash, he won't be able to compromise any other services.

Password durability: the password should be changed every 90 days in order to ensure the attacker doesn't have continuous access to our service in case he manages to compromise the password. By changing the password, the attacker will eventually be locked out of a service and won't be able to access it in order to steal sensitive information.

Minimum password length: There are different recommendations on the internet about the password length, but they all agree that we should choose a password of at least eight characters in length, while some support the idea of even longer passwords. Password strength- the password should not contain only letters and numbers, but should also contain special characters as well as lowercase/uppercase letters. By using such a password, there are many more combinations the attacker has to go through when trying to obtain the password via brute force or dictionary attacks.

Password history: the system should keep historic versions of passwords in order to compare them to the current password in password change functionality. This ensures the password is somewhat different from the previous passwords. An alternative solution to this is to use a password manager. In order to keep passwords secure, we should use a password manager, because otherwise we won't be able to remember the passwords of all of the cloud services while following the best practices already described.

## 4. CONCLUSION

The real science and power lie in the correlation between these two, allowing for the most dynamic and most proactive security posture an organization can obtain. One of the greatest advantages of threat hunting is, it increases the skill of a team of threat analysts and hunters to find out threats especially new and unknown threats against the particular system or a group of systems or systems of a huge corporate organization. Plus, the added benefit to such an activity is that it is always fun to discover and dive into unknown areas.

Threat hunting is never going to be the first priority. To start, it may not even be a full-time role just a few hours a week of one's time. There is no set threat hunting process that will apply to every company, so the team must have expertise in that organization's network. Without being familiar with the systems and knowing how everything is supposed to look, it will be impossible to determine how to best hunt for threats. With the cloud it is the run anywhere see anything factor that appeals to the audience. And a big part of working on the cloud is gaining, keeping and continuously fostering the environment where trust is valued and communicated to everyone that is participating in it. It would be beneficial to take advantage of cloud native tools to increase automation and maintain visibility while limiting the time investment from your team.

The more one analyses threat hunting and in broader terms information security, the more one realises that it is not just about the bugs or threats or security at all. It is more about the intent and trustworthiness which is led by

perceptions. Once again, the cloud brings some new opportunities ranging from the availability of commercial products located within a cloud platform to the ability to obfuscate and gain efficiency via public cloud options. The first step is to start looking at the requirements. The next step is to find a matching solution, not the other way around.

REFERENCES

[1] Condon, J. (March 22, 2017). Building a Threat Hunting Practice Using the Cloud [PowerPoint Slides]. Retrieved from https://www.slideshare.net/ProtectWise/building-a-threat-hunting-practice-in-the-cloud

[2] Rubens, P. (May 17, 2019). How to Run a Threat Hunting Program [web blog comment]. Retrieved from https://www.esecurityplanet.com/threats/threat-hunting.html

[3] Lord, N. (September 11, 2018). What is Threat Hunting? The Emerging Focus in Threat Detection. [web blog comment]. Retrieved from https://digitalguardian.com/blog/what-threat-hunting-emerging-focus-threat-detection

[4] Byrne, L. (September 12, 2018). A Beginner's Guide to Threat Hunting. [web blog comment]. Retrieved from https://securityintelligence.com/a-beginners-guide-to-threat-hunting/

[5] Fontaine, A. (July 18, 2017). Threat hunting and the cloud- A dynamic tension. [web blog comment]. Retrieved from https://www.rsa.com/en-us/blog/2017-07/threat-hunting-and-the-cloud-a-dynamic-tension

[6] Cloud Computing Risk Assessment. (2019). Enisa.europa.eu. Retrieved 2 October 2019, from https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

[7] Shu, X., Araujo, F., Schales, D. L., Stoecklin, M. P., Jang, J., Huang, H., & Rao, J. R. (2018, October). Threat intelligence computing. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 1883-1898). ACM

[8] Five Reasons Why Security Professionals Need the Cloud. (2017). Infosec Resources. Retrieved from https://resources.infosecinstitute.com/five-reasons-security-professionals-need-cloud/

[9] Cloud Computing Security: Be Secure Before Moving to Cloud. (2017). Infosec Resources. Retrieved from https://resources.infosecinstitute.com/cloud-computing-security-secure-moving-cloud/

[10] Before you move to the cloud. (2013). Infosec Resources. Retrieved from https://resources.infosecinstitute.com/before-you-move-to-the-cloud/

[11] Securely Managing Cloud Credentials. (2015). Infosec Resources. Retrieved from https://resources.infosecinstitute.com/securely-managing-cloud-credentials/#gref

[12] Open-Source Intelligence Collection in Cloud Platforms. (2018). Infosec Resources. Retrieved from https://resources.infosecinstitute.com/open-source-intelligence-collection-in-cloud-platforms/

[13] Sussman, B. (2019). Threat Hunting Capability in the AWS Cloud. Secureworldexpo.com. 17 December 2019, Retrieved from https://www.secureworldexpo.com/industry-news/threat-hunting-capability-in-the-aws-cloud