MSc Cyber Security

7030CEM - Cyber Security Individual Project

Analysis of various vulnerability scanner tools for preventing cyber threats in an organization based on customer requirement.

Author: Maneesh Mohanan Arippa Parayil

SID: 10660878

Supervisor: Dr John Filippas

Submitted in partial fulfilment of the requirements for the Degree of Master of Science in Cyber Security

Academic Year: 2020/21

Declaration of Originality

I declare that this project is all my own work and has not been copied in part or in whole from any other source except where duly acknowledged. As such, all use of previously published work (from books, journals, magazines, internet etc.) has been acknowledged by citation within the main report to an item in the References or Bibliography lists. I also agree that an electronic copy of this project may be stored and used for the purposes of plagiarism prevention and detection.

Statement of copyright

I acknowledge that the copyright of this project report, and any product developed as part of the project, belong to Coventry University. Support, including funding, is available to commercialise products and services developed by staff and students. Any revenue that is generated is split with the inventor/s of the product or service. For further information please see www.coventry.ac.uk/ipr or contact ipr@coventry.ac.uk.

Statement of ethical engagement

I declare that a proposal for this project has been submitted to the Coventry University ethics monitoring website (https://ethics.coventry.ac.uk/) and that the application number is listed below (Note: Projects without an ethical application number will be rejected for marking)

Signed: **Maneesh Mohanan Arippa Parayil** Date: **27th August 2021**

Please complete all fields.

First Name:	Maneesh
Last Name:	Mohanan
Student ID number	10660878
Ethics Application Number	P123129
1st Supervisor Name	Dr John Filippas
2nd Supervisor Name	Dr Derrick Newton

This form must be completed, scanned and included with your project submission to Turnitin. Failure to append these declarations may result in your project being rejected for marking.

Abstract

In Today's world computers has been commonly used in various sectors and lot of sensitive information has been stored, in order to protect from cyber-attacks, we have to be more cautious from the security compliance level. Web sites has been hosted in internet and when we are trying to access the applications from office or from at home so there is a chance of cyber-attacks, if it is an untrusted site. Internet is playing a vital role in IT organisations, Banking sectors, Public sectors also. Protecting from the cyber-attacks it is a too difficult task, and also if any cyber-attacks happens in a military, Police, Research and analysis Wing (RAW) it will treat as a national security threat. In order to safeguard the security compliance, we need to deeply thing about which tools (Network monitoring tools, Antivirus protection software, Vulnerability scanner tools and so on) and which are all the extra devices (Firewall, RSA authentication, VPN tunnel, Access control and so on) are required for improving the security measures of an organization. If any Internet based software is developing then the developer should be aware of the risks and security measure when they are planning, designing, developing and during the implementation stage. Once the attacks are happened in an organisation, then the firm goodwill will be losing and then the customers will not be going into the respective organisation in future. In this paper we will be discussing about the most common cyber-attacks and how to prevent the cyber-attacks at a large extent and also which are the best technique and tools which help us to analyse and detect and prevent from the cyber threats.

Table of Contents

Acknowledgements

It was an immense pleasure to join in the esteemed Coventry university for doing the Masters in Cyber Security course. During my project report “Analysis of various vulnerability scanner tools for preventing cyber threats in an organization based on customer requirement” preparation time there are lots of doubts and clarification had pop up. We are taking this opportunity for thankful to my Professor Dr John Filippas, Dr Derrick Newton and Project coordinator Dr Rochelle Sassman for proper guidance and support. Without your proper mentoring this will not be successfully completed.

1 Introduction

My Cyber security project title is “Analysis of various vulnerability scanner tools for preventing cyber threats in an organization based on customer requirement”. We all are living in the cyber world and we all know lot of innovations are happening and, also lot of security breaches are happening on daily basis. We can’t imagine the world without the computer. If we are not handling or managing the computer properly it will lead to a big consequence. In this report we will discuss about the various cyber-attacks and how we can restrict to a certain extent with the help of few tools which is available in the market. Cyber security threats are happening in various sectors like public and private sectors if there is a proper security measure are in place we can control these attacks like updating the security policy of the organisation, process, we should analyse which are all the security weakness areas and strengths and also we need to update and keep the security measures in place for the various cyber-attacks in the premises from internal and external threats. In this report we will explain what are the cyber-attacks are happening, and if the attacks are happened what would be the impact to the organisation.

1.1 *Background to the Project*

In today’s world cyber-attacks had become a universal security threats and we need to avoid these attacks in private, public and financial sectors by keeping the proper security measures in place. As the technology is developing on the other side there are lots of ransomware and malware also designing and developing by the hackers. The main intention of the hackers is to steal the confidential data, sensitive data and individual personal information like computer passwords, credit card details and with respect to organisation perspective like client details, client proposal details of the project, trade secrets of the firm and so on. In the year 2021 the major cyber-attacks where happened and those types of attacks are Microsoft Exchange Server Cyber Attack, Channel Nine Cyber-attacks, Harris Federation Cyber Attack, CNA financial Cyber Attack, Bombardier Cyber Attack, Colonial Pipeline Cyber Attack (Nadkarni, 2021). In this paper we will cover how to mitigate different types of cyber-attacks, with some proposed solution like implementing some vulnerability assessment tools in the organisation machines. Most of the attacks are happening from intranet and internet, so first we need to analyse thoroughly the network security, system security and compliance level of the organisation, and also weak and strength areas so that we can come up with a better proposed solution. Due to cyber-attacks the respective country economy will get declined and also in some cases the organisation should be shut down until the issue got fixed. As an initial step for securing the organisation from cyber-attacks the firm should invest some money for procuring the latest monitoring tools and hardware devices but eventually as a long run if the firm is secure from the cyber-attacks, they can gain the trust from the clients and they can get a lot of business proposal in future. In this paper we will be explaining in details of three different types of vulnerability scanner tools and will explain how it will be benefits to the organisation if it implements in the real scenario.

1.2 *Project Objectives*

The main of this project is to protect the organisation form various type of cyber-attacks for that we need to analyse what are all the common types of attacks are happened in the recent years. And which sectors are targeting and what are all the outcomes once the attacks are happened so that we can secure the organisation appropriately. Till now there is no unique method to defend against the security breach occur against the governments entities, organisations, financial

sectors, schools and financial sectors. Now a days most of the applications has been hosted in the cloud networks so we have to think about the 360-degree security in terms of cloud security, on premises device security and mobile security. Advanced Persistent Threats (APTs) are frequently blamed for the most dangerous and deadly sequences of attack today. APTs attacks are normally happens across the network by using any third-party software or scripts and once it is successfully attacked to the targeted machine it will gain the unauthorised access and it will be stay for a long period of time without been detected (Noam Erez, 2018). There are different ways to keep the information security objectives as secure those are mentioned below (8 Information Security Objectives to Manage Risk | ThreatModeler Soft, 2019).

- Information security strategy should be outlined.
- Security objectives should be defined on initially.
- Evaluate the Outcomes of the Information Security Function.
- Perform a Cost Estimation.
- Establish Information Security Policy.
- Protect the Four Levels of Data Privacy.
- To reduce security risk.
- Use the leading technology threat software application.
- Implementation of Information Security Management System.
- Facilitating the business.
- Risk management.
- Efficient operation.

As per my research we have identified the leading vulnerability assessment tool for mitigating the security breach. As per my detailed analysis we have selected three different types of tools, which is the leading in the market, and lots of the IT organisation, Financial sectors and government entities are using this software for avoiding the security breach. In this report we will discuss further in detail about below listed tools and why we have chosen these tools what are all the benefits by using these tools in detail.

1. **CrowdStrike.**
2. **Acunetix.**
3. **Qualys.**

As per the report the hackers are becoming expertise in their areas and also APTs are becoming more advanced day by day and on the other hand the security measure is not updated. The main reason of cyber threats is increasing is that there is a shortage of Cybersecurity specialist. In the year of 2018 there are two million of cyber security jobs are vacant (Noam Erez, 2018). Few of the objectives of my project are listed below.

- How to control the cyber-attacks.
- Performing a detailed analysis with respect to the security controls of the organisation.
- Selecting the Leading vulnerability assessment tools.
- Implementing the ISMS and Managing it updating it as and when required.
- Different types of attacks and technique.
- Risk assessment plan.
- Conducting regularly the training awareness to the Employees and grooming their technical skills set.
- Budget details and licensing of the tools.
- Ease of use and accuracy.
- Report generation and Meeting with as per the industry standard audit compliance.
- Periodically Security Audit meeting.

1.2.1 Analyse and Requirements Gathering

Software vendor will arrange a meeting with the Senior management along with the Different technical team (Security operation team, Network Team, Server Team, change management Team) for understanding the requirements and gathering the information what are all the areas they are focusing, what type of security they required. They will be taking the total number of assets it includes servers, desktops, laptops, network devices and how many locations it needs to be ran the scanning tool and what is the frequency and all? Then they will be collecting the system logs, network logs as per the ISM team's approval, then they will do the thorough analysis and they can understand which are all the areas should be focused more addressed, what are all the additional features to be enabled, any additional hardware appliance to be procured from outside to securing the organisation more secure. From the logs or the details provides from the management and technical team we will be understanding the following points.

- What are all the Standard operating Environment software are currently using.
- What are all the flavours of operating system are used within the organisation.
- How many applications has been hosted in the internet and intranet?
- Which are all the freeware's software are currently used.
- Which Antivirus tools are currently using?
- Are they conducting periodically internal and external audit meeting for against the security compliance as per the industry standards?
- How frequency the OS patches had been done and service packs are up to date or not.
- What is the policy and process of the external vendors or clients to the organisation, when they come for meeting?
- How the employees are login into the respective machines and how they are connecting form home to the office network.
- How the Access control list has been configured.

By understanding the above details and what is the budget they are planning to invest we will be giving an appropriate solution for making the organisation more secure. Once they have implemented then after the external audit if they receive the external audit and receives the ISO 27001:2017 information security certificates. By achieving this certificate, we can prove that how much data are secure within the organisation, by gaining the strength we can get more contract from international clients and eventually there is an increase in the economy of the respective country.

1.2.2 Criteria for selecting Vulnerability Assesment Tool

Vulnerability assessment tool helps to scan the entire devices such as desktop, laptops, servers, firewalls, operating systems, Applications within the network infrastructure which we are selecting and generate the report as per the priority list (Normal, Low, Medium, Heigh). Based on the reports we can take the necessary actions. Most of the vulnerability scanner tools have the unique features like identification of assets, classification of assets, detecting the vulnerability and classifying and categorising, missing patches and linking to the information's, customising of the templates run, sometimes console will be a centralized one and it can be accessed via web-based portal and vast range of hosts and operating system will be supported. Finally, about the cost estimation and the customer support which they are providing to the organisation, then they will finalize the product.

1.3 *Overview of This Report*

My report is prepared in the consideration of the university standard format. The entire report explains about the various types of cyber-attacks and we have to mitigate those attacks by using different tools and some few system etiquette to follow by the end users, customers and employees. Firstly, starting with the introduction and background of the project and with respect to the best vulnerability tools which is available in the market by addressing lots of key features. Secondly, starts with the Literature review, methodology. In methodology We explained about the different types of tools individually. In the Requirements section we talked about the how the vulnerability can be scanned by using these tools. Finally, we have done the comparison study, Solution, Recommendation and conclusion.

2 Literature Review

Cyber-attacks are getting increased every year and the main motive of the hackers are to gain the money by hacking their individual or organisation data. Cyber-attacks will be in two types targeted attacks and untargeted attacks. In targeted attacks the hackers will be paid, there will be some persons who will interested in your firm or personal data, where in untargeted attacks the hackers will choose random business organisation, devices or individual data. Hackers will choose the various methods for hacking the targeted organisation, infrastructures, personal computer devices and after the gaining the access to the targeted machine they will amend the data or restrict the access to the authorised person. Once a successful cyber-attack is happened in an organisation there are lot of impacts like economic lose, goodwill loses and some legal issues also. When we are taking the projects from clients, we used to keep their customers data, business information and some confidential information, if at all data breaches happened and when these data reach to the anonymous person, they can do any malpractices by using that information. There are cases like once the data breaches had happened then the client take it up legally and the respective organisation needs to pay penalty in millions of dollars. Finally, for mitigating the security issues they might have to shut down the business for a day, and there would be a lot of financial impact on the organisation when there is a disruption of business in an organisation. Most of the security breaches are happening due to the weakness in security configuration in system security and network security areas.

2.1 Reasons for Cyber attacks

Most of the times when the cyber-attacks are happened due to human error or technical glitches. It been normal like most of the days we are hearing news in social media or some media channel that some of the organisation has been hacked and they had stolen lot of sensitive data and personal data and it ends up by paying penalty or ransom money to the hackers for getting back the access to their data. There are cases like after paying the ransom money also the customers will not gain back the access to the normal machine sometimes, they will demand more money depends upon the data which hackers is having. To keep out this risk from the hackers and from the news which is yet to come in media channel about our firm or as an individual, we must take care of few things into consideration. Few of the main reasons where hacking is happening in an organisation are listed below.

- **Password is Week or Stolen –** It's been a common practice that instead of forgetting the password we used to write it down the password in somewhere else, if the password reaches to the anonymous person, they can do anything else and victim will be end up in trouble. Sometimes we will use the first name, last name, DOB, Sure name, mother name, father name, wife name etc, so once the hackers hack into the respective computer, if they know our personal information then they can login into the machine. So, a remedy we should keep the strong password which consist of alpha numeric with some special characters. We should make a practice that we should change the password periodically and as per the organisation standard there should be a password policy and employees should forcefully change once the password expires days is over.
- **Application and Network Vulnerability –** If there is no hardening has been done in switches as per the organisation security standards and if any applications are accessing from intranet and internet without a firewall in place then it will be heigh risk of hackers to get into the targeted machine. If we are building any applications and if the source code is available and poor coding it will leads to the hacking and once, they hacked they can retrieve our data. As a good practice we have to be updated the application with the

latest patches and the hardened the server and placing a firewall and putting an outbound and inbound rule for access.

- **Lack of permission access –** If there is no proper access control list in place then the data can be access and copied into their respective machine and they can modify as per their wish. For e.g. in an Organisation, individual data are storing in a file drive and if there is no proper permission is in place then the manager or HR data can be accessed by the employee. In order to get rid of these issues there should be a restricted permission access in place.
- **Internal Attacks –** We should not be shared out personal data or company confidential information to anyone, we don't know in future what it will happen. If any contractor or any employees leave the company there should be a proper procedure in place like for terminating the access, deleting the data at the end of the day, if any laptops or desktops are sharing to any employees after their termination it should be formatted and re-image and assigned to the new employee.
- **Remote access from Home –** Most of the IT organisations has been allowed to the employees to work from home concept due to this pandemic situation and earlier also in case of an emergency work. So, if any employees are accessing the company network from outside the premises there should be a proper way in terms of accessing the office network. There should be a VPN tunnel access to the organisation network and RSA token with two factor authentications so that the outside person cannot intermediate into the access channel when they are accessing the organisation network.
- **Social Engineering –** Hackers will interact with the victims in terms of taking survey and victim by unknowingly used to share their individual information and the hackers will take these as an major advantage to get rid of access into their systems .Even though sometimes advanced typed of cyber security systems also can't able to control the hacking mechanism .Now a days the social engineering attacks a listed as an top level of cyber threats, sometimes the gifts and promises they are giving after accomplish the task is an huge. So as an individual we should be more aware about these types of malpractices.
- **Exposure on Third party –** Instead of going to shop directly most of the people used to purchase the item as in online because it will consume their time and travelling cost. So, when we are doing the online purchase, we used to give our credit card, debit card, CVV number etc but we don't know as an individual is it secure or not. When we are taking E.g. as an online purchase, they will we relaying to the third party for making the online payment and the retailers believe the customers information will not be breached in any point of time. But when it come to the reality sometimes third party will not be taking any responsibility of data breach. Incident which was happen in 2013 attack by using the hackers and malware attack they steal the data from the third-party vendors and it has been ended to lose the contract of the third-party vendors and they have paid millions of dollars as a penalty.
- **Patch management –** In most of the cases the attacks are happening in an outdated hardware. In terms of organisation point of view most of the security breaches are happen in lack of updating the patches with respect to the operating system and the applications or software's they are using. When the hackers known about the software's or operating system vulnerability they can exploit the type of techniques to perform the cyber-attack. In the year 2018 in may month two major types of cyber-attacks happened. Hackers known about the windows operating system vulnerability known as Eternal Blue and they take the advantage if hacking into the organisation system. But the Microsoft aware about those types of vulnerability and they have released software patches two months before to address those vulnerability but organisation was not updated with the latest software updated and due to this it was end up by paying millions of dollars.

- **Cloud environment Vulnerability** – As a todays trend most of the companies rely on cloud technology, reason being is that it is a cost effective in terms of hard ware procurement, office space occupying, power saving and addition resources hiring for managing the devices. They will store their sensitive data on cloud network and on the other hand it as heigh risk of security breach. Using the cloud technology might be a higher risk of cyber security attacks if we are not incorporating the security compliance in place. Most of the company will be focusing on the cost estimation which cloud company is offering such as Amazon and Azure. The major types of attacks are Denial of service (DOS) attacks or account hijacking which will prevent the organisation to avail their sensitive data. Most of the company believes the cloud technology is advanced and their data will be secure, but when it comes to reality it is not secure and sometimes it might be get compromised. Till today there are no technology is advanced, the technology is just giving the advanced solution. There should be a holistic approach for against the data protection in their companies.
- **Non-Compliance with respect to Data protection** – As an organisation perspective meeting the audit compliance is not a secure thing for protecting the data but also, they have updated the policy as and when required. Most of the companies will make the documentation and proof whenever there is an external audit but in a reality in a normal business hour, they may not be adhering to the policy so there might be a chance of data breaches. As per the report from "Version PCI compliance report" there are four out of five companies had failed to meet their compliance at their initial assessment. Once they have got certified and they got ISO certified they will not be thinking about the additional security compliance so this will lead to the cyber-attacks.
- **Attacks on mobile phones** – Now most of the companies are offering their necessary services from their individual smart phones, organisation is thinking it is an advanced feature when employees are far from offices or vacation, they can access their necessary application and email from phone. But the if there any attacks are happened on phone the data will be reaching to the unauthorised person and it will lead to the cyber-attacks to the respective organisation. As per the report from "mobile security report" there are one out of five organisations is getting the data breaches and the most of the cases the attacks are happening from the malware or unsecure Wi-Fi connection.
- **Bring your own devices (BYOD) to organisation** – Most of the companies will encourage their associates to bring their own gadgets to the respective organisation. If they are connecting to the respective organisation and if it is any malware or virus will be affected then there will be a security breach. In one hand organisation will be having the advantages of bringing their own employee's devices but on the other hand there is a chances of security breach.

2.2 Top 10 common type of Cyber attacks

Cyber-attacks are increasing day by day and it is an offensive action. We cannot stop it at any point of time but we can control it by putting the adequate security control in place. We would be discussing in details about the top 10 listed various types of cyber-attacks (Melnick, 2018).

- **Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks** – A DOS attack exhausts a system's resources, preventing it from responding to service requests. DOS attack is mainly affected on the system resources and it is spread from the other machines which is in the same network, where the hackers are already hacked and controlled by them. In contrast to attacks which are required to facilitate the hackers to gain or increase access, DOS attacks will not provide additional benefits to the hackers.

By using the DOS attack the hackers can take the targeted machine as offline and they can perform various types of attacks in order to increase the access level, the best example is session hijacking. There are different types Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks few common types of attacks are botnets, TCP SYN flood attack, smurf attack, ping-of-death attack and teardrop attack.

- **Man-in-the-middle (MitM) attack** – In man in the middle attack scenarios hackers will create a communication link between the client and server. The best example is like a we had received email from the bank where we are holding our account, so it is just asking to update our personal records. So, we will be logging in to the bank and updating our details. Actually, what was happening is like hackers had created a website and we are sharing our every detail to hackers. There are different types of MitM attack some of them are IP spoofing, DNS spoofing, HTTPS spoofing, SSL hijacking, Email Hijacking, Wi-Fi eavesdropping, Stealing Browser cookies.
- **Phishing and spear phishing attacks** – Phishing attack is like we will be receiving email from a trusted source sometimes they used to perform some surveys, or to clink link which is attached in the email, or to click on the attachment with contains in the email. Once we downloaded the attachment then the malware will be installed to the victim's machines or by doing the surveys, we are sharing our personal information to the anonymous person. Spear phishing attack is like victim will be targeting to any individual and they will be researching them for a while and depends upon they will create the email and send it to him by making him to feel that it is from a trusted company, clients, Management, Banks.
- **Drive-by attack** – This method is mainly used for installing the malware into the victim's machine. Here the attackers will be tracking an insecure website and attacker will install a malicious script by using the HTTP or PHP code into the web page. When someone visits these websites, the malware will get installed into the victim's machine and also hackers will gain access to control the webpage. A drive-by attack will happen if there is lack of security flaws when there are no patch updates in operating system, browser and software's.
- **Password attack** – By using password normally user authenticate into the respective machine and retrieve their necessary information. Most common type techniques of password attack are searching at the employee desk, sniffing into the network connecting and looking into the unencrypted password or by using the social engineering. Final approach is trying the personal information of the targeted users. There are two types of attacks Brute force attack and Dictionary attack. Brute force attack is trying with the user personal information, Dictionary attack is like gaining the access into victim machines or into the network and getting the encrypted password and by using the tools they can decrypt the password.
- **SQL injection attack** – These attacks will happen when there is database is linked into the websites. The hacker will inject the SQL code into the database and they can perform the input command like client to the server. A successful SQL injection can modify the data in the database, they can shut down the database and even they can give the commands to the operating system. SQL injections is mainly work where there is a dynamic SQL is using in the websites and also it is common in the ASP applications and PHP code where they are using as older functional interface. Due to the programmatic interface available in J2EE and ASP.NET application and exploited easily with the SQL injection attack.
- **Cross-site scripting (XSS) attack** – Here the attacker will identify a website for injecting the script for vulnerability. Hacker will use the payload technique to inject the malicious script in the database for stealing the browser cookies. The website sends the page containing the attacker's payload to the victim's browser. The malicious script is executed by the user's browser. Once the script is executed successfully then then the

victim’s cookies will be shared with the attacker. Then the attacker will extract the targeted machine cookies and then they will perform the session hijacking. The more dangerous part is when it exploits the targeted machine more vulnerability then there is a more chances of various ways of attacks and they can steal the data, get the network information, access into the targeted machine remotely and they can control the targeted machine.

- **Eavesdropping attack** – Eavesdropping is mainly happened during the interruption of the network traffic. Then the hackers can steal the data of the victims like Bank details, Password, Confidential information when they are passing into the network. Eavesdropping can be of two types like active and passive.
- **Birthday attack** – Birthday attacks are carried against the hash functions, which are used to validate the integrity of a text, applications, or public key. The birthday attack refers to the likelihood of discovering randomly generated two different messages that produce the same message digest (MD) once prepared by a hash function. A successful attack will happen when the attacker calculates the MD of the user message then attacker can replace the victim’s message and the receiver cannot able to identify replacement when he compares with the MD.
- **Malware attack** – Malware attack is like when we are browsing internet then unwanted software’s will get it installed into user machines without his or her consent. Sometimes there will be malicious code also attached with that software and moreover it will be a useless application and It will spread throughout the internet. Some of the malwares are macro viruses, file infectors, system or boot record infectors, polymorphic viruses, stealth viruses, trojans, logic bombs, Worms, Droppers, Ransomware, adware and spyware.

3 Methodology

In order to making more secure of the organisation security compliance from the cyber-attacks we had done a thorough analysis and got three different types of tools for vulnerability scanning. Since now a day we are using the cloud technology and on premises devices we are addressing security aspects of these two areas also. By using these tools, we will be sharing a dummy report which had been generated with the customers and which are all the key areas it is checking, time taken to run, how many machines can be scanned at a type, which are all the flavour of operating system it will support. The report will be compliance with the audit point of view. The main motive of this project is to keep more secure an organisation from cyber threats and also, we will be doing a comparison study with other tools and the key features. To improve the security feature of an organisation as a First step we should analyse what all type of threats will happening towards to the organisation. Secondly, as per the list of the threats we can modify the changes in the device side and process and procedure. Thirdly, we have to manage the security level of the organisation we need to perform a vulnerability assessment test on monthly basis and in order to keep as a proof we should conduct an Internal and external audit periodically. By using the vulnerability assessment test, we can understand the weak areas in the system and we can close it on priority in order to avoid any data breach. Finally, we need to review the existing mechanism can close these vulnerabilities or add any new devices or replace and adding new security features in place.

Data which is shared in the cloud network or in a file server it must we encrypted form and the data which is in unencrypted it is more risk whenever any external or internal attacks happened. The most of the cases for a cloud basis file sharing service provided had been using a same key for encrypting the user data. Here the issue is any hackers get those keys they can access into cloud file server and access the user's data. Also, a remedial measure we should install any encrypted software in the servers and client machines so that data would be encrypted, it will be a type of two factor authentication where in initially it will ask for the encryption password for booting up the screen and secondly the windows login password. If at all the laptop is stolen or lost and the person who got that devices, he cannot operate it until and unless he does the complete format of the machines. We should be more care when we are using the cloning images for redeployment of images in an organisation machines, by using this method we can achieve the time consuming and large deployment can be done with the complete software package in a small amount of time. Before redeploying those images we should do the proper hardening and patch updates as per the latest releases from the various flavours of operating system and also we should not uses the old image each and every time month new images should be created so that the latest patches would be installed and most of the vulnerabilities will be closed so that there is a less chance of data breach.

When we are taking as an example of an organisation, there should be a wired local area network and Wifi so if there is any client, service provider is visiting the office premises then they should not connect to the Wired LAN or Employees Wifi. If they are connecting to the Employees who has connected to the Wifi or Wired LAN there is a heigh risk of attacks. In a corporate organisation network, there should be lot of devices connected like Laptops, desktops, Server, Storage, Tap Library, Mainframe computer, mobile phones so if any data breaches happen then it will spread to every device.

By understanding the risk and how to keep more secure the organisation from cyber-attacks, had done a detailed analysis and find out a best three tools which are available in the market. The criteria which was mainly look into was like reviews of the product, like time taken for the execution of scanning, How many numbers can accommodate during a scan run, what are all the key areas vulnerability scanning is happening, the report generation and is it fine with the audit point of view and finally about the cost for the procurement and type of support we will be

getting from the respective vendor. In this report we will be discussing about the tools **CrowdStrike, Acunetix and Qualys** in detail.

3.1 CrowdStrike

CrowdStrike is a leading tool which used to protect the data breaches in the cloud environment. CrowdStrike was founded in 2011 as a different kind of cybersecurity company, inspired by George Kurtz's vision. CrowdStrike, which is cloud-native, immediately brought a vulnerability perspective, performance, reliability, and efficiency to the industry that had never been before – perfectly trying to align Individuals, Future technologies, and Procedures. CrowdStrike Falcon has transformed security level for the era of cloud computing. Its only one ultra - light architecture uses artificial intelligence (AI) to provide real security and availability throughout the organisation, stopping threats on end devices and work overload in and out of the network. The CrowdStrike Falcon Framework is the top endpoint security remedy, bringing together the intelligence, technology, and expertise needed to better combat malware. A large amounts of data set (5 trillion activities each week) and malware attacks intelligence power Digital machine learning and behavioural indicators of attack (IOAs) to detect and blacklist malware. Professional ethical hackers add layers of defence to detect and stop even the most insidious attacks. Some of the key features are listed down about the CrowdStrike.

- **Cloud native:** In the sense that it reduces the complexity and easy to deployment and cut down the operational costs.
- **Artificial Intelligence powered:** It allows the team for instant visibility with the combination of power big data.
- **Single Agent:** It is a combination of entire packages and provided the maximum effective from the starting day of the deployment.
- **World class Intelligence:** Data which is residing into the cloud it will perform the threat intelligence in the cloud environment and provide a detailed report so that we can put a proactive security measure in place to control the security threats.
- **24/7 threat hunting:** With the help of falcons it will do a proactive check on the customers infrastructure. A separate team sits 24/7 support and they will be monitoring for suspicious activity and act like as additional layer of support for addressing if any solutions where missed.
- **Fully managed service:** Provides a better and more secure solution with a nominal cost if at all any poor security measure are in place. Experts from CrowdStrike will remotely access and do the configuration and solution to the respective organisation.
- **Better Protection:** With respect to the cloud platform to make more secure it combines with the package of providing the threat graph, artificial intelligence, combining machines learning, behavioural analysis and proactive checking of the threat hunting.
- **Better Performance:** As a single light weight agent works everywhere, it works in the office premise's devices, cloud infrastructure, devices hosted in the Data Canters and in the Virtual machines and even though when the devices are in offline status also.
- **Better value:** Without making more complexity on the infrastructure with more secure protection depends on the needs as per the infrastructure requirements.

Above mentioned are the important key features which is listed in the Crowdstrike webpage (Why Choose CrowdStrike? | Cloud-Native Security Solutions, 2019).

3.2 Acunetix

Acunetix is tool which is used for web applications and websites in order to make secure from the various types of cyber-attacks. Scanning will be performing very quickly and reliable and based on that the dashboard report will be prepared. Nowadays hackers are more concentrated in hosted applications in websites, because it can be accessible from Internet across the world as 24/7. Few of the hosted websites applications are Online banking, Online purchase, Shopping carts, Login page etc. Hackers will be targeting to the insecure websites, once they have identified the vulnerability, they can get into the corporate network through PHP injection, SQL injection, Cross Site Scripting, Directory Traversal Attacks, Parameter Manipulation (e.g., URL, Cookie, HTTP headers, web forms), Authentication Attacks, Directory Enumeration and other exploits and they can access the respective device and steal the sensitive and confidential data. Hackers will get into the targeted website and they will perform the illegal activities like hosting the phishing sites and due to this unlawful activity's owner would be liable to pay penalties to the customer. If the Websites application are not properly configured and secured the external and internal attacks will be happen at any point of time and the customers Bank details and personal details will be compromised and it will end up by paying millions of dollars as a penalty. As per the recent study from the Gartner group around 75% of attacks are happened into the web hosted applications. Few of the points are listed down for the reason for becoming websites as vulnerable.

- Websites are available in the Internet so that it can we accessible in 7 days a week for 24 hours for the customers, employees, clients and also for the attackers.
- Sometimes websites have been hosted in Internet and it will accessible from private and public IP address also there is no SSL or Firewall rule put against the cyber-attacks.
- Few cases from the websites there might be a direct access to the main database.
- Since the website applications are custom made there might we less level involvement of testing and parallelly custom made applications are heigh level of cyber threats.
- Most of the cases if the web applications are more securely configured and if there is a chances of web applications got compromised then the hackers will get in to the backend data through the web portal application. Even though if there is a secure firewall and machines are updated with the latest software patches also.
- Since the network security defence has been configured in port 80 there won't much protection against the web-based applications for making the day to day operations have to perform smoothly.

It would be a tedious and time-consuming task for checking the code regularly for identify the vulnerability in the web application source code. Source code consist of heigh number of lines and which involves the heigh level of expertise to monitor to rectify if any vulnerability is present in the code. On the end the hackers will be keen watch to the security blogs and they will be knowing before us, if there are any weak areas in the web application source code.

Acunetix is and automated web application tool which will scan for any sort of vulnerability like PHP injection, SQL injection, Cross Site Scripting, Directory Traversal Attacks, Parameter Manipulation (e.g., URL, Cookie, HTTP headers, web forms), Authentication Attacks, Directory Enumeration and other exploits. Acunetix uses the protocol like HTTP and HTTPS for scanning, it uses as browser page for scanning.

As a part of network audit, Acunetix will perform a Network audit for the server which is going to shot the web application in Internet and Intranet and will share the dashboard report accordingly if there is any vulnerability had been identified. The key area the scanning includes

for the Operating system latest patch updates, if there are unnecessary services are running, If there is any vulnerable ports are opened, Malwares or trojans are present in the system, if there is any weak password has been configured. All these actions which may lead the hackers to attack the system easily. Also scanning has been doing as per the secure of the popular protocol port such as FTP, DNS, SMTP, IMAP, POP3, SSH, SNMP and Telnet.

Above mentioned report has been referred from the Acunetix web portal which is listed in the Acunetix webpage (Introduction to Acunetix, n.d.).

3.3 Qualys

Qualys is a leading cloud-based services provider in order to secure our organisation data for against the data theft and compliance level. Qualys provide the touch base support for the Its infrastructure, cloud-based application, web application and for vulnerability patching. Qualys was founded in 1999, it has been established by the leading managed service providers and by integrated the major IT organisations like Wipro, NTT, IBM, Tata, HCL, HP enterprise, Cognizant and Infosys. Qualys is a part of Cloud Security Alliance (CSA). You know for managing the Asset inventory manually it would be a tedious task, as an organisation like MNC IT company their multiple locations like across region and across globe. So, in order to secure the devices from internal and external attacks we need to secure the machines, so we can use Qualys for getting that information of assets. Following mention are the details which we can get by the feature called as Cyber security Asset management of Qualys.

- Assets Host Details.
- Vulnerability Scan report.
- Compliance Policy scan report.
- Asset Inventory.
- Configuration of respective security details.
- Certificate view report.
- Vulnerable ports scan report.
- Last login Date and time.
- Active directory communication is enabled or disabled.
- Local User Name details.
- Software inventory details.
- Agent is active or Inactive in Internet.
- Software inventory report.

The Important key feature which is available in Qualys are listed below.

- **Global Asset View:** It will provide the real-time report for the complete assets which is present in across the organisation.
- **Cybersecurity Asset Management:** If there is any non-security compliance with respect to the device security features and updated patches will get a detailed report.
- **Certificate inventory:** Certificates information will be provided and if any devices is using the expired certification it will provide the notification separately.
- **Vulnerability Management, Detection and Response:** Patching the latest patches in real-time across our global assets.
- **Threat Protection:** Prioritize the threats as per the severity and as per the critical updates it will patch the system.

- **Continuous Monitoring:** Monitor the network regularly and if there is any abnormal activity found alert will be triggered immediately.
- **Patch Management:** Sync with the real-time patch updates and whenever the new patches have been released and tested, patching for the devices will be done automatically if the devices if in Office or travelling.
- **Endpoint Detection and Response:** It will act as a prevention if at all any attacks has been detected toward any endpoint.
- **Certificate assessment:** Validate the TLS configuration and digital certificates.
- **SaaS Detection and response:** Immediate fix on the compliance and security perspective on SaaS Application.
- **Cloud inventory:** Monitor in the cloud environment for the users, storage, instances, VM and networks.
- **Cloud security assessment:** Monitor in the cloud environment for any non-compliance and mis configurations.
- **Container Security:** Monitor the container for any attacks and tracking.
- **Web Application Scanning:** Provides end to end protection for the web applications.
- **Web Application Firewall:** Block the attacks and if any vulnerability is found it will block the attacks and patch it, it is simple, reliable and scalable.
- **Policy Compliance:** Updating the compliance as per the internal external policy regulations.
- **Security Configuration Asset:** Scan the configuration and security compliance in the virtual machines.
- **PCI compliance:** Important for the industry for the payment processing especially for online banking, so it will quickly update the compliance.
- **File Integrity Monitoring:** Track the files which is sharing across the network and alerting if there is any malicious activity is found.
- **Security Assessment Questionnaire:** Organisation will be doing with the external vendors and clients in order to mitigate the security risk there is automatic solution and streamline of vendor management risk process.
- **Out of band configuration assets:** Assets which is placed in Air gapped, in accessible assets and locked machines, Qualys will easily detect the mis configuration and vulnerability.

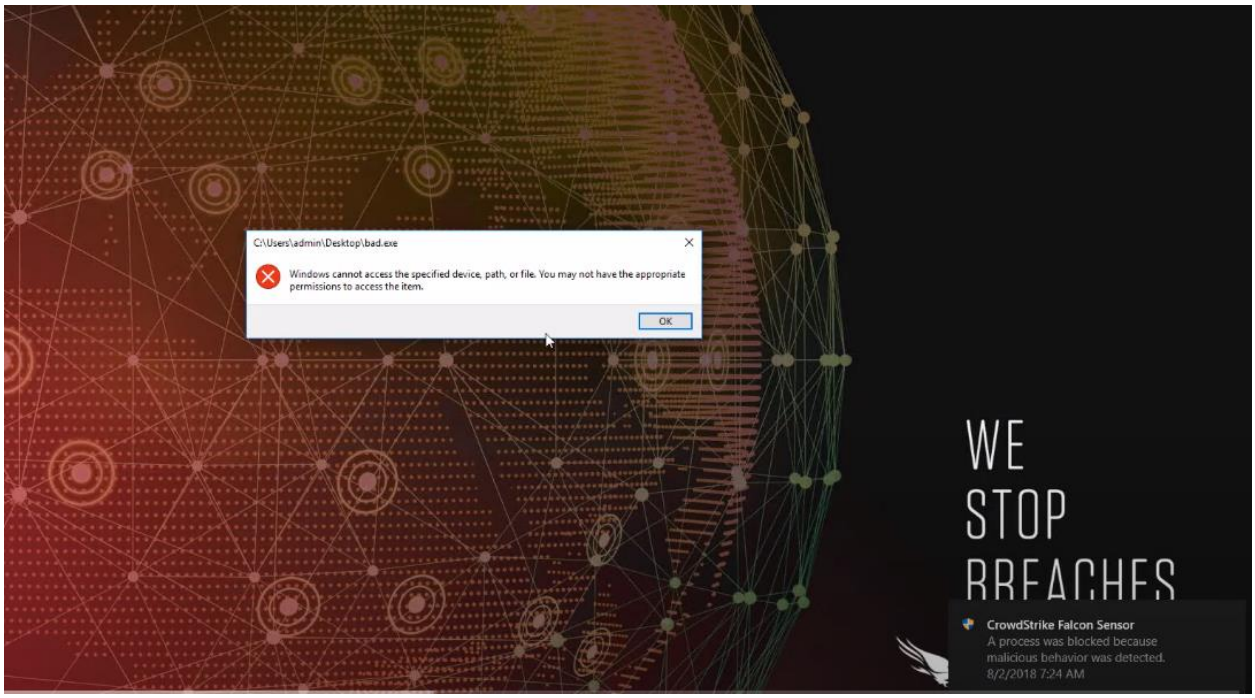
Above mentioned report has been referred from the Qualys web portal which is listed in the Qualys webpage (Qualys Cloud Platform Apps. | Qualys, Inc., n.d.).

4 Requirements

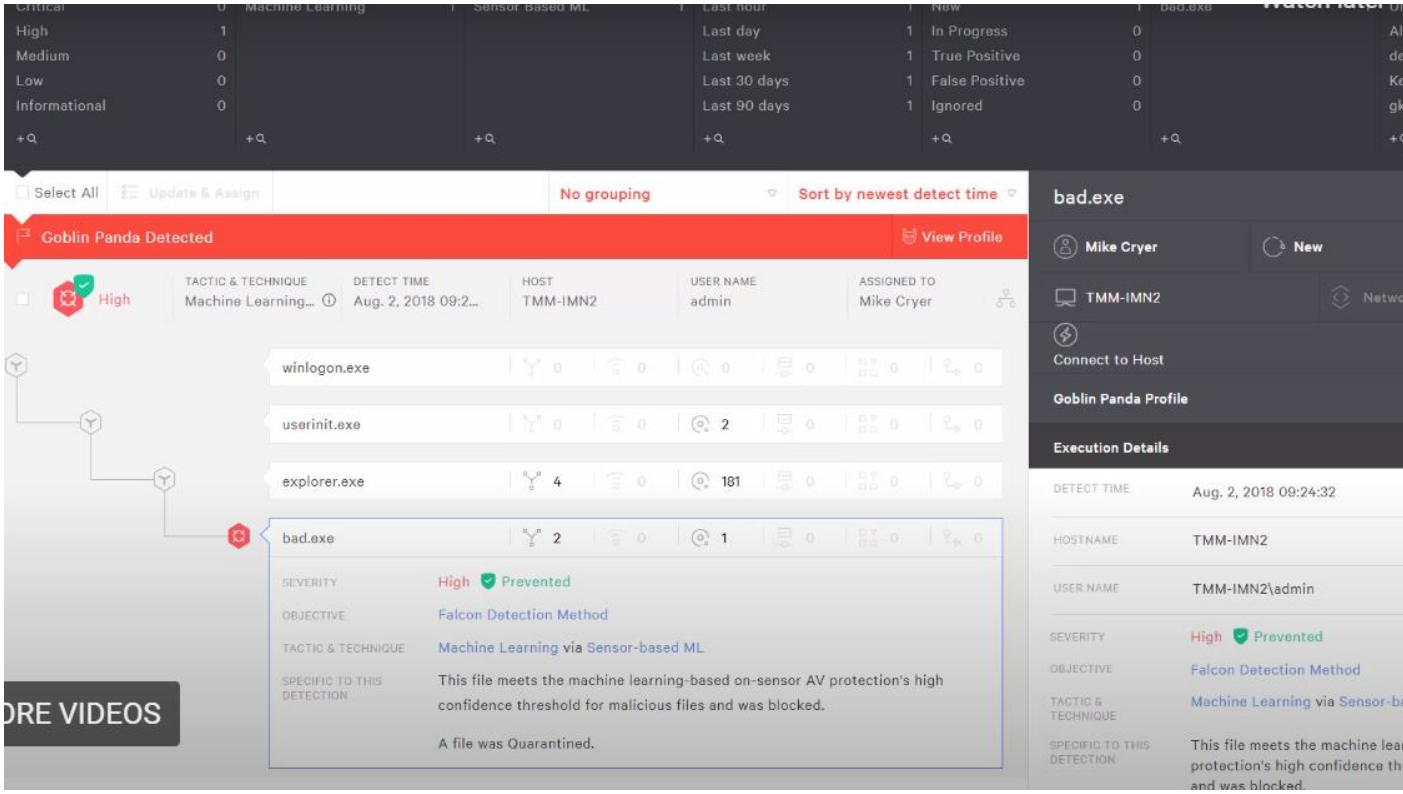
For configuring any tools, we need to find the best tools available in the market depends upon the requirements from the customer side. As an initial step we will be scheduling a meeting with the vendor and the client's management for the requirement and information gathering, once the necessary information is gathered then we will be selecting the tools based upon the feedback received from the organisation. Here we will be discussing about each tools configuration to identify the various types of vulnerability. As discussed earlier there should be basic configuration and the hardware's which they are using in the organisation, different flavours of operating system and various software's and web-based application they are using. In this report will be sharing with the installation steps, configuration and the dummy reports generated after the vulnerability scan.

4.1 Crowdstrike – How to Automate the threat intel by using the Falcon

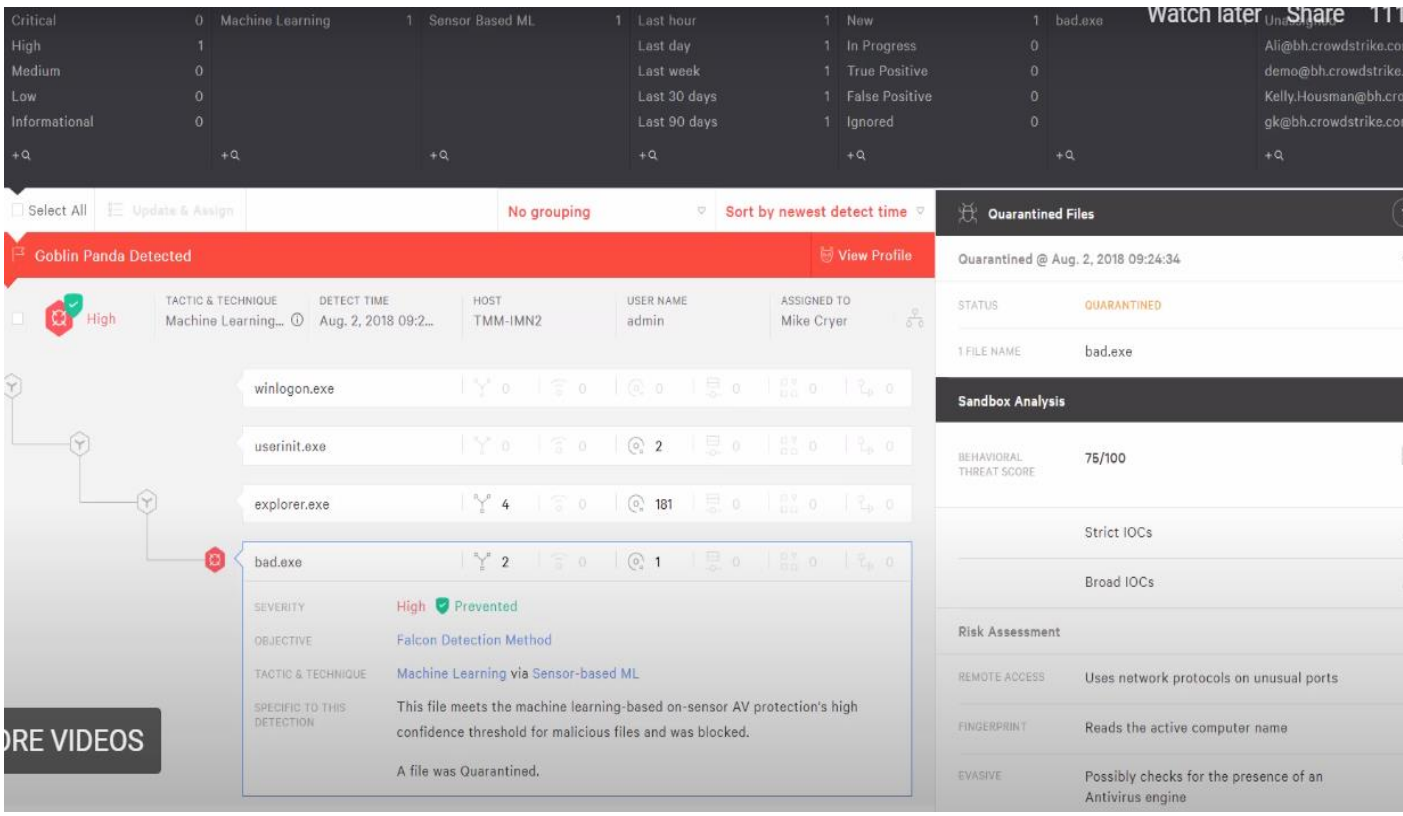
In this report it will shows the advantages of automation of threat intelligence with the Falcon X When the falcon is installed in the organisation endpoints as an example when a user had received a .bat file and they downloaded and tried to open the .bat file then we will be receiving the notification stating that it is blocked since there is some malicious activities has identified. Falcon X will act like as an antivirus tool so that no extra amount has been invested for the procuring addition antivirus tools and scanning report with respect to the report generated from the antivirus tools (Scobey, 2019).



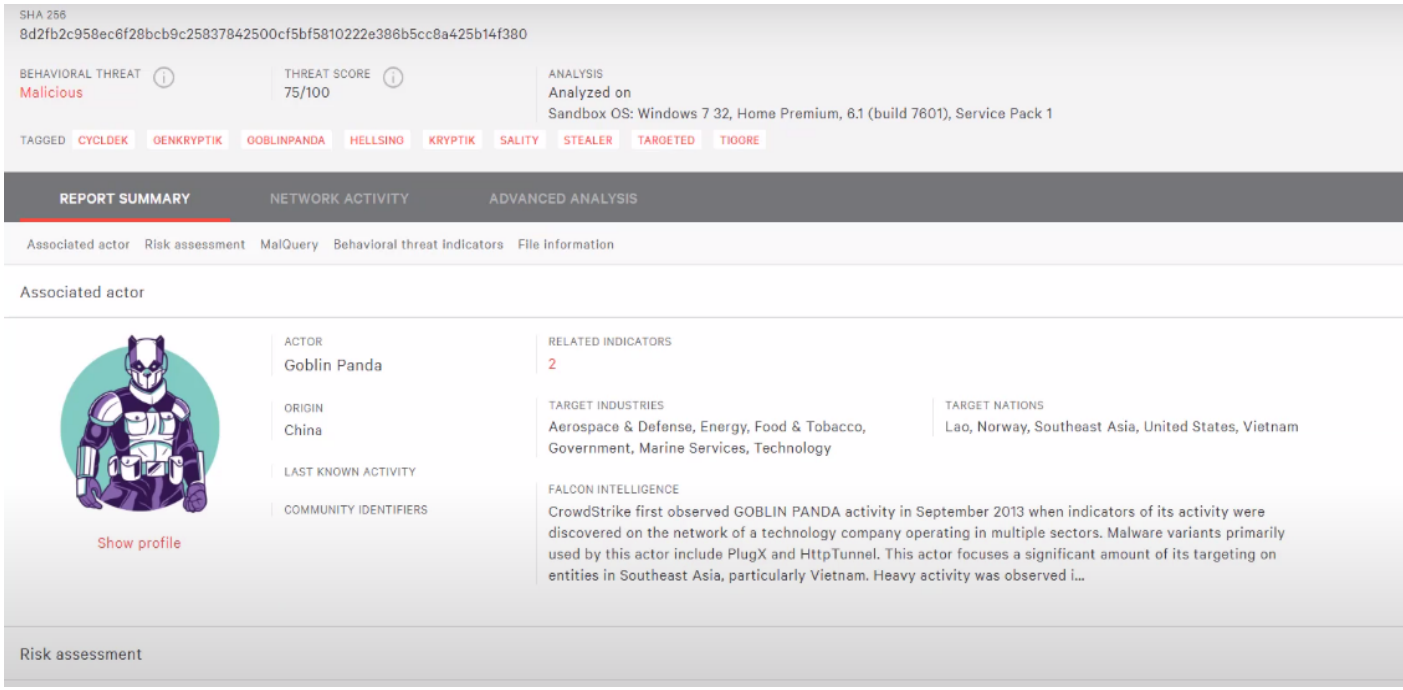
There is a feature available in Falcon interface for security threat analysis option wherein it will show as in description why this file has been blocked. And the respective filed has been quarantine with the help of falcon. Also, Falcon will act as an antivirus tool.

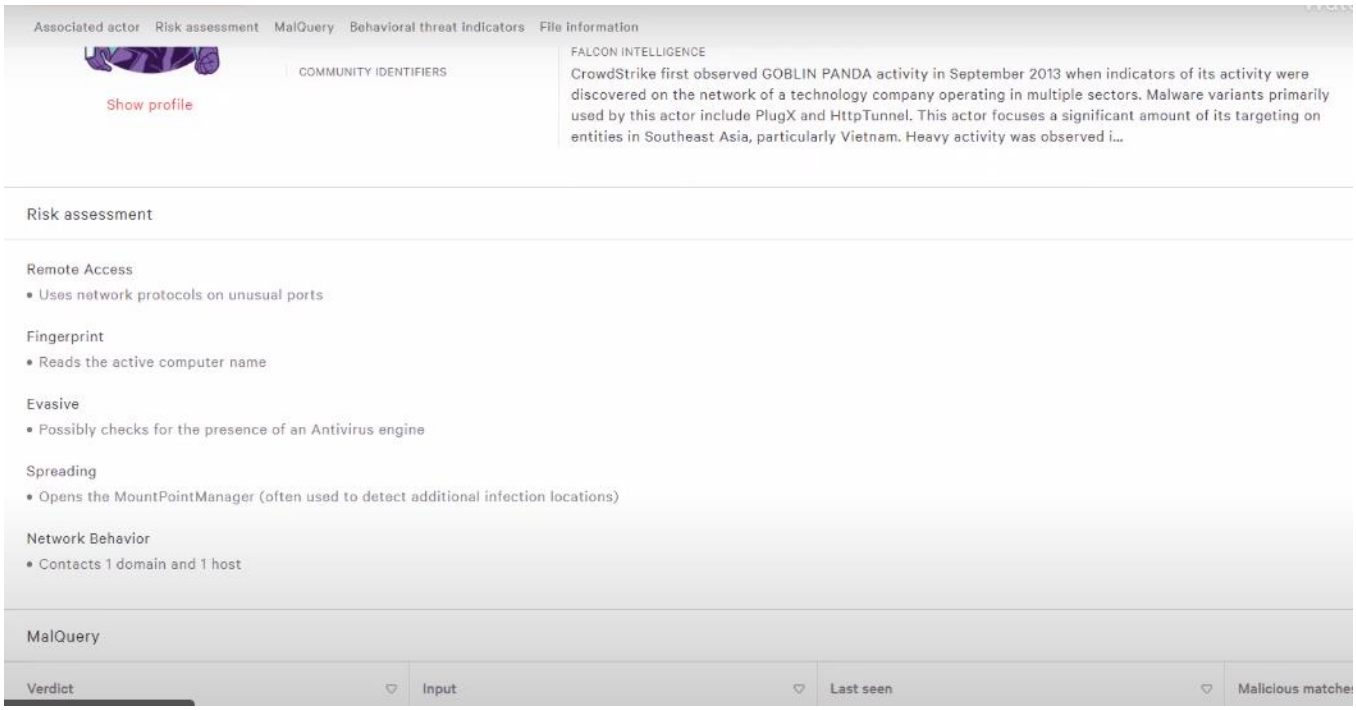


As a next step the quarantine file has been sent to the sandbox for the detailed investigation and the risk assessment.

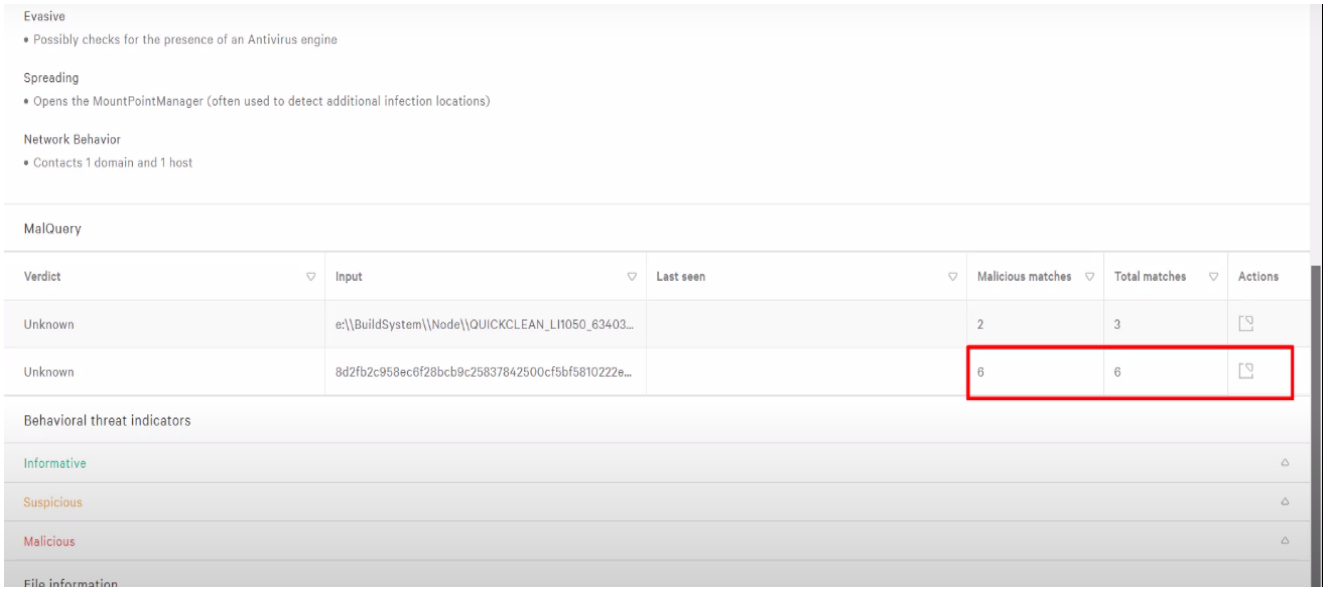


From the Sandbox analysis we will be getting the detailed information with the help of Falcon X. It will describe what are all the activities been done in the various organisation sectors and a detailed risk assessment analysis.

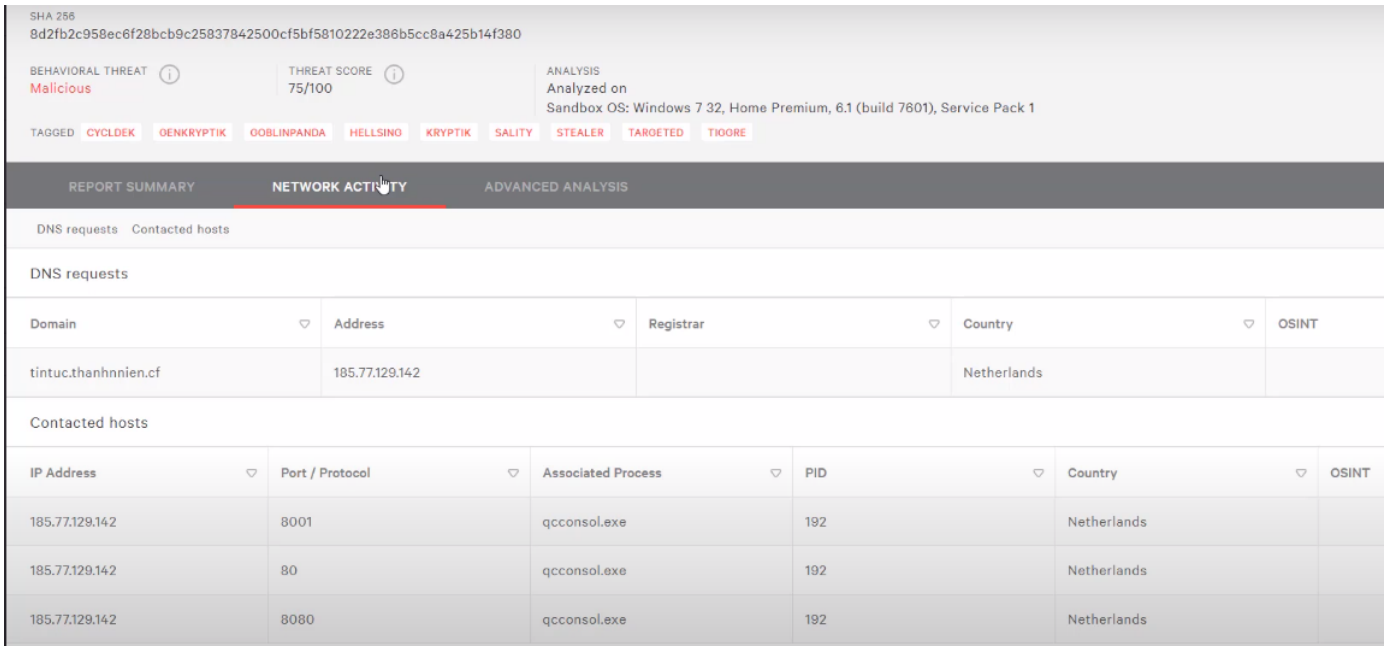




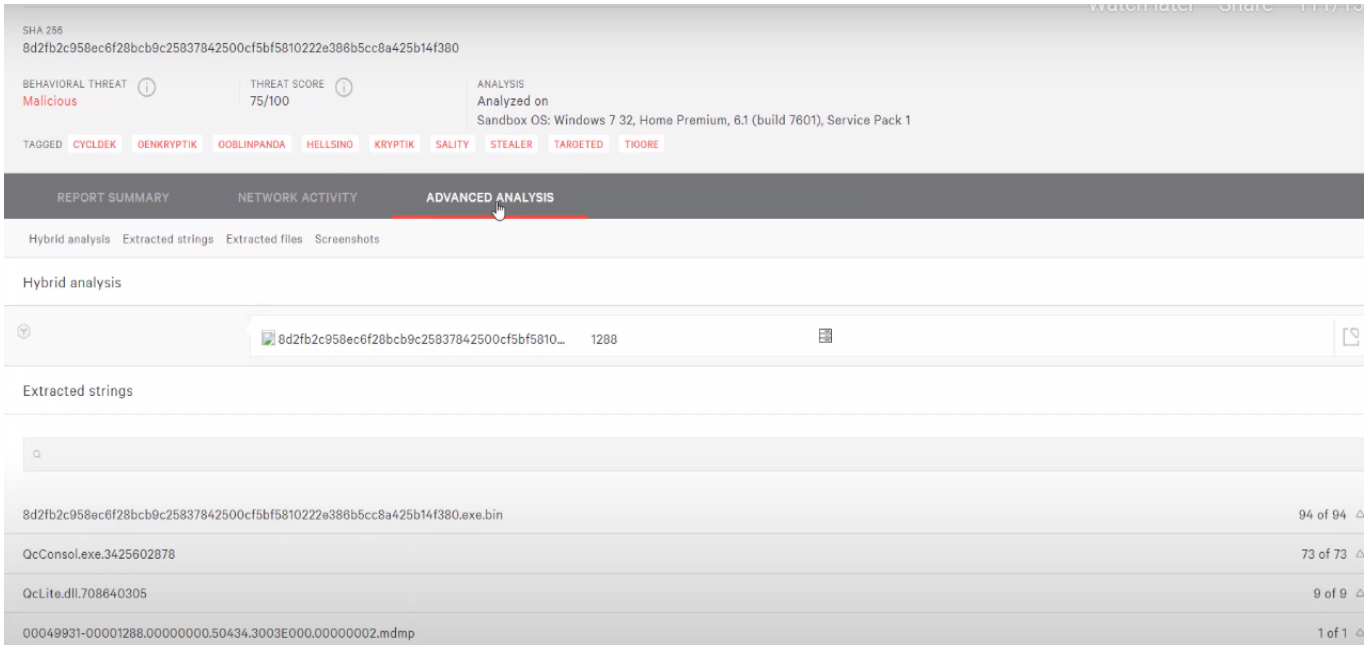
There is a tab showing the various types of behavioural threat indicators like informative, malicious and suspicious also under the Malicious tabs it has indicated as 6 matches.



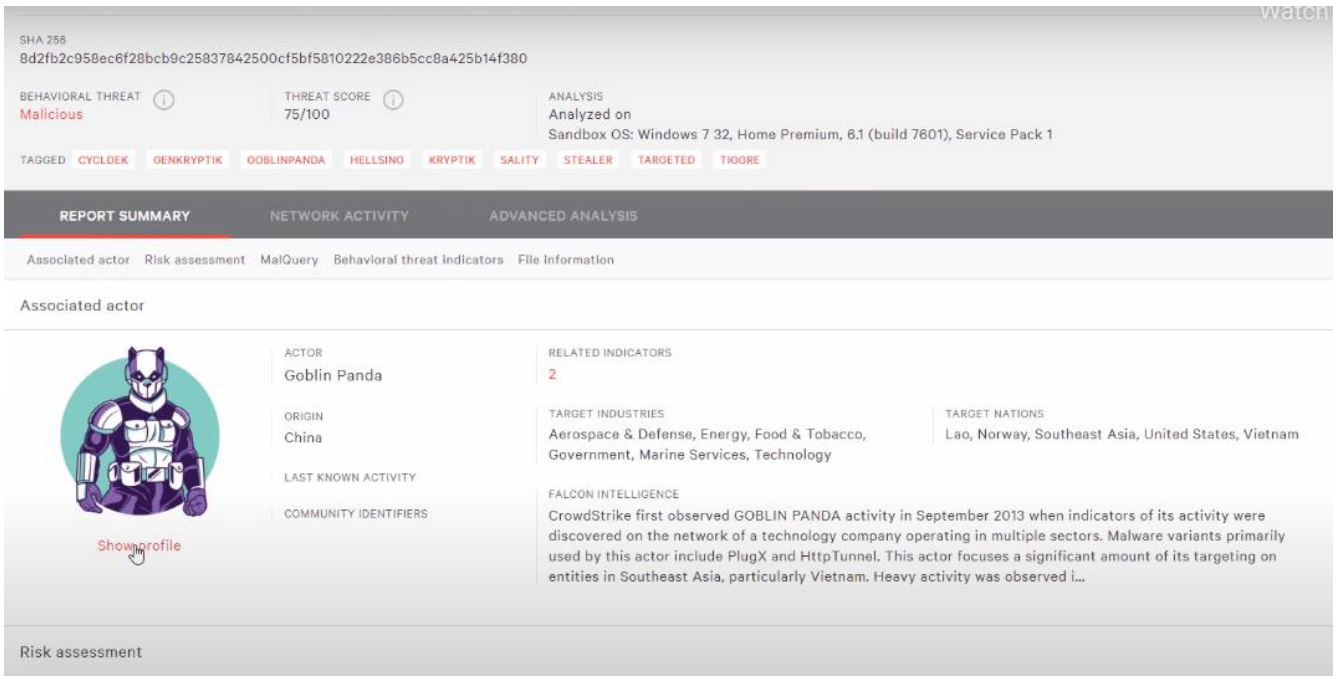
When we do the network activity analysis, we can find that it has started the communication with the external IP by using this information we can identify which are all the devices are contacted and also, we can block it from the network end and we can improve the security feature.

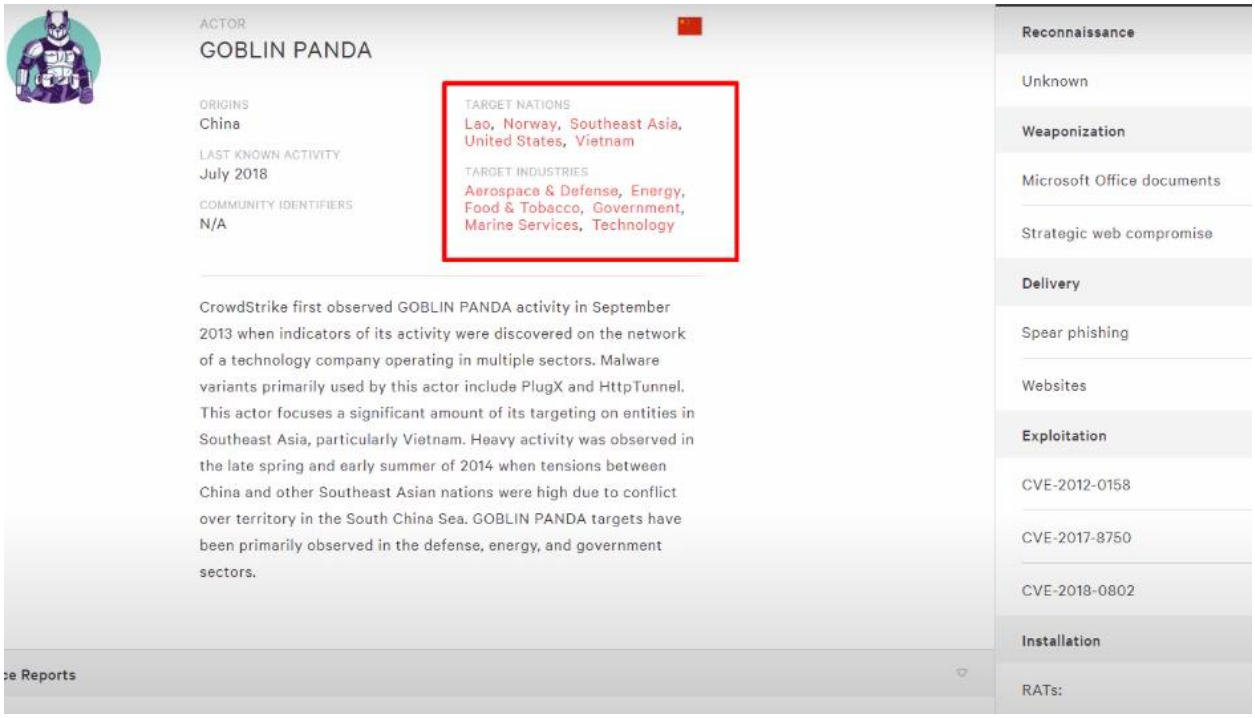


Finally, we can go through the advanced analysis where it will show as a hybrid analysis and extracted strings.

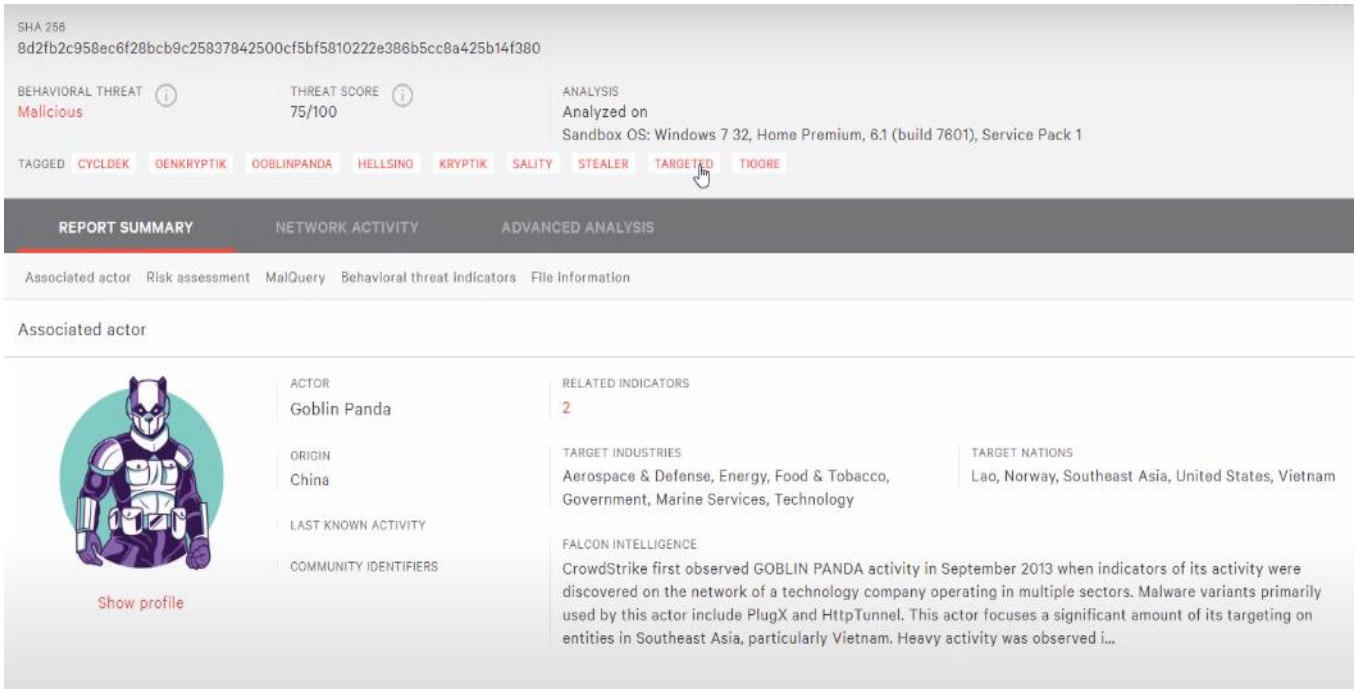


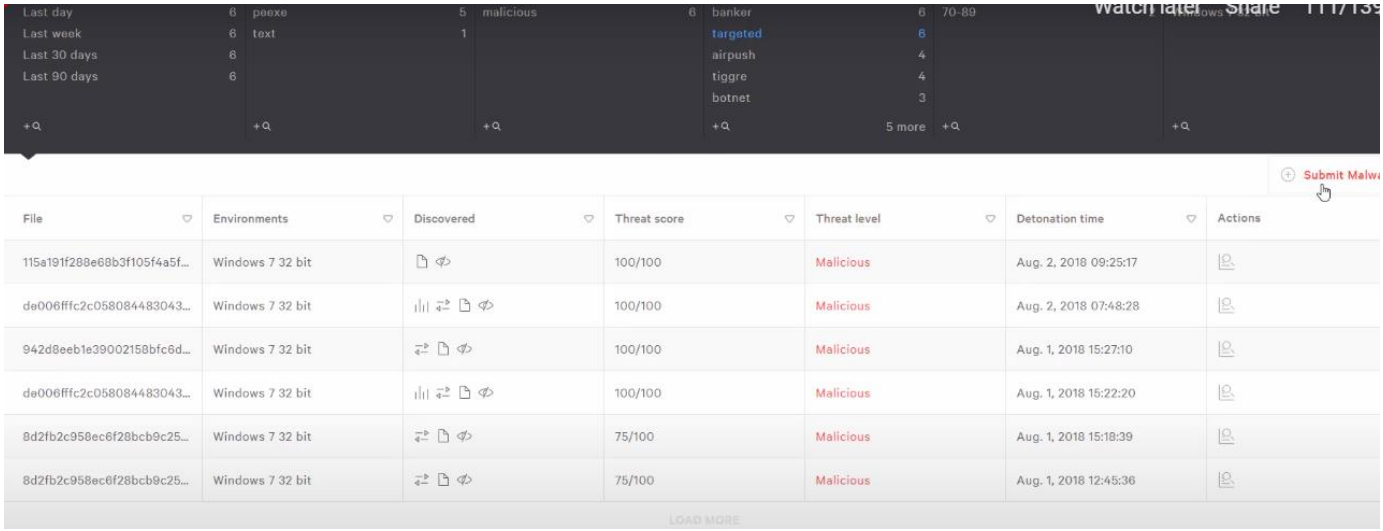
By clicking on “Show profile” it will give as detailed information of the hacker who and where is the targeted place and organisation. As per the CVE code mentioned in the screenshot, we can update the required patches and in order to protect the devices in future attacks.



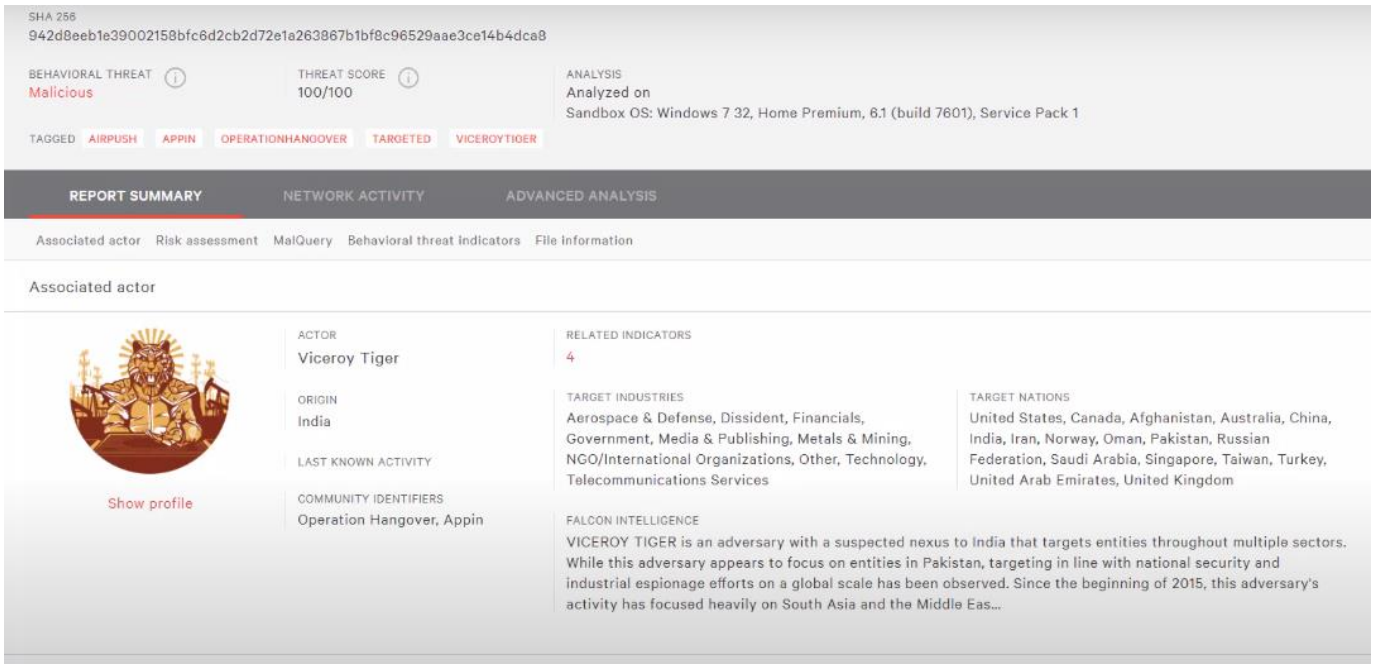


We can use the targeted tab to understand in detail about the attacks and it will check in the database about the various types of targeted attacks. From the second screen we can perform the two types of analysis. As a primary step we can submit malware analysis so that it will shows as a sandbox analysis report like which are all the hosts are connected and secondly, we will get a detailed report like who all tried to approach our environment.

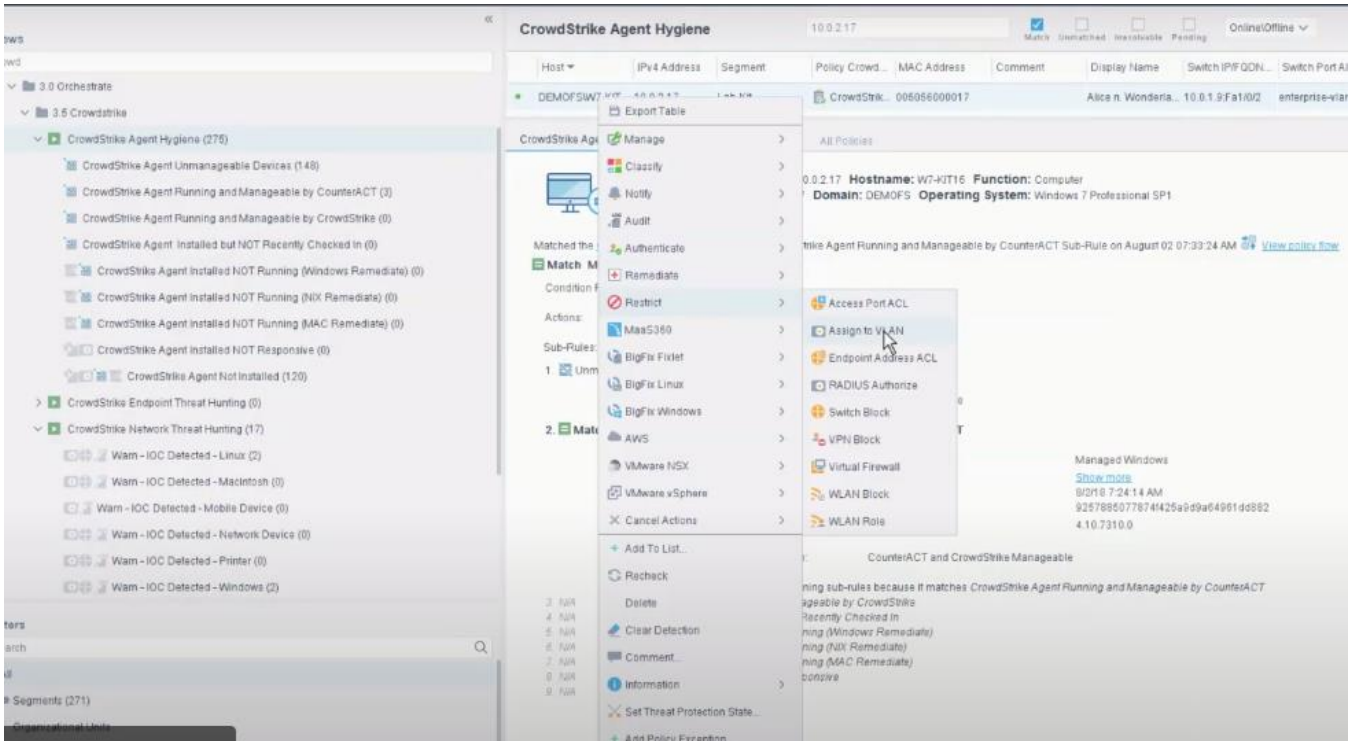


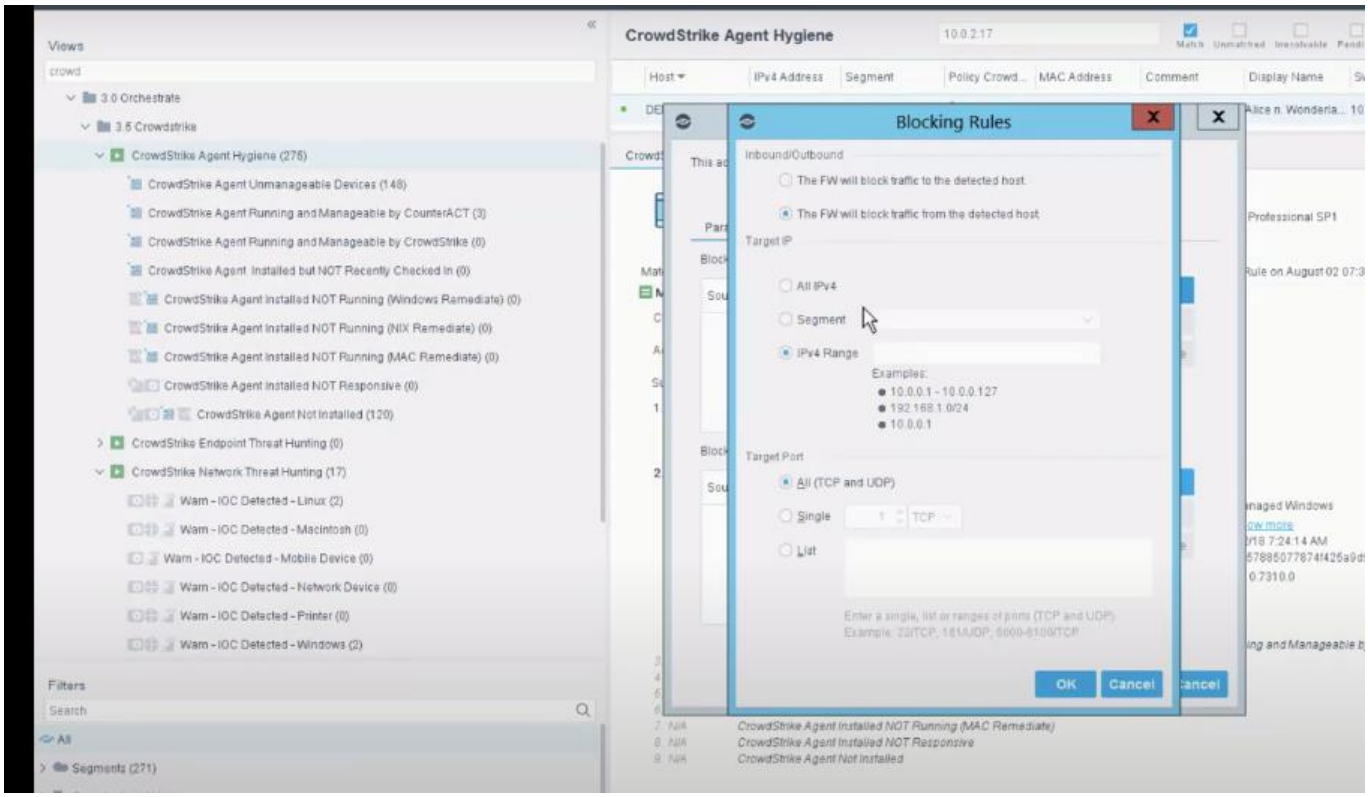


By selecting the reports under the “Actions” it will gives the detailed report like which are all the organisation has been targeted and where it is origin.



Coming back to the sandbox analysis, by downloading the IOC .csv file we can modified the Virtual firewall rules in order to protect these types of attacks in the firewall.

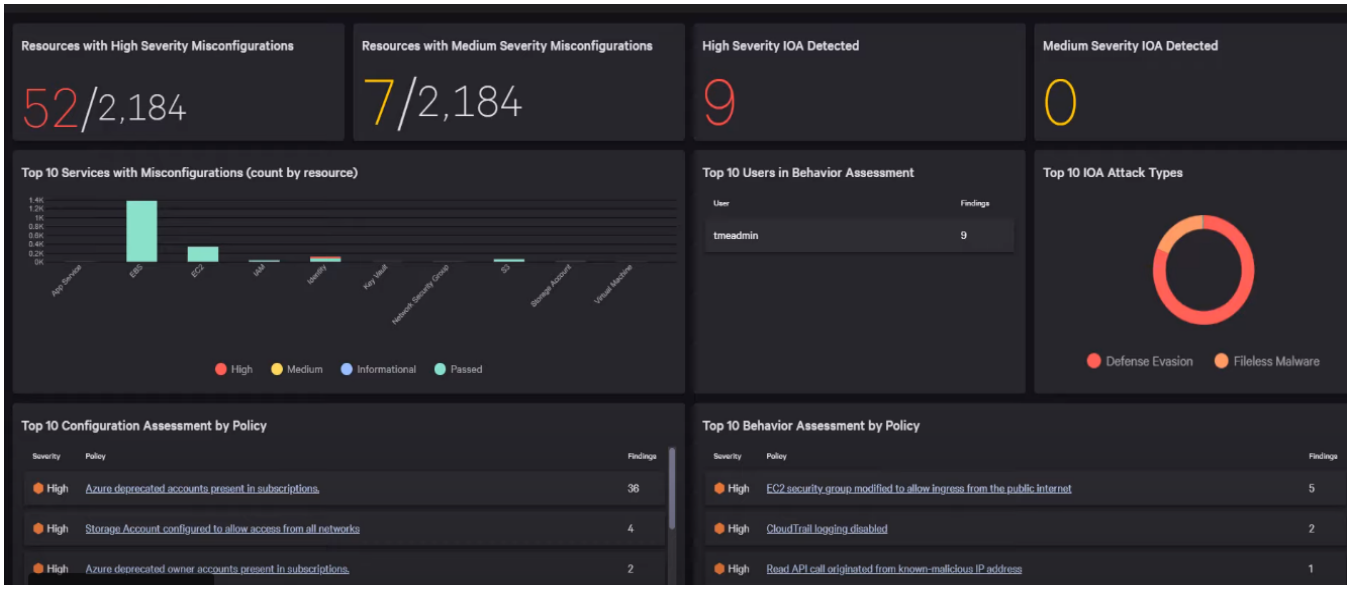




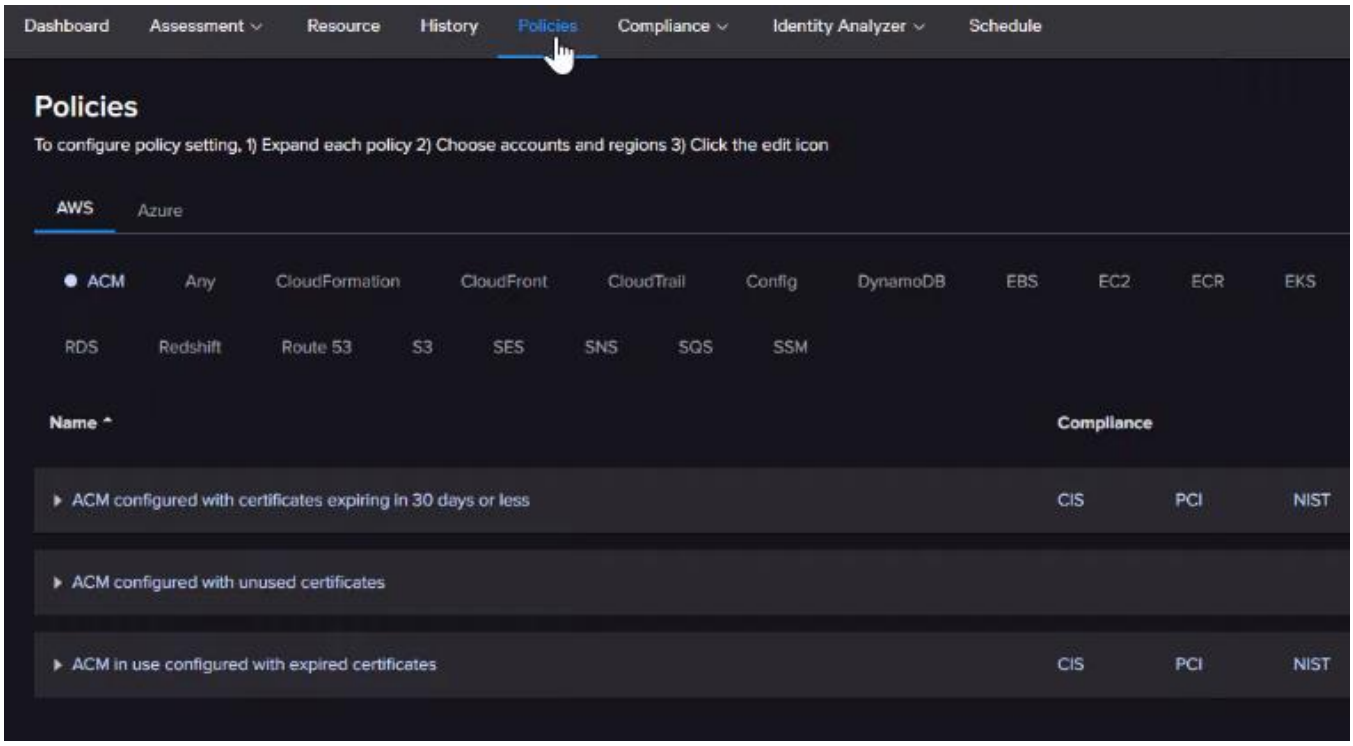
4.2 Crowdstrike – How to improve the cloud security by using the Crowdstrike

As a todays trend most of the organisation is moving to the cloud technologies so that lots of benefits are there like procurement cost reduces, energy consumption cost reduce, extra resource hiring reduce, no addition cost to give for the storage space. On the other hand, there are few risks also there but we can handle it by proper security measure are in place. So, cloud strike is a best tool for providing a better security in the cloud environment. Cryptojacking it will be a good target in the cloud environment. With the help of crowd strike the cloud environment will be continuously monitored in place of misconfiguration and also for any suspicious activity (Scobey, 2021).

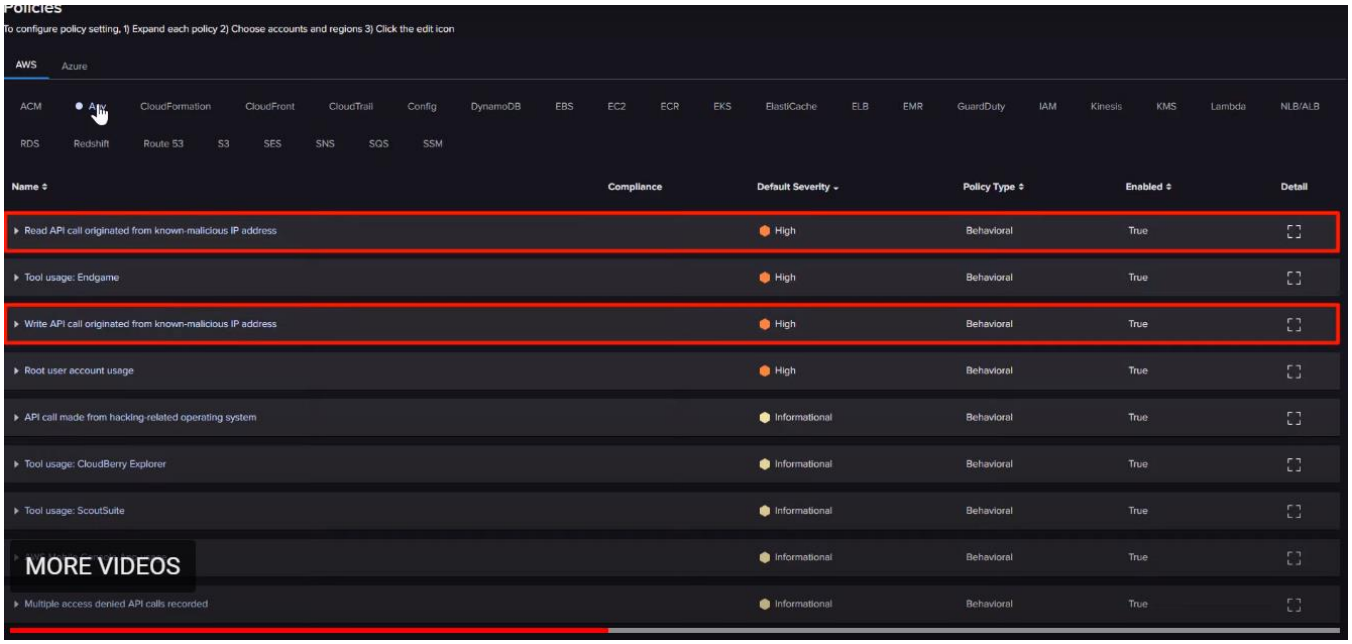
This tool will monitor the public cloud environment as a 24/7 and notify us if there is a suspicious activity has been carried out in the environment. This dashboard reports provided two types of information like which are all the clients are registered and secondly it will list out if any malicious activity has been identified in the cloud network.

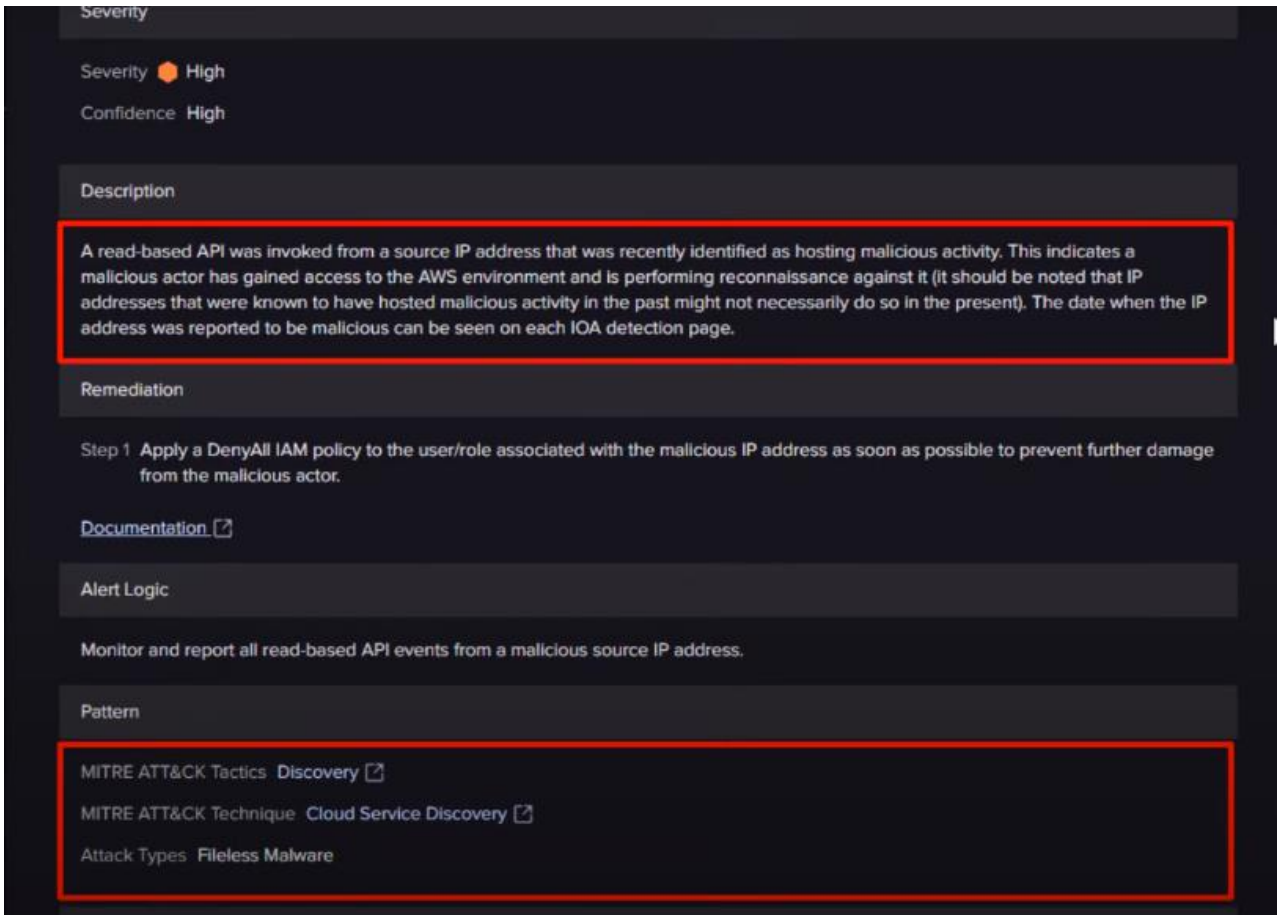


As per the policy we have set it will be continuously monitored

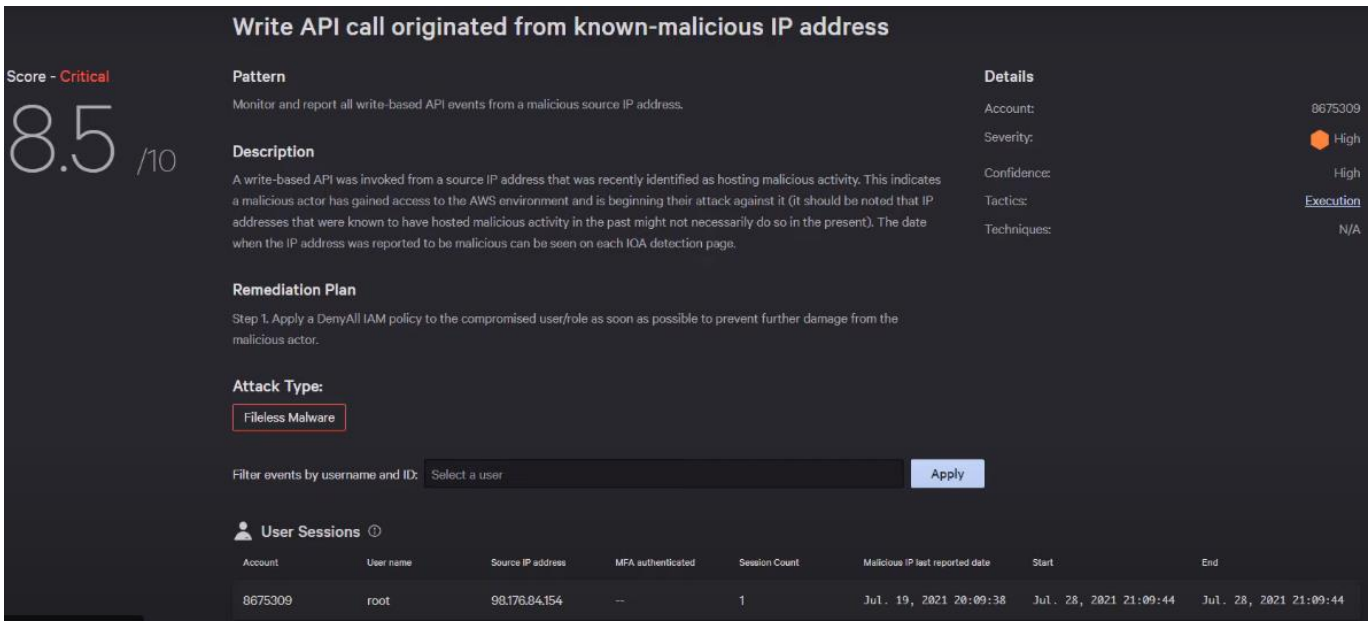


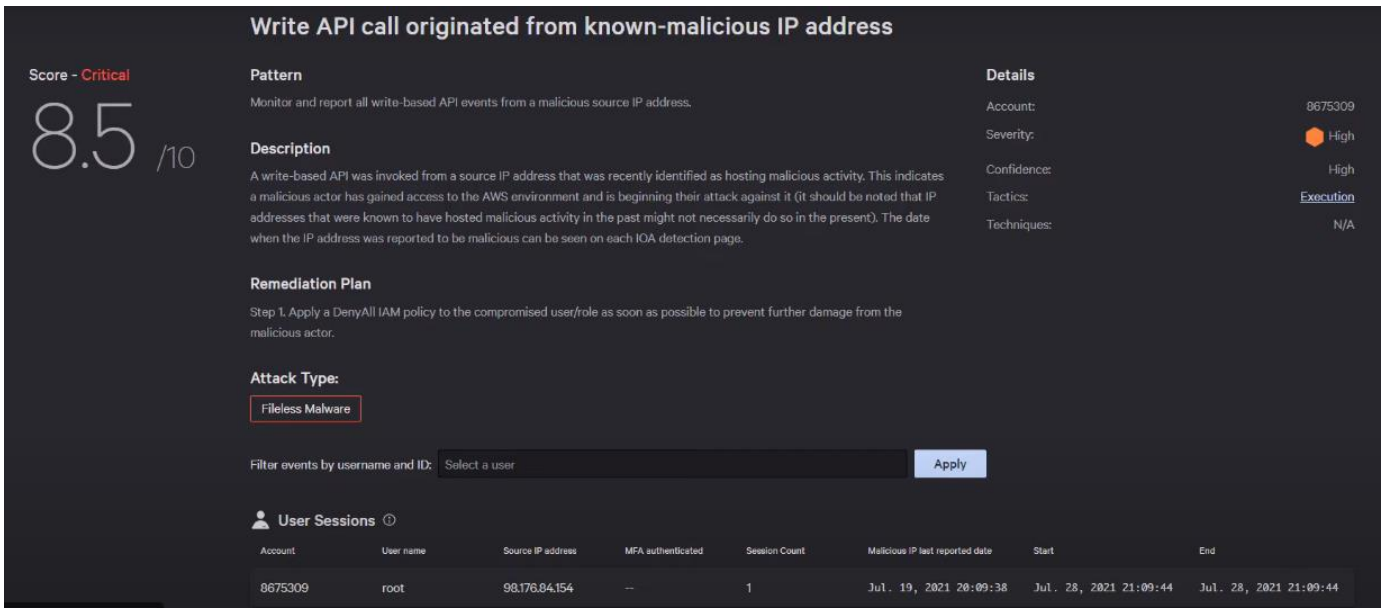
As per the public cloud provider we can set the policy, there is no limitation with the cloud service provider, if there are any behavioural changes happens it will be listed out. When we click on the “detail” it will explain the pattern of the attack, description of the attack and the mitigation plan.





With respect to the AWS provider it will list out the API call which is originated from the malicious IP address and the mitigation plan for blocking these types of attacks in future. It will show the credit score and what type of priority is for the effected malware also it will show the victims IP address.

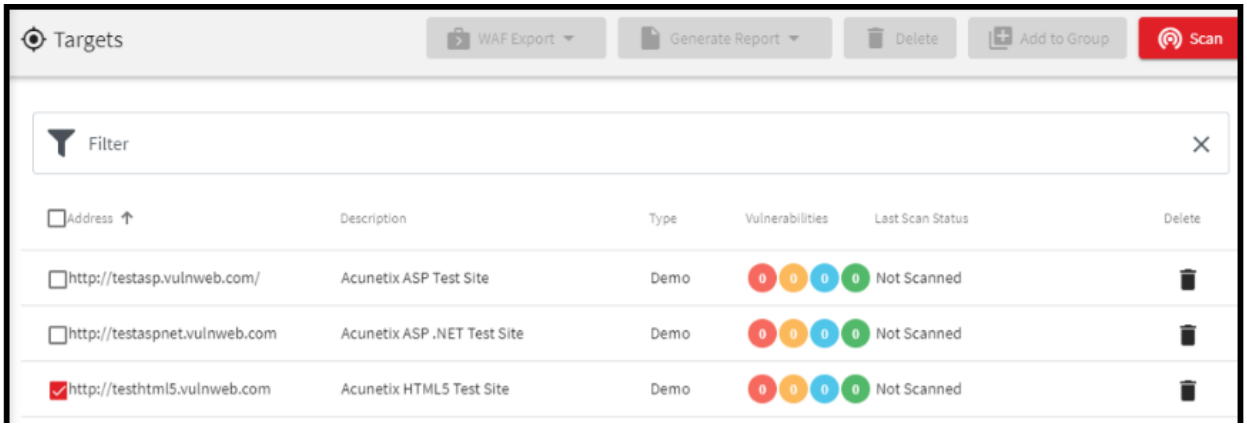




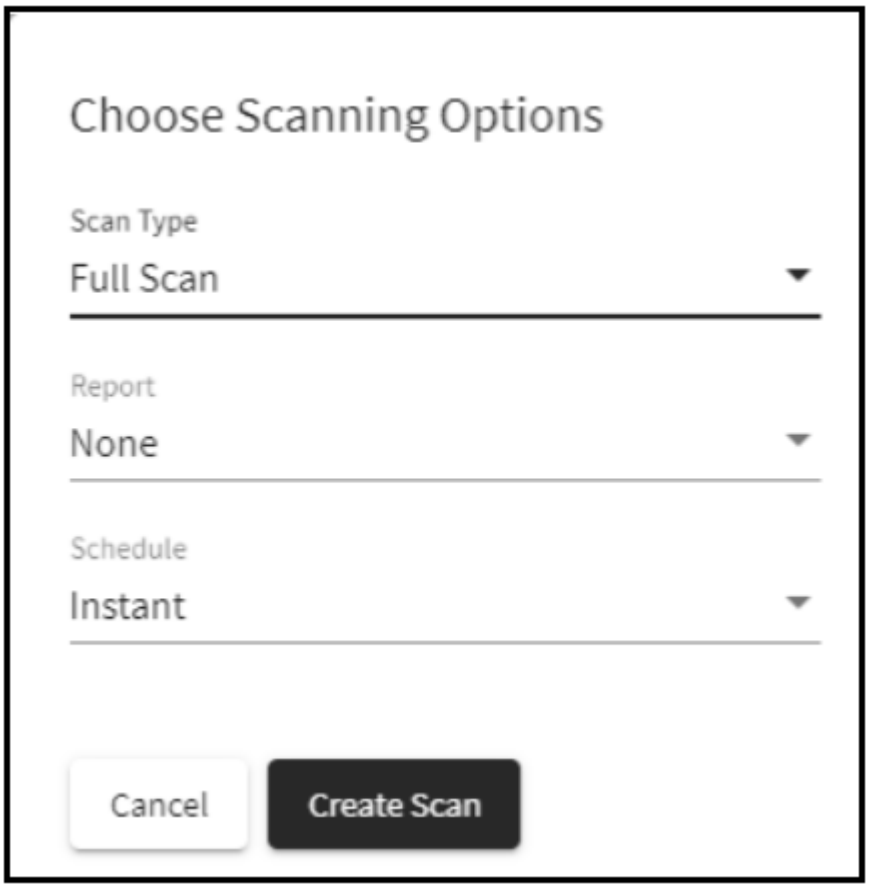
4.3 Acunetix – Launching Scans, Reviewing Scan Results and Managing Vulnerabilities

If you are not an authorised console administrator to perform the Acunetix scan run, you should inform to the authorised administrator. If we are performing a dual run from the multiple system then there might be a chance of websites to get crashed or restart. Once we set the target scan, we can start the scan for identifying the Vulnerability (Acunetix Support, n.d.).

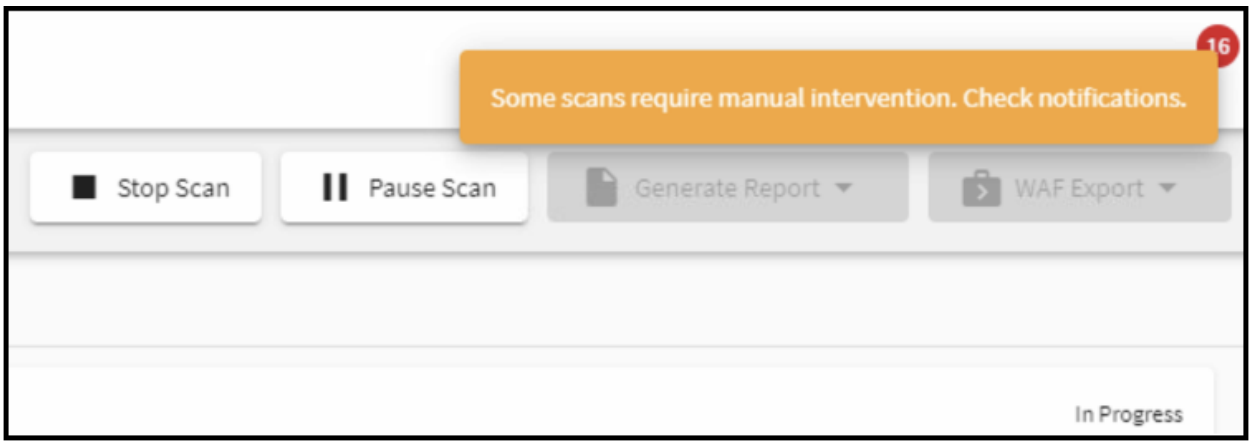
From the Below list we should select the target address and initiate the scan.



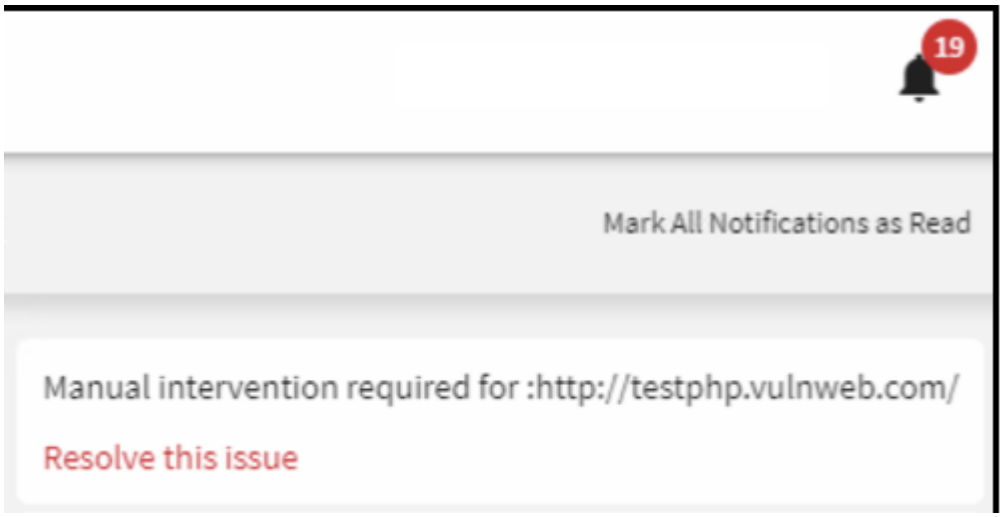
From the Scan option there is an option for “Scan Type”, “Report” and for Schedule”, then we can “create scan” accordingly as per the customer requirement.



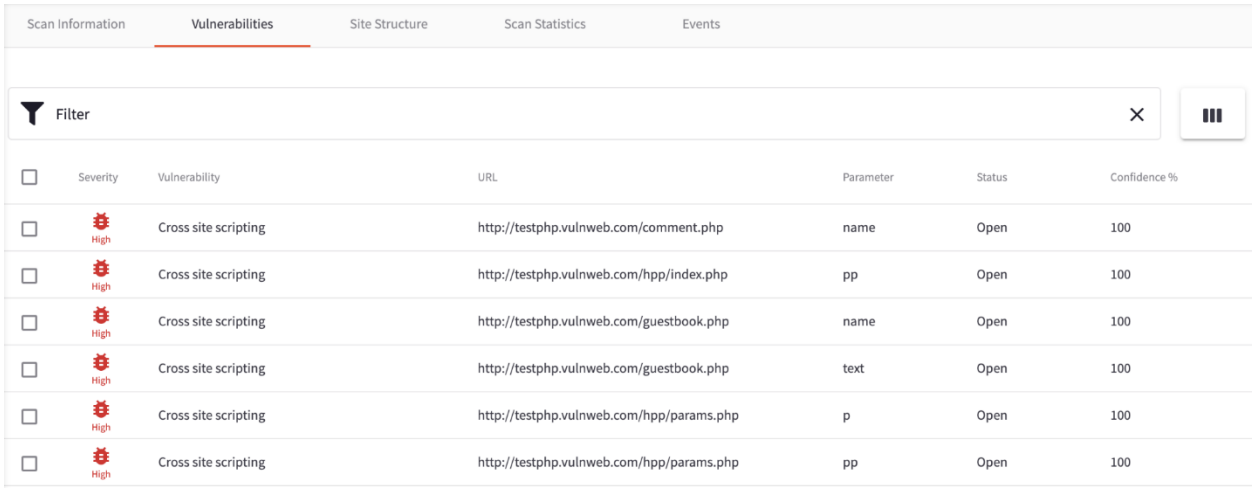
Most of the cases scanning would be like automated and sometimes there might user interventions be required where in web portal might be more secured then we need to provide the login user and password or two factor authentications for proceeding the scanning.



Sometimes notification pop up will come, in that case you need to click on “resolve this issue”

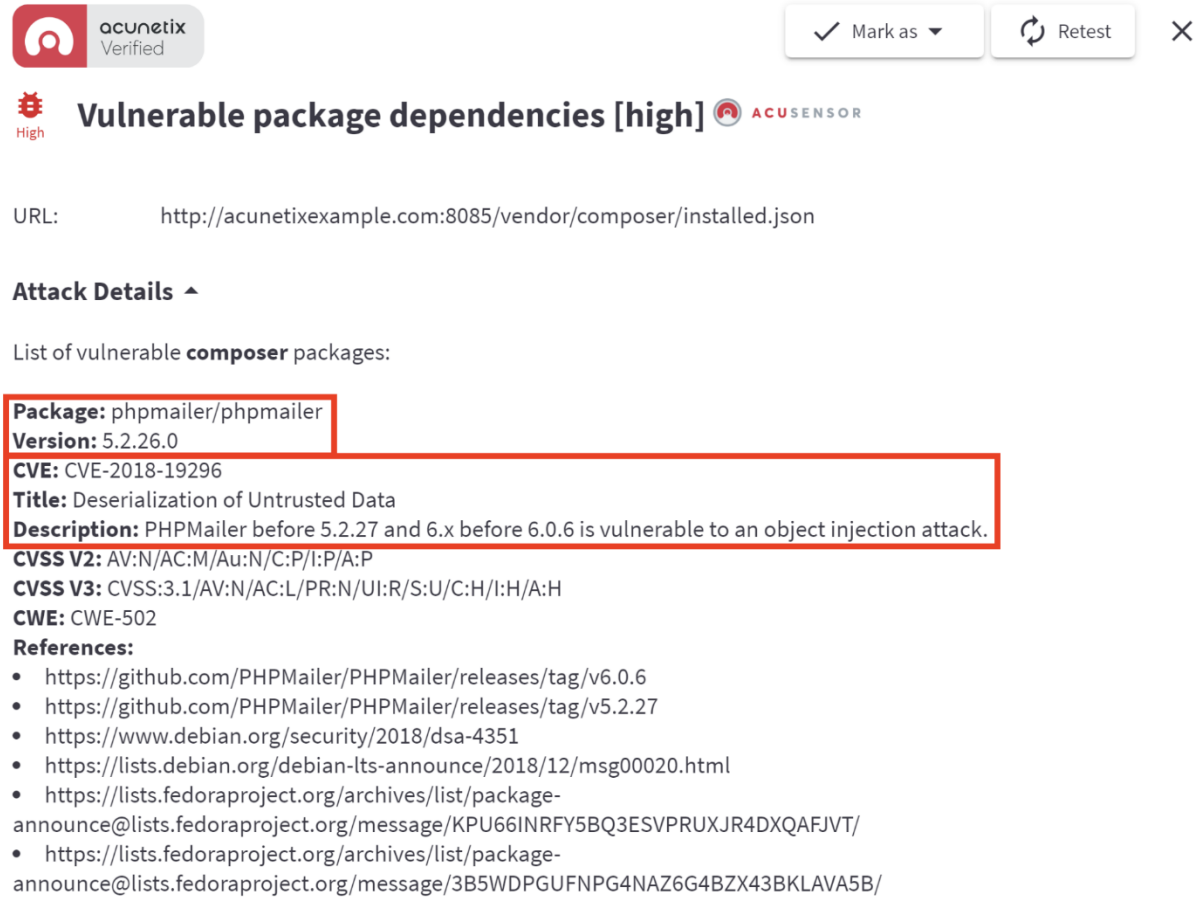


Once the scan is completed it will show the below mentioned window with vulnerability has been identified and with the severity.

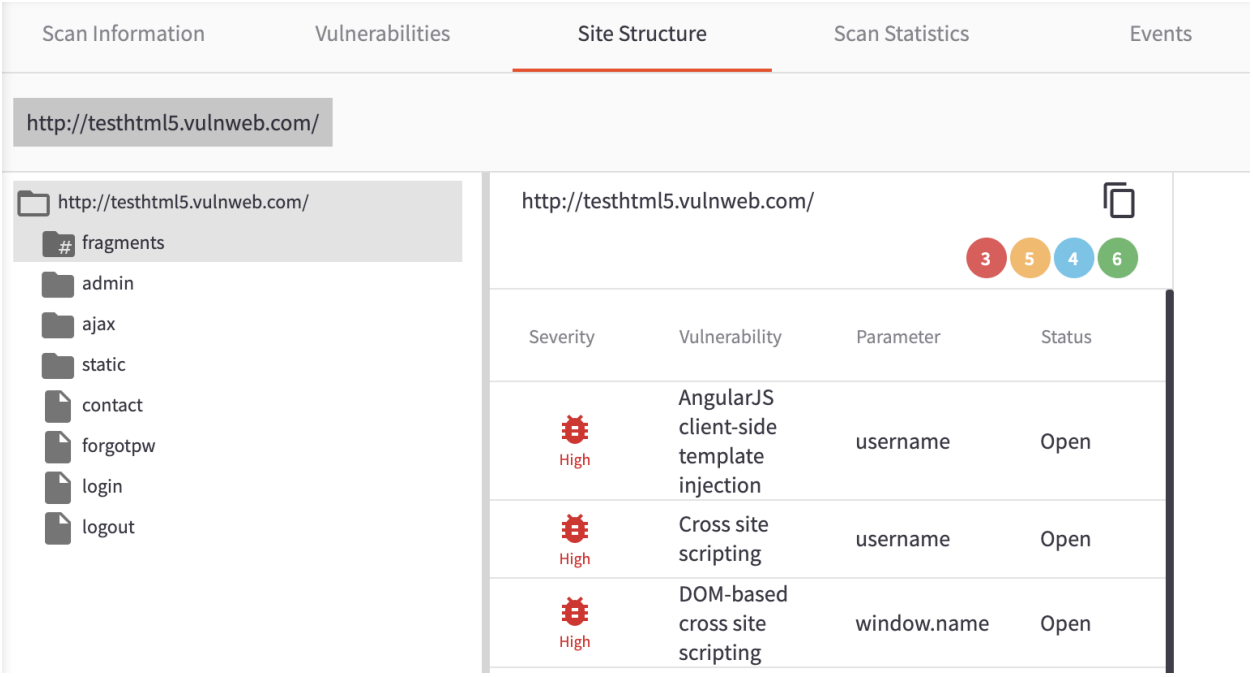


Severity	Vulnerability	URL	Parameter	Status	Confidence %
High	Cross site scripting	http://testphp.vulnweb.com/comment.php	name	Open	100
High	Cross site scripting	http://testphp.vulnweb.com/hpp/index.php	pp	Open	100
High	Cross site scripting	http://testphp.vulnweb.com/guestbook.php	name	Open	100
High	Cross site scripting	http://testphp.vulnweb.com/guestbook.php	text	Open	100
High	Cross site scripting	http://testphp.vulnweb.com/hpp/params.php	p	Open	100
High	Cross site scripting	http://testphp.vulnweb.com/hpp/params.php	pp	Open	100

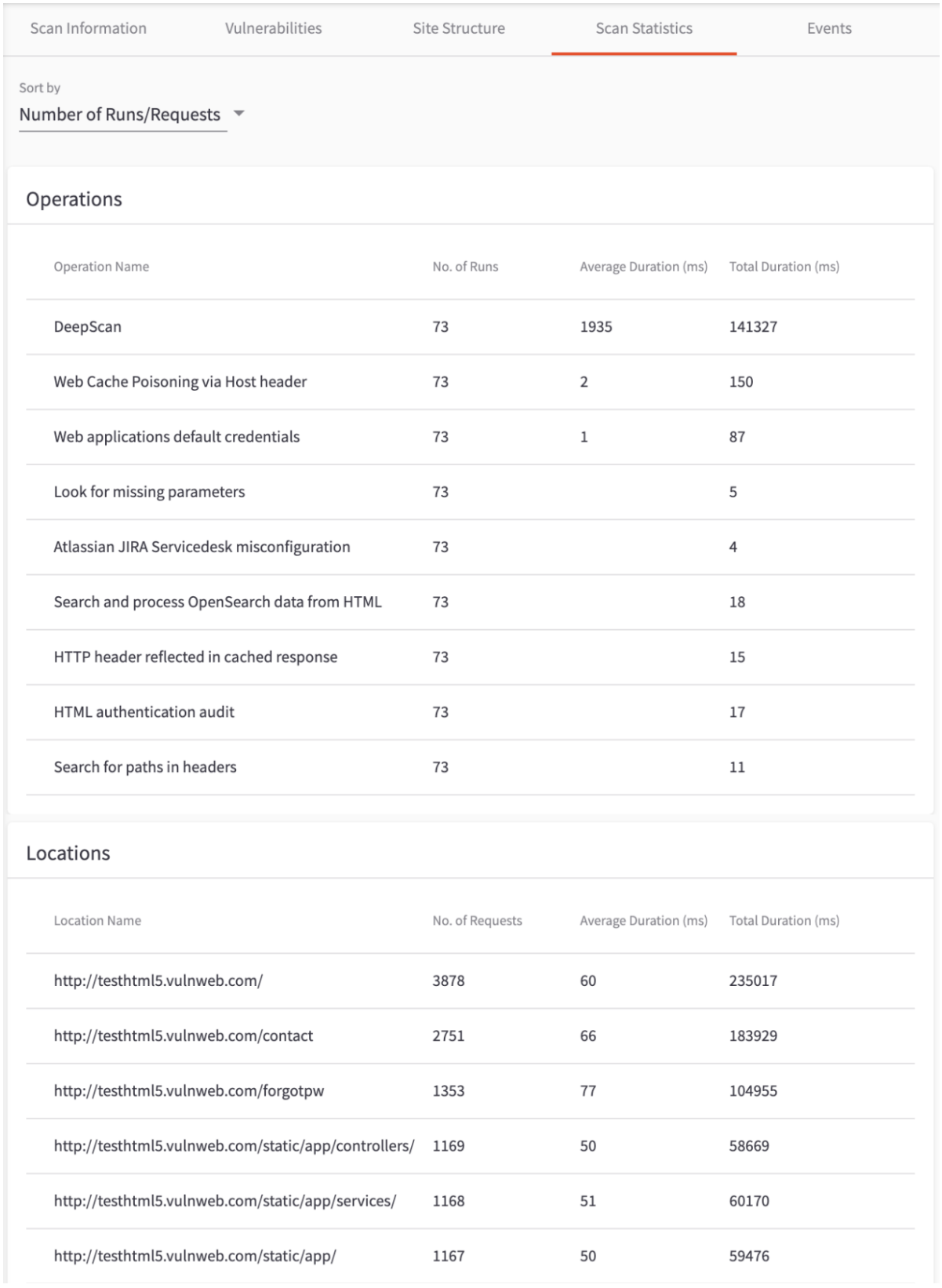
We can view the detailed vulnerability by selecting each vulnerability.



Site structure can he used for listing all the sites which has been scanned and it will list out the vulnerability as per the folders structure. Under “fragments” folder it will list out which are all the URL are tested.



Scan statistics tab list out the “operations” like various types of scanning has been performed and duration. “Locations” tab denotes the how many times scanning has been performed and duration of the URL scanned.



Scan Information | Vulnerabilities | Site Structure | Scan Statistics | Events

Sort by: Number of Runs/Requests

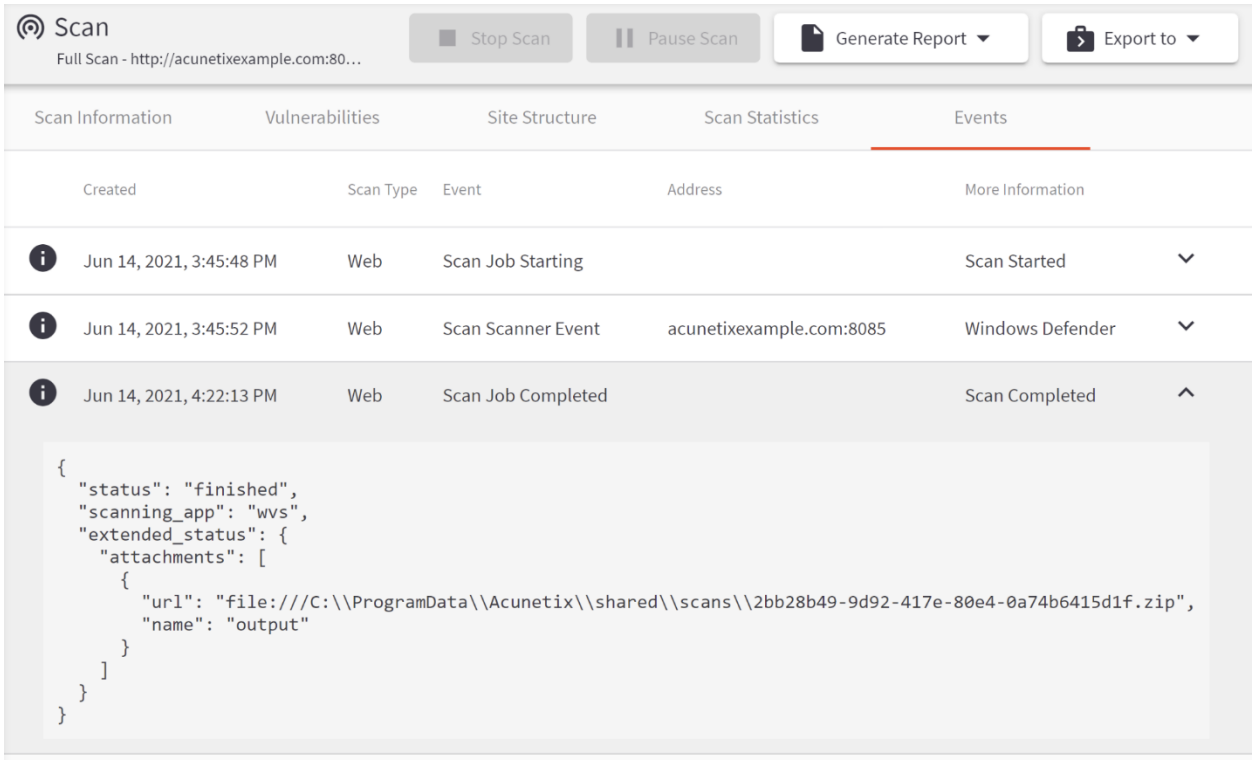
Operations

Operation Name	No. of Runs	Average Duration (ms)	Total Duration (ms)
DeepScan	73	1935	141327
Web Cache Poisoning via Host header	73	2	150
Web applications default credentials	73	1	87
Look for missing parameters	73		5
Atlassian JIRA Servicedesk misconfiguration	73		4
Search and process OpenSearch data from HTML	73		18
HTTP header reflected in cached response	73		15
HTML authentication audit	73		17
Search for paths in headers	73		11

Locations

Location Name	No. of Requests	Average Duration (ms)	Total Duration (ms)
http://testhtml5.vulnweb.com/	3878	60	235017
http://testhtml5.vulnweb.com/contact	2751	66	183929
http://testhtml5.vulnweb.com/forgotpw	1353	77	104955
http://testhtml5.vulnweb.com/static/app/controllers/	1169	50	58669
http://testhtml5.vulnweb.com/static/app/services/	1168	51	60170
http://testhtml5.vulnweb.com/static/app/	1167	50	59476

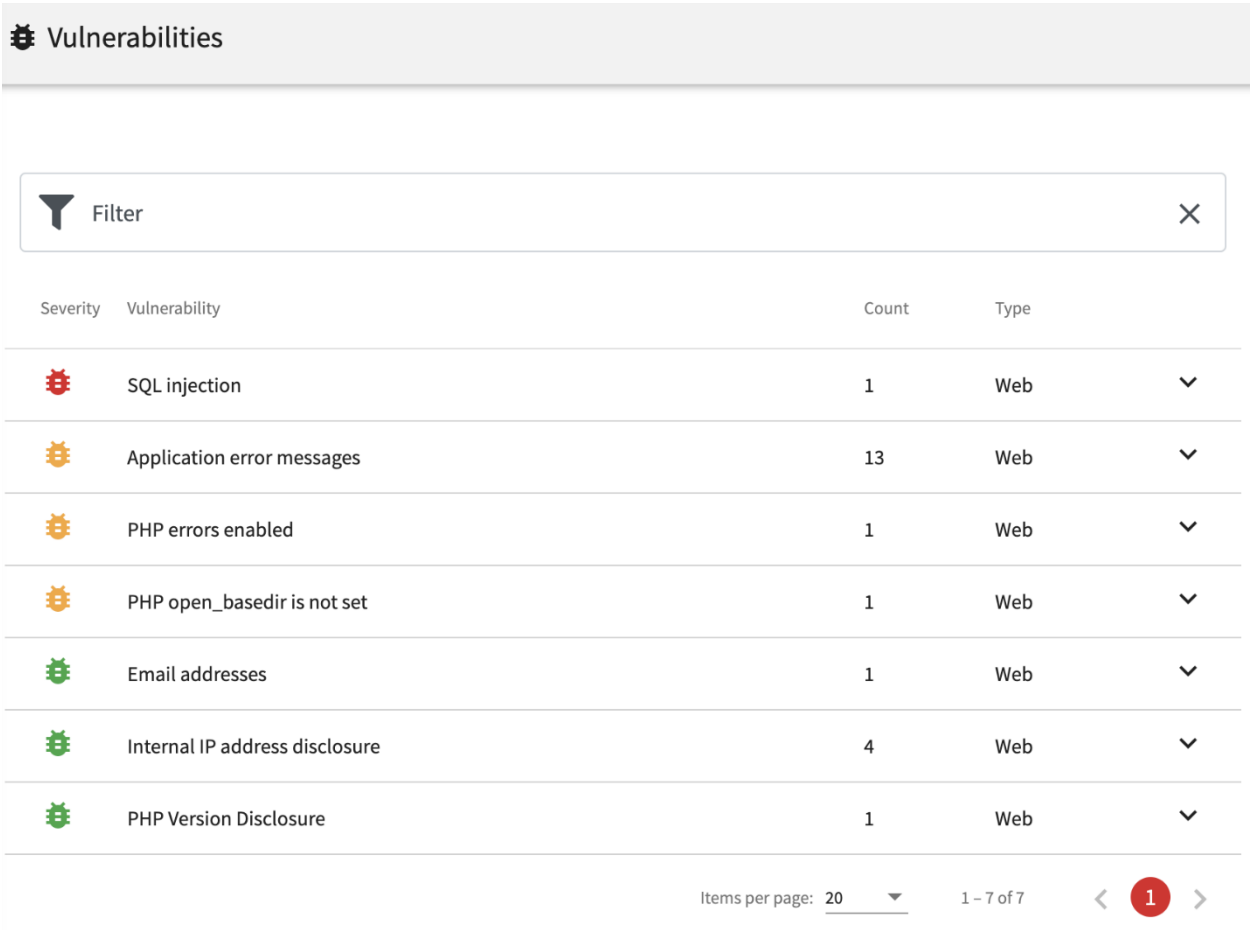
Events tab shows scanning start time and end time and also if at all any error occurs during the scanning time.



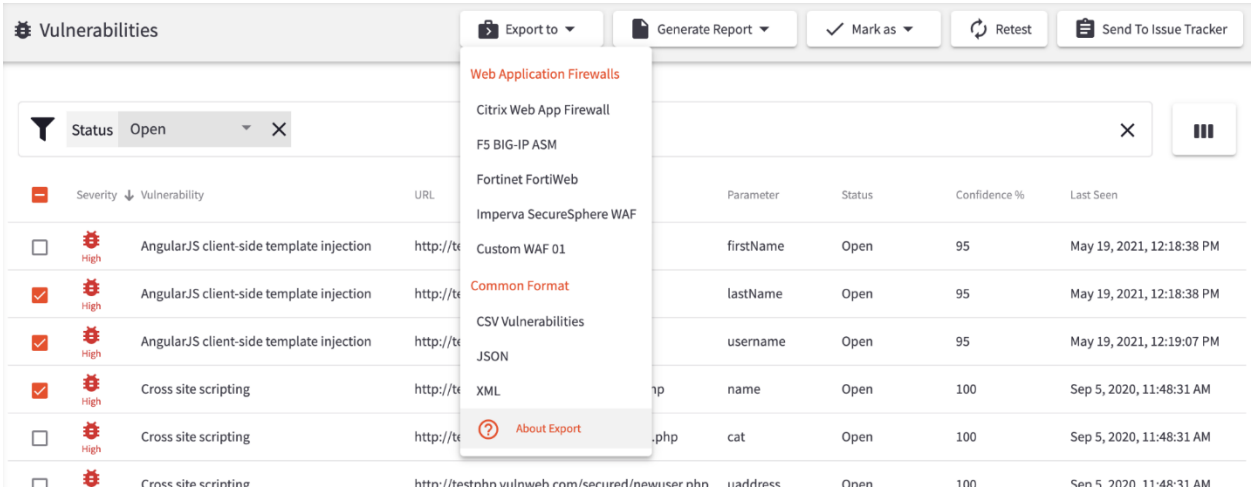
Once the vulnerabilities are identified it has been categorised into 4 different types as mentioned below

- **Level 3 heigh Risk:** It is a heigh risk of getting the cyber-attacks for data theft.
- **Level 2 Medium Risk:** Where in this risk is caused by the misconfiguration in server which may cause the server into the intrusion and disruption.
- **Level 1 Medium Risk:** Vulnerabilities may cause of data encryption and necessary patches has been updated.
- **Alert Information:** It is just like the information which has been disclosed like IP address, email address which may intended to cause the security breach.

Vulnerabilities are identified we have to fix it by securing the web applications. And the vulnerability has been listed down as per the priority level and fix it by using the Acunetix.



If we patching the vulnerability manually it may be taking days to fix it, by using the feature known as Web Application Firewall (WAF) available in Acunetix. We can export the vulnerability into Acunetix an imported into WAF we can virtually patch the respective vulnerability.

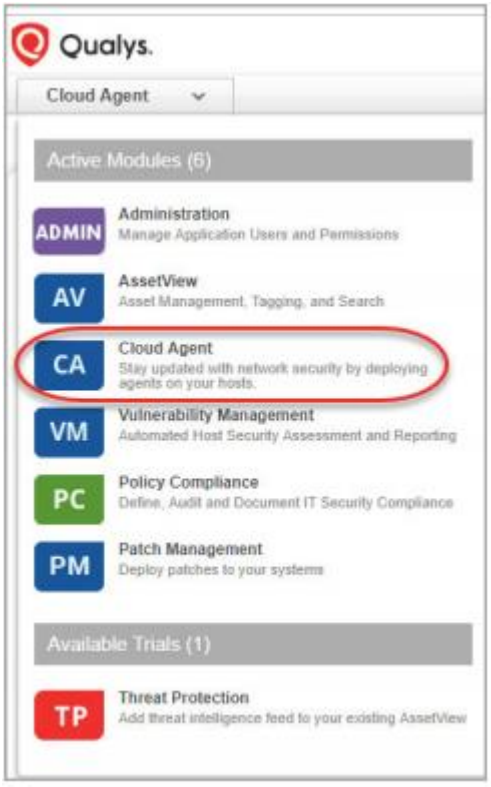


Once the Vulnerability is fixed, we can retest the vulnerability by using the “Retest option” and then we can re ran the new scan by customising the profiles for the corresponding vulnerability and we can get the confirmation results.

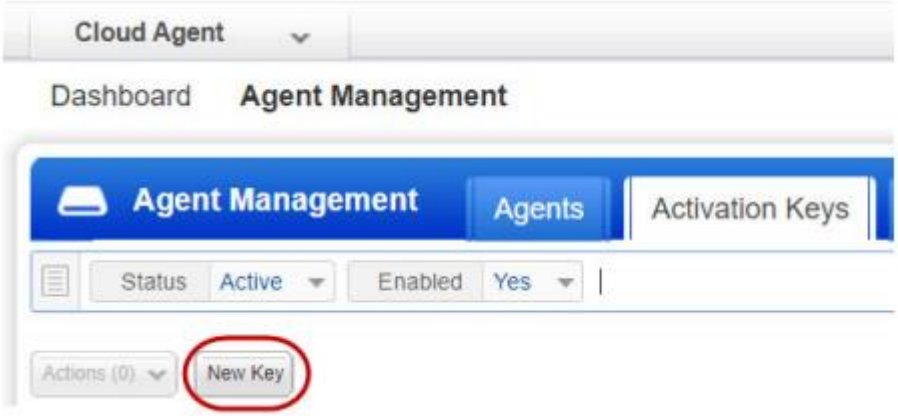
4.4 Qualys – Patch Management

Qualys patch management will keen monitor our infrastructure assets and if at all any vulnerabilities are identifies it will push patches and keep updated in terms of cyber-attacks. These automotive tools help us to consume the time for the patch deployment in Linux and Windows machines. Also, it will help us to view the real-time patches available and if at all any patches has been released after the Vulnerability assessment test it will pushes to the required machines. Windows and Linux agents will download the necessary patches from Internet and after authentication it will download and get it installed. However, Qualys patch management will analyse whether the required patches has been installed or not. Below snapshot shows like scanning of the assets and patching the devices if there are any latest patches are missing (Patch Management Getting Started Guide Version 1.5, 2021).

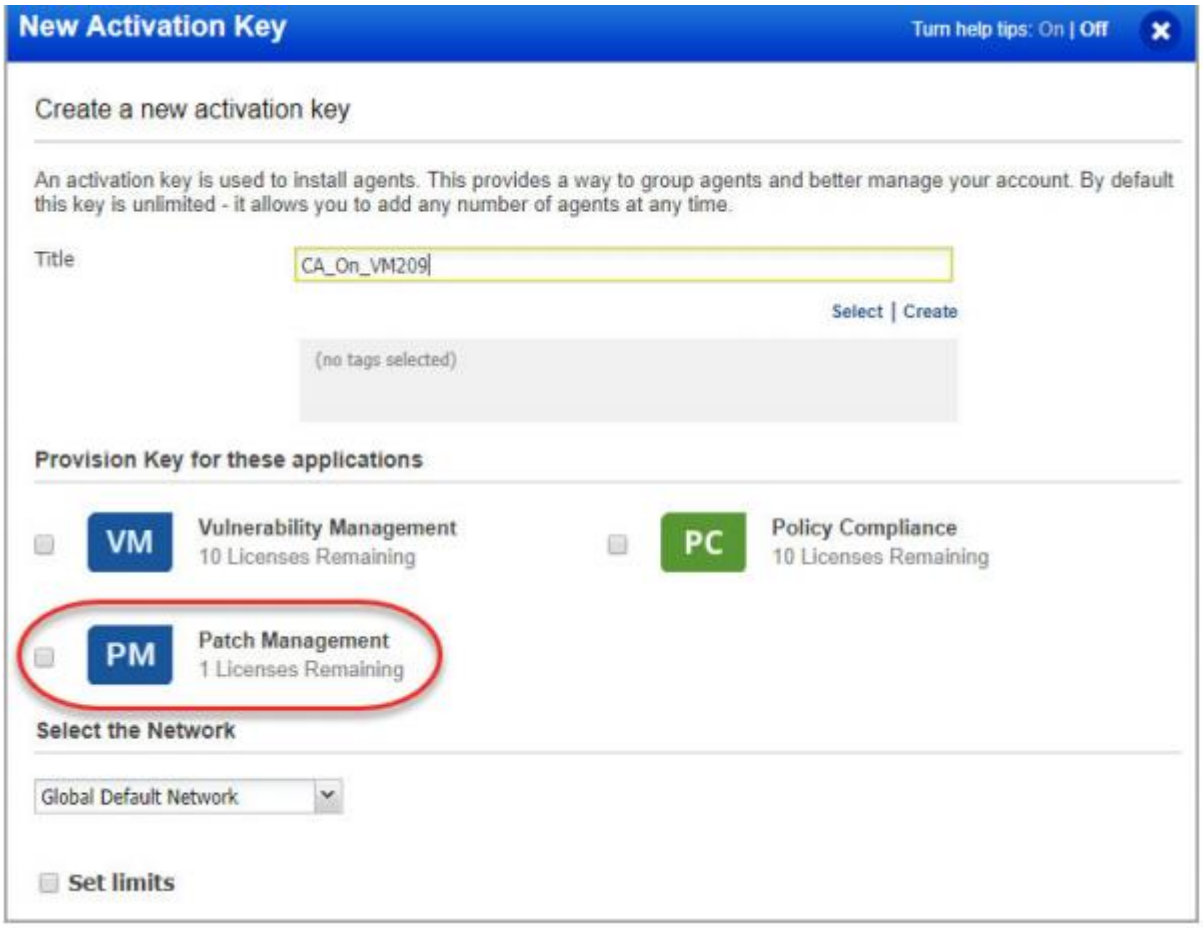
As a first step we need to download "cloud agent" from Qualys for patch deploying in windows and Linux machines. Cloud agent will be manging for the agent installation.



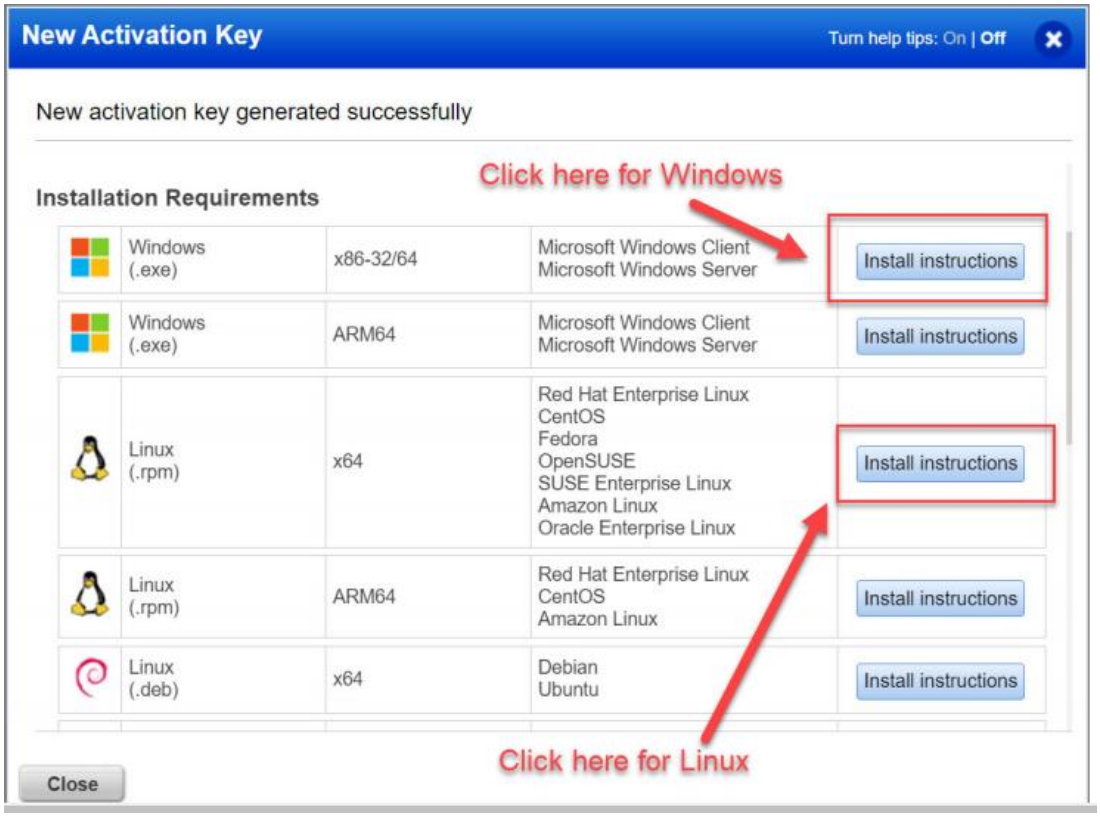
For creating and activation key. Activation key→new key→Title "Test"→Generate



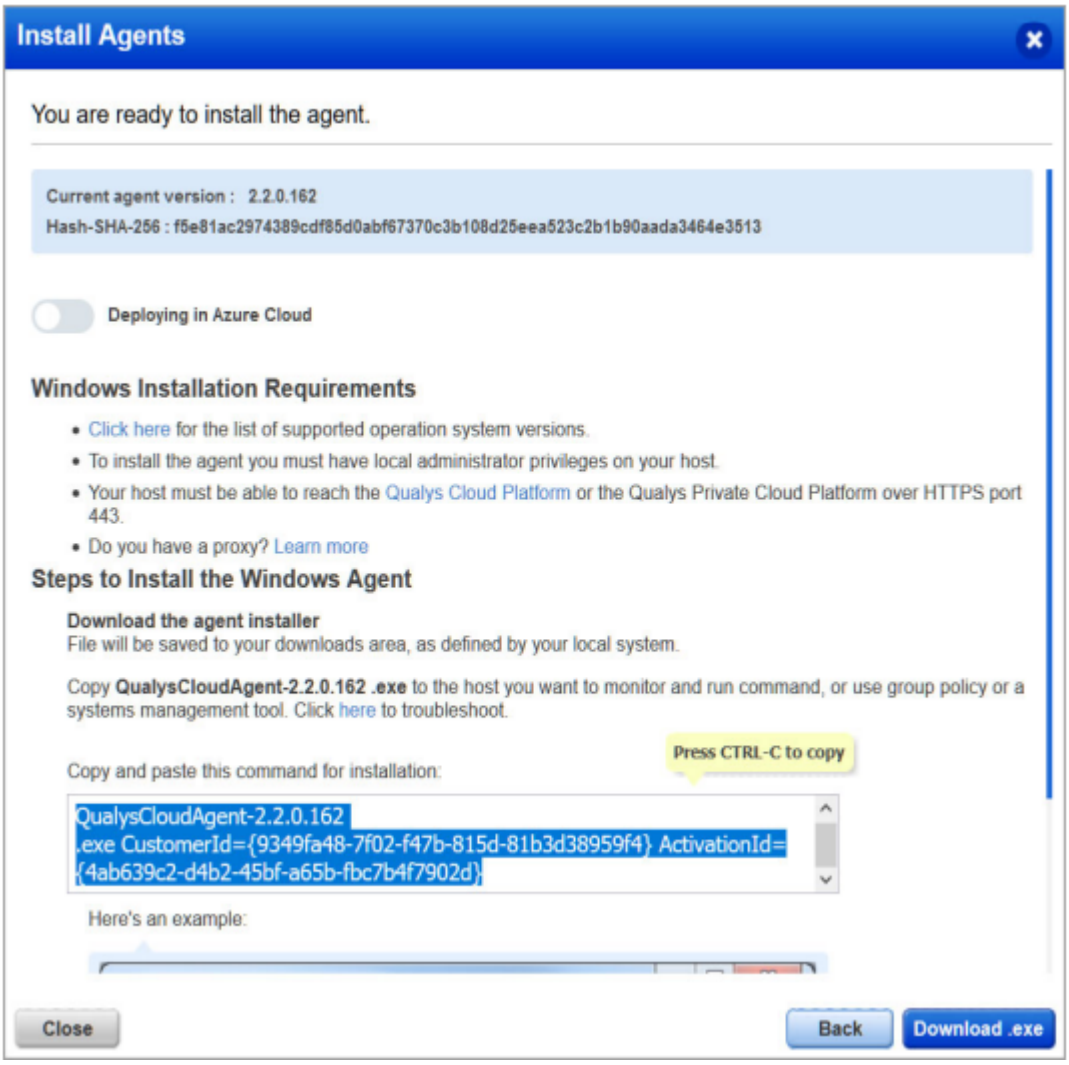
For the other applications also, we can use the same key.



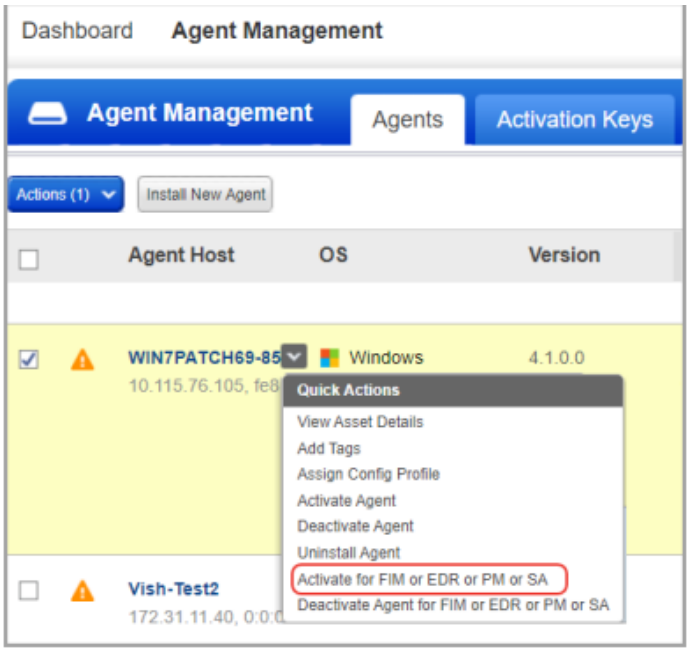
Downloading the installer. Install instructions→ Windows/Linux



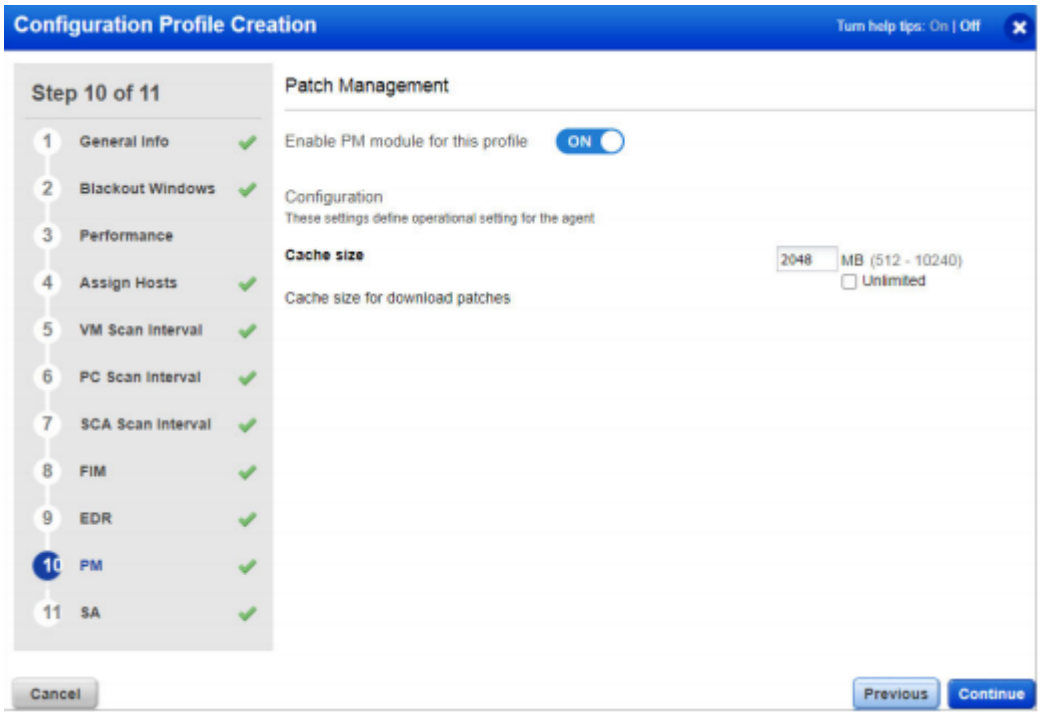
Installing the agent we need to use the windows group policy or system mangement toll after that the agent will start communicating with cloud.



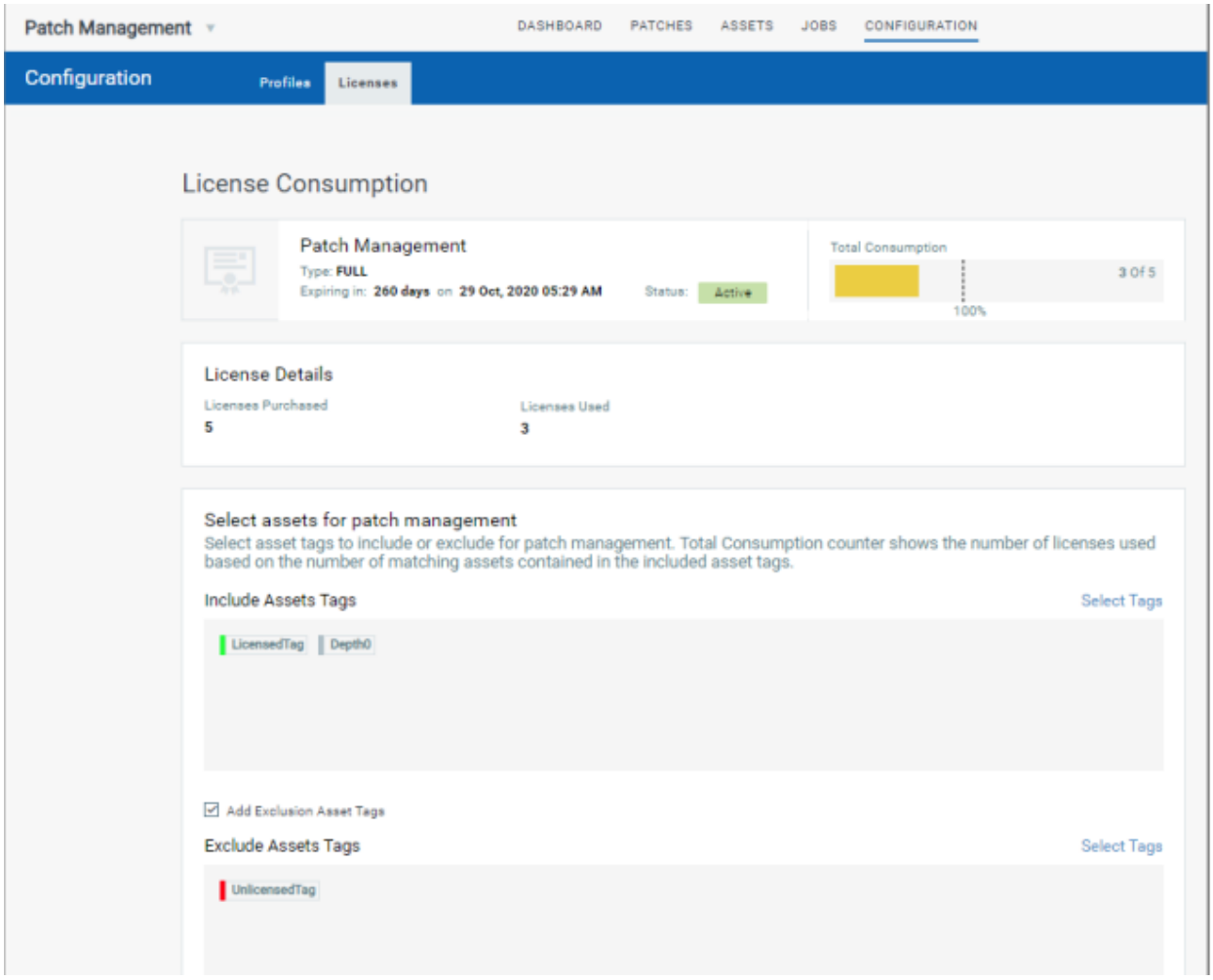
Below snapshot shows for activating the agents for patch management.



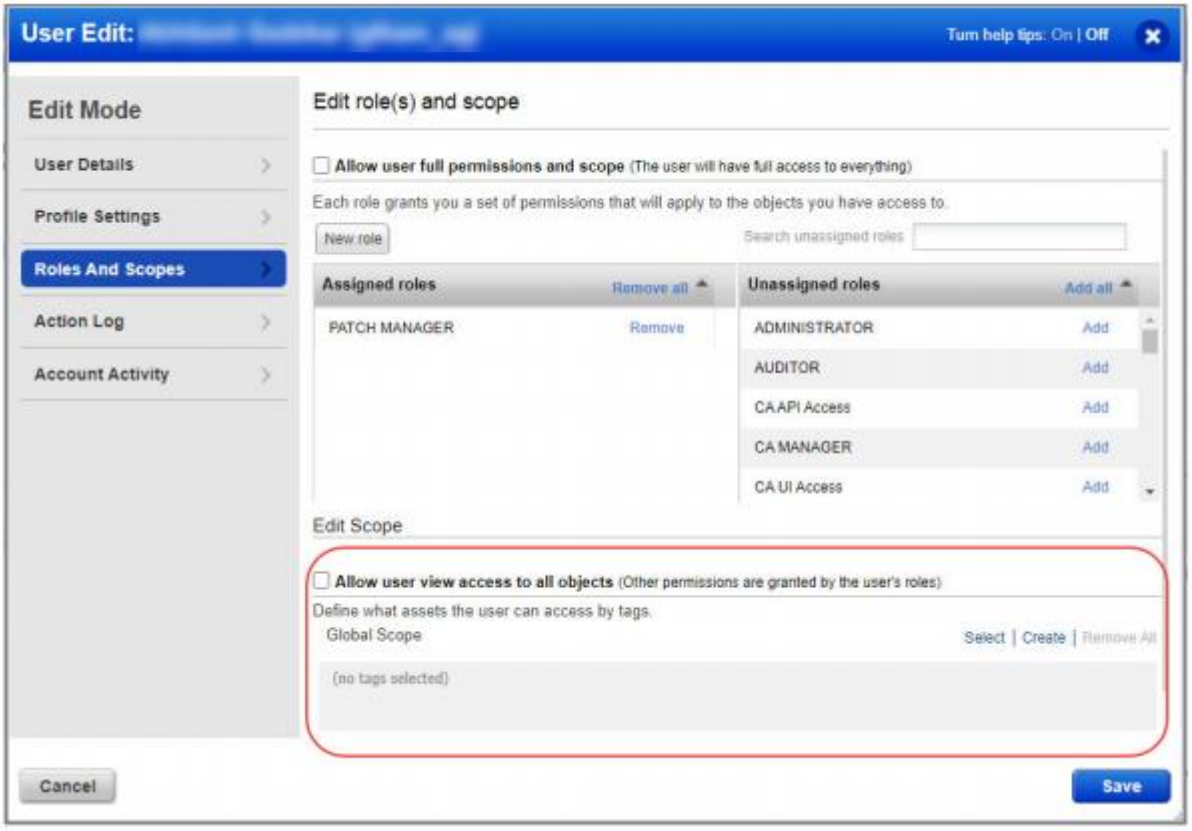
Activating the patch management in the cloud agent console



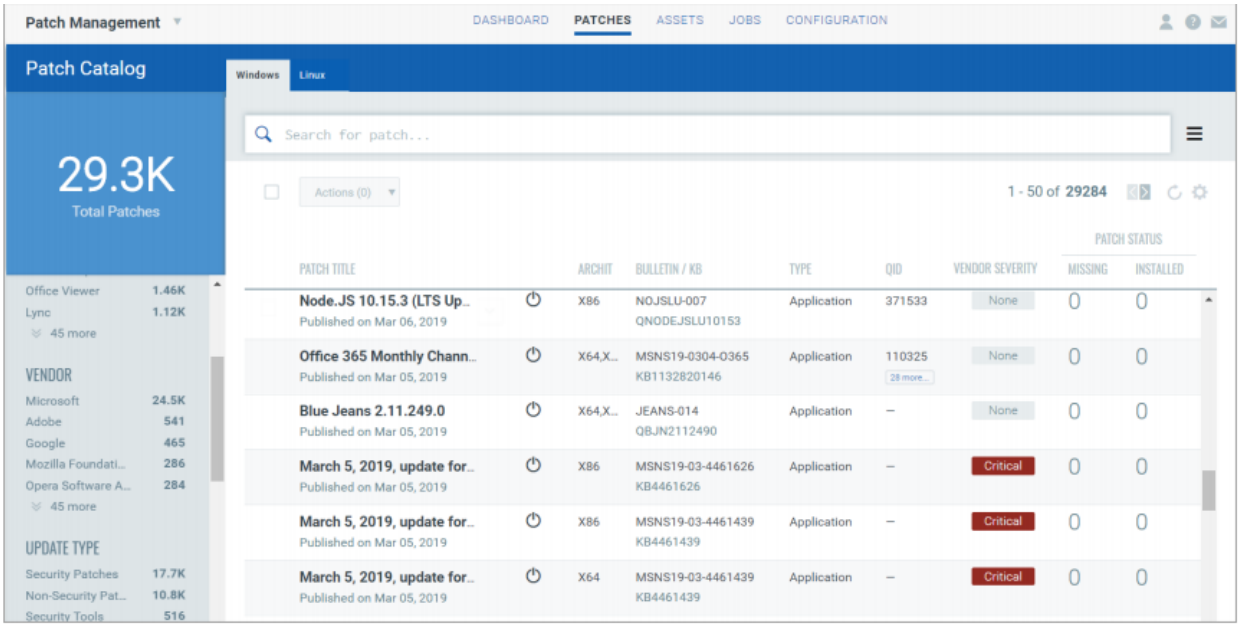
Patch management is now active and ready for Installing and uninstalling the patches



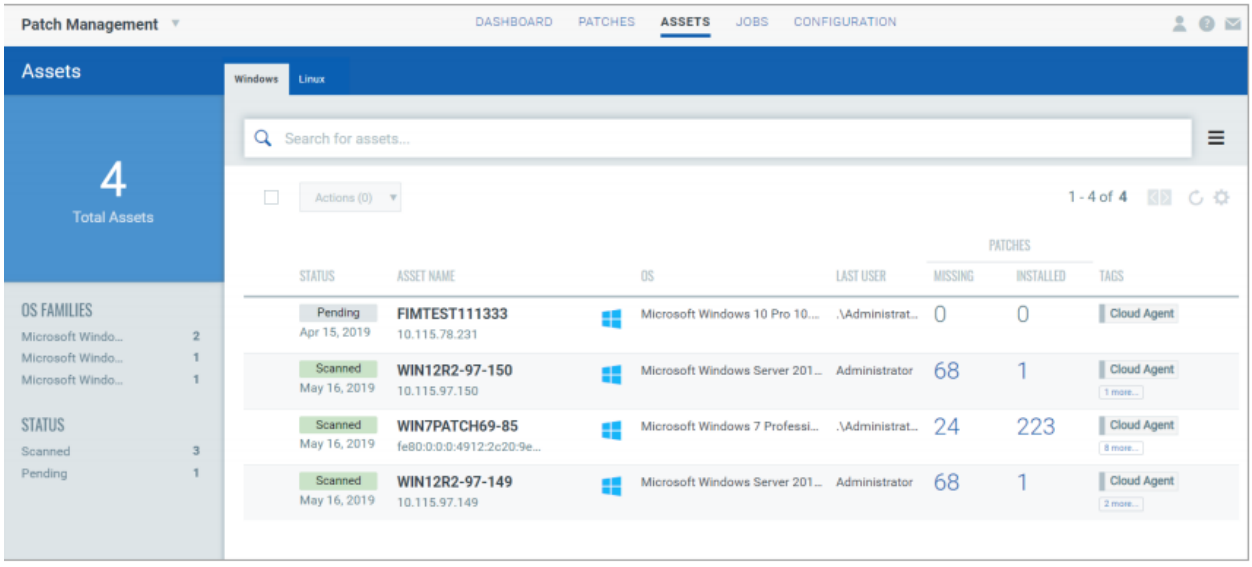
We can give the level of access permission as per the role



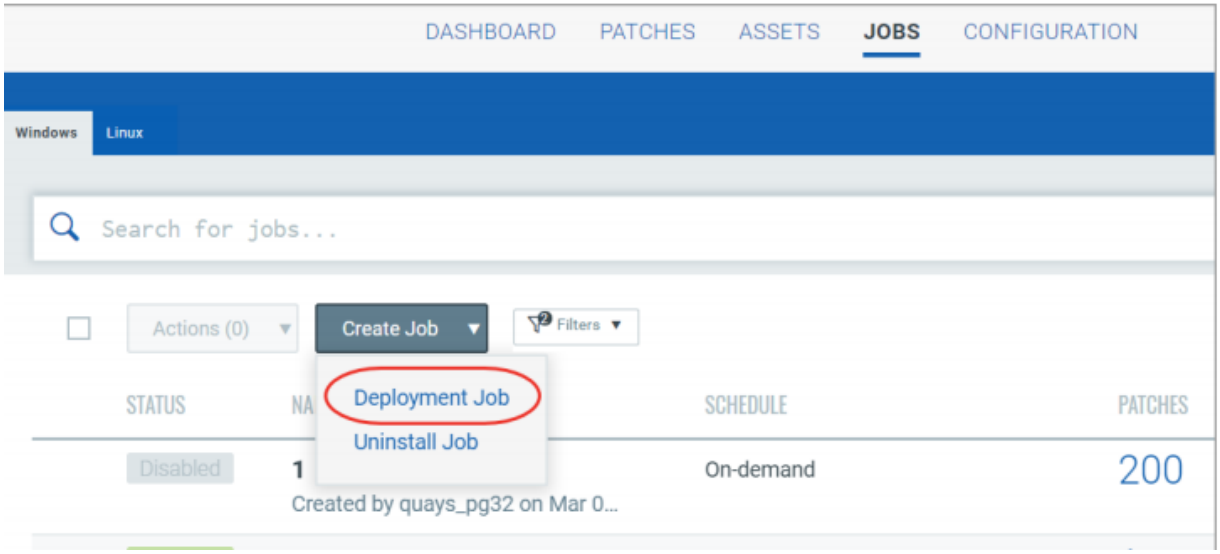
Now we are ready to install the patches in windows and Linux machines, it will scan and get the required patches and get it install into the agent machines.



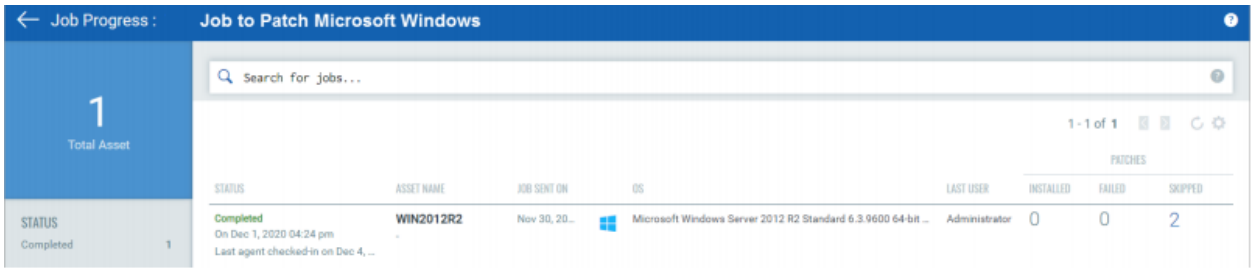
From the assets tab we will get the list of assets where patches are missing.



We can deploy/uninstall forcefully to the Agents machines. Jobs→windows→create Job→Deployment Job



We can view the completion of the installation from Jobs→Quick actions→View progress



5 Analysis

Here we will be discussing comparison of each tools so we can understand which tools is best and what are all the additional features and easy to management.

5.1 Crowdstrike vs Symantec

Below comparison study has been referred from the website (CrowdStrike vs Symantec | Cybersecurity Comparisons, n.d.).

Key Feature	Crowdstrike	Symantec
Delivery	It supports the cloud management console with the single light weight agent.	It is a complex mix, Multiple management console with multiple agents for managing the Cloud, hybrid and local devices
Detection	Machine learning, behavioural analytics, and interconnected malware detection provide advanced, signatureless protection.	It depends on scans and signatures.
Attack Visibility	Full attack visualisation, as per the UI console we can understand the types of attacks quickly and in detail.	Antivirus alerts, but there is a less information available about the threat in order to understand in detail we need to procure the additional product like Symantec EDR
Response	Realtime Response, for further investigation and mitigation we can accessed remotely connection into the systems.	Policy updates, by policy update only the for rules distribution and blacklist. we need to procure the additional product like Symantec EDR for remote access.
Threat Intelligence	Integrated, Malware analysis and threat intelligence alerts are automatically developed.	Separate, requires two different type of product such as Symantec EDR and Symantec Deepsight intelligence.

5.2 Acunetix vs Burpsuite

Below comparison study has been prepared in terms of the web application vulnerabilities referred from the website (Altaf et al., 2015).

Key Feature	Qualys	Rapid7
Injections	Can be detected	Can be detected
Cross Site Scripting	Can be detected	Can be detected
Session Management	Can be detected	Cannot be detected
Sensitive data disclosure	Can be detected	Can be detected
Server Misconfiguration	Can be detected	Cannot be detected
Implementation of SSL	Can be detected	Can be detected

5.3 Qualys vs Rapid7

Below comparison study has been referred from the website (Digital Security Comparison: Tenable.io vs. Qualysguard vs. Rapid7, 2017).

Key Feature	Qualys	Rapid7
Cloud Virtualization	It is Cloud based and Infrastructure on premises supportive.	It's not a cloud-based tool, only locally can be managed
Local Service for Virtualization	Its counts for the service for Virtualization.	Not applied.
Resource Consumption	Local Scanners to be installed in network.	Bandwidth consumption is heigh.
Particular features	Installation can be done via network appliance or VM's	Lots of data to be collected.
Scan deployment	Required operating policies pre configurations.	Requires previous configuration for initiating the scanning
Real time scanning	Very quickly depends upon the host number	Minimum Two hours

6 Solution

As the technology is develop, we cannot able to stop the cyber-attacks but we can put some counter measure to restrict the cyber-attacks. Even though if we are using the latest tools also, we need to update our security measures as and when required. As per the common attacks which is listed in top 10 list, we can restrict the attacks by putting some come control measures. Few of the solutions are listing out below.

- **TCP SYN flood attack:** There should be a link between firewall and switch and rules should be configured for stopping the inbound SYN packets. Connection queue should be increased and open connections timeout should be decreased.
- **Tear Drop Attack:** If the machines were not patched properly then we have to restrict few vulnerable ports like 445,139 and SMBv2
- **Smurf Attack:** From routers we need to restrict the access for broadcasting the IP as directed.
- **Ping of death attack:** Need to check the size of the fragmented IP address if it is maximum size then it needs to be blocked from the firewall end.
- **Botnet:** We should enable the black hole filtering; it will stop if at all any unwanted traffic is coming towards to the secure network.
- **Phishing Attack:** We can configure the email rules as external emails are not allowed towards to the organisation employees ID. If it is in our external personal email ID, we should do a critical thinking and we should analyse email and if it is not required do not open and delete it.
- **Drive by attacks:** Do not open the web portal which is suspicious, always update the web browser and operating system, do not install more plugin it may cause high risk of attack.
- **Password attack:** Always use the complex password which contains alpha numeric, implement the password lockout policy, implement the password change policy like after every one-month period it will prompt for change.
- **Eavesdropping attack:** Whenever we are storing the data local machines or file server it should be encrypted and there should be having the access restriction using the Active directory group permission access.

As a best practice we should update the firewall rules, update the vulnerable ports as and when required instead of waiting for any abnormality activity to be happened. We should be conducting a vulnerability assessment test for any new software should be installing into the production machines. If at all any new devices is adding into the production environment, we need to perform a hardening of the server as per the organisation standards.

7 Recommendations

After the cyber-attacks there are lot of impacts towards to the organisation like losing confidential data, sensitive data, Client proposal, business impact and financial impact. So, in order to resolve from as an individual and from organisation perspective few control measures can be taken in order to block the cyber-attacks. Few of the recommendations are listed below.

- **Training the employee:** Proper awareness training programmes should be conducted by cyber security specialist so that they will be more cautious about the latest type of cyber-attacks. Latest type of Phone etiquette, email etiquette training should be conducted.
- **System should be patch updated:** Ensure by using any tools the devices in the organisation should be updated with the latest patches.
- **Demilitarized Zone:** If any POC is conducting it should be in a Demilitarized zone and once it conducted successfully completed it should be formatted and then only used in the production environment.
- **Endpoint protection:** The devices which is using to connect with the corporate network it should be protect with the endpoint protection software's.
- **Firewall installation:** There should be a firewall should be placed when there is any traffic is going internet and there should be a proper inbound and outbound rule should be in place. Vulnerability ports should be closed.
- **Backup data:** In case of the cyber-attacks and if the data is lost then without the business downtime, we can do the normal operation from the BCP site.
- **Access control system:** We should have the proper access control system so that we can avoid the tail gaiting. And the external devices like USB and CD should be restricted for the employees to bring.
- **Information Security Management:** In every IT industry there should be an ISM team so that in case of any infrastructure changes, new software and freeware installation, additional privilege access etc each employee has to seek permission with ISM. ISM then validated the business proposal and they will approve or reject it accordingly. Also, strict action they will take for any disciplinary actions.
- **Wifi Access security:** Unauthorised person should not give access to the organisation employees. Service providers, vendors and client should not connect to the office Wifi, if required they should connect to the guest Wifi.
- **Access management:** Employees should not have admin right in their respective machine. Also, there should be an Active directory in place so that they can login into their domain from any other machine and by using the security groups we can give access to the respective employees. So that we can restrict the level of permission and also, they won't be able to install any software in their machine.
- **Authentication from Home:** When they are working from home each employee should connect to the VPN and they have to connect it with RSA two factor authentication, so that we can avoid the external attacks.
- **Classification of Data:** Data can be classified into Public, confidential, client and sensitive. So that we can segregate and store it into the respective file server with proper access control.
- **Desktop and Server Security:** There should be an infrastructure team should be there and if at all any issue comes, they should be the first point of contact for trouble shooting and fixing the issue. There should be group policy, system security policy, password policy and domain policy should be applicable in every machine, server hardening should be performed when it is adding to the production.
- **Offboarding/Onboarding Employee:** While onboarding the employees there should be proper induction program so he or she would be aware about the process and procedure

to be adhere. While offboarding the employees his or her access should be terminated on the last day of the employment. For a new employee proper training to be given before he or she doing the hands on the production environment.

- **Change Management:** If at all any changes had been made in the Infrastructure side or new installation. Then they have to raise a change management request and after that they do the Change Advisory Meeting for understanding the Business justification. Once they have met the security standards and if it is justified with the board members then only, they will approve it and will get it implemented.
- **Security Operation Centre:** They can monitor the network utilization and the any malicious activity performed in the network by using some tools, if at all any suspicious activity found they will get alert and they can take proper action.

8 Conclusion

In this report we have discussed about various types of latest attacks and also, we have discussed certain points for mitigating the risk. We had been discussed about various reasons for the Cyber-attacks. Even though we cannot control the security breach entirely but most of the case it happens due to the human error. As an effective method there should be an Internal and external audit should be conducted periodically so that if there is any vulnerability found with respect to the system security, Information security, Client security, Vendor security and Network security it can be fixed in the industrial standard format. As per the International Organisation for standardization (ISO) the standard guidelines to follow in the various sector like Defence, financial, private and public sector so that we can defend against the cyber-attacks. Try to achieve the ISO 27001 so that more business and business proposal will be coming. And from the management wise try to groom the technical skill set by giving them the adequate technical training, conducting cybercrime awareness program, weekly share the etiquette to follow to control the cyber threats, blocking the social website and unnecessary site from organisation. From the HR and management side they have to set a target for each employ to finish the technical certificate, most of the cyber threats is happen due to lack of technical knowledge about the cyber-crime. Finally, we can achieve this only we should be more cautious while using the Internet connected devices.

9 Project Management

As my background was from IT field, using most of the ITIL process, Incident management, Risk management and Change management was using while preparing this report. So, while preparing this report and researching the topic initially was facing some difficulty to come up with best topic. My supervisor Dr John Filippas has help me a lot for finalising the topic. He always mentors me in a proper way like what all the things should be added in this report and what type of project to be selected. For each stage we have a multiple of meetings, sometime he asked me to make some changes in the report. My supervisor proper mentoring and valuable feedback has help to complete this project in a successful way.

9.1 *Project Schedule*

Different Stages of Project	**Time spend (Hrs)**
Background Investigation and the Acquisition of New Skills	110
Gathering and Investigating Requirements	70
Selection of tool and research in depth	150
Recommendation	30
Solution	30
Coursework report preparation	110
Total Hours spend	**500**

10 Critical Appraisal

This report is about the various types of attacks and what is the reason for the cyber threats. Initially for proceeding with my topic needs to be do a lot of research about the latest type of attacks and technique. So, by doing my research we can understand that we cannot stop cyber threats at any point of time but we can control it by adding some better security measures in place. As per the lots of research we can finalize with three different types of latest tools in the market. Positive thing is that, now I can expert in these three different types of tools and if at all any opportunity to get to work in this tool in any organisation it would be a really helpful and easy to work. The valuable knowledge and information which I have gained will be try to implement in my professional and carrier growth.

11 Student Reflections

While doing this project there are lot of technical things I can able to learn. During my previous coursework there is a shortage of time to complete the project in proper way. This time I utilized the time well and took time for proper planning and selection of the tool and researching the tool and coming to the conclusion how the report should be covered all of the key areas. My project is really technical and for educational purpose and it will be very useful in the real life. Hope this project had covered most of the majority areas like various types of latest attacks, reasons for various types of attacks, how to mitigate those type of attacks, which are all the latest tools can be used for preventing from cyber-attacks and as best precaution we had come up with the three different types of tools which is available in the market. By doing this project we would be able to understand the technical areas in depth about the functionality of the tools, also in real scenario if there is any opportunity comes, I would be able to handle the situation.

Bibliography and References

1. *8 Information Security Objectives to Manage Risk | ThreatModeler Soft*. (2019, October 23). ThreatModeler Software, Inc. https://threatmodeler.com/identifying-security-objectives/
2. *Acunetix Support*. (n.d.). Acunetix. Retrieved August 26, 2021, from https://www.acunetix.com/support/
3. Altaf, I., Rashid, F. ul, Dar, J. A., & Rafiq, Mohd. (2015). Vulnerability assessment and patching management. *2015 International Conference on Soft Computing Techniques and Implementations (ICSCTI)*. https://doi.org/10.1109/icscti.2015.7489631
4. CISCO. (2019, October). *Cyber Attack - What Are Common Cyberthreats?* Cisco. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#~types-of-cyber-attacks
5. dcomisso. (2019, March 7). *Different types of cyber crime*. Nibusinessinfo.co.uk. https://www.nibusinessinfo.co.uk/content/different-types-cyber-crime
6. *Digital Security Comparison: Tenable.io vs. Qualysguard vs. Rapid7*. (2017, April 18). GB Advisors. https://www.gb-advisors.com/comparison-tenable-io-vs-qualysguard-vs-rapid7
7. Dunham, R. (2018, July 26). *Information Security Policies: Why They Are Important to Your Organization*. Linford & Company LLP. https://linfordco.com/blog/information-security-policies/
8. Durrani, A. (2014, June 1). *Analysis and prevention of vulnerabilities in cloud applications*. IEEE Xplore. https://doi.org/10.1109/CIACS.2014.6861330
9. *Introduction to Acunetix*. (n.d.). Acunetix. https://www.acunetix.com/support/docs/introduction/
10. Melnick, J. (2018, May 15). *Top 10 Most Common Types of Cyber Attacks*. Netwrix.com. https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

11. Merrit, D. (n.d.). *S DOS DOS*. https://www.splunk.com/pdfs/ebooks/top-50-security-threats.pdf
12. Nadkarni, S. (2021, June 18). *Major Cyber Attacks in 2021*. Www.linkedin.com. https://www.linkedin.com/pulse/major-cyber-attack-2021-sanil-nadkarni/
13. Noam Erez. (2018, June 22). *Cyber attacks are shutting down countries, cities and companies. Here's how to stop them*. World Economic Forum. https://www.weforum.org/agenda/2018/06/how-organizations-should-prepare-for-cyber-attacks-noam-erez/
14. *Patch Management Getting Started Guide Version 1.5*. (2021). https://www.qualys.com/docs/qualys-patch-management-getting-started-guide.pdf
15. *Qualys Qualys Cloud Platform Apps. | Qualys, Inc.* (n.d.). Www.qualys.com. https://www.qualys.com/apps/
16. Scobey, R. (2019, January 2). *How to Automate Threat Intelligence with Falcon X*. https://www.crowdstrike.com/blog/tech-center/automate-intel-falcon-x
17. Scobey, R. (2021, August 6). *How CrowdStrike's Intel Improves Cloud Security*. Crowdstrike.com. https://www.crowdstrike.com/blog/tech-center/cspm-intel-ioa/
18. *Top 10 Cyber Security Threats*. (2019, July 22). ProWriters. https://prowritersins.com/cyber-insurance-blog/top-10-cyber-security-threats/
19. *Why Choose CrowdStrike? | Cloud-Native Security Solutions*. (2019, January 2). Crowdstrike.com. https://www.crowdstrike.com/why-crowdstrike/
20. *Trustwave Contact Us*. (n.d.). Trustwave. Retrieved August 12, 2021, from https://www2.trustwave.com/rs/815-RFM-693/images/Ebook_OnceandFuture%20Threats_Final.pdf
21. Le, D.-N., Kumar, R., Mishra, B. K., Chatterjee, J. M., & Khari, M. (2019). *Cyber Security in Parallel and Distributed Computing : Concepts, Techniques, Applications*

and Case Studies. https://ebookcentral.proquest.com/lib/coventry/reader.action?docID=5741215

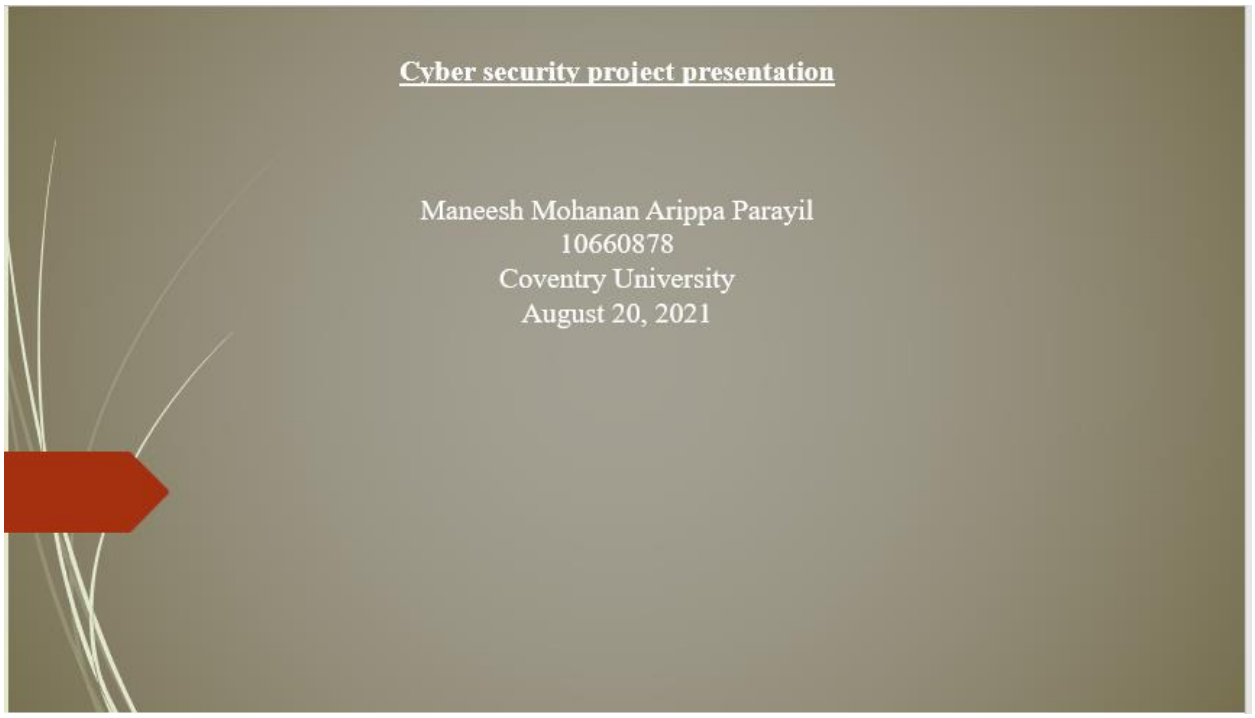
22. Al-Matari, O. M. M., Helal, I. M. A., Mazen, S. A., & Elhennawy, S. (2020). Integrated framework for cybersecurity auditing. *Information Security Journal: A Global Perspective*, 1–16. https://doi.org/10.1080/19393555.2020.1834649
23. Zech, L., Seungmug. (2020). *A Basic Principle of Physical Security and Its Link to Cybersecurity*. https://www.proquest.com/docview/2404395113?pq-origsite=primo&accountid=10286
24. István, P. (2018). *BASIC OF CYBERSECURITY PENETRATION TEST*. https://www.proquest.com/docview/2224304348?pq-origsite=primo&accountid=10286
25. Derek, R. (2018). *Cyber Security & IP Cameras: Everyone's Concern*. https://www.proquest.com/docview/2051214274?pq-origsite=primo&accountid=10286
26. Merrit, D. (n.d.). *Top 50 Security Threats*. https://www.splunk.com/pdfs/ebooks/top-50-security-threats.pdf
27. Melendez, S. (2011). *The Effects of Computer Hacking on an Organization*. Chron.com. https://smallbusiness.chron.com/effects-computer-hacking-organization-17975.html
28. *Network Operations Center Best Practices & Challenges*. (n.d.). ThousandEyes. https://www.thousandeyes.com/learning/techtorials/network-operations
29. *The roles and responsibilities of the Security Operations Centre (SOC)*. (n.d.). FutureLearn. https://www.futurelearn.com/info/courses/security-operations/0/steps/89288
30. Anon. (n.d.-b). *Identity Management – Access Management – RSA*. RSA.com. https://www.rsa.com/en-us/products/rsa-securid-suite/rsa-securid-access
31. Freedman, M. (2019). *How to Secure Your Computer From Hackers*. Business News Daily. https://www.businessnewsdaily.com/11213-secure-computer-from-hackers.html

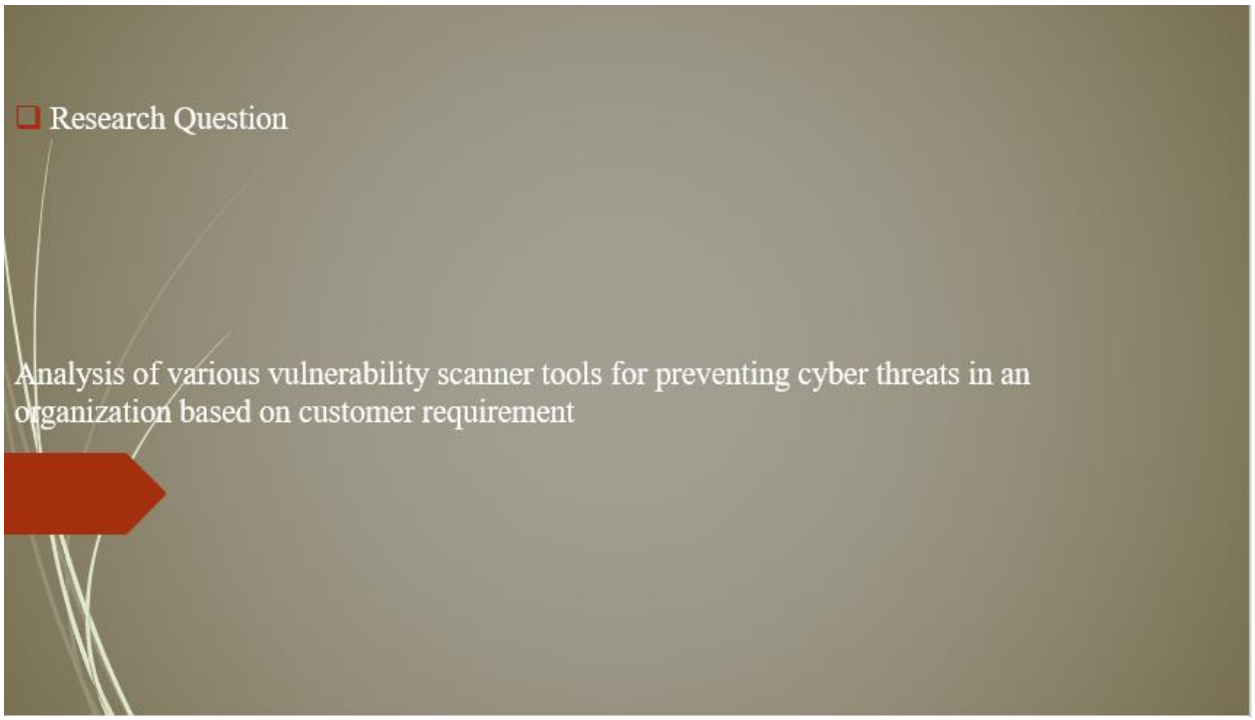
Appendix A – Interim Progress Report and Meeting Records

I have conducted meeting with my supervisor Dr John Filippas regularly and keep him updated about my progress of my coursework preparation. I always show a keen interested to learn a new technology for groom my skill set to pursue in IT industry. Before starting the project had a clear understanding from my supervisor how should be the coursework and what type of project title I should be selecting. By keeping all this benchmark, I came up with the topic and My supervisor had made necessary changes and finally came into the conclusion as my project title is "Analysis of various vulnerability scanner tools for preventing cyber threats in an organization based on customer requirement". During this project I faced some challenges, few of them I sorted out by browsing in internet and others I got the proper guidance from my Supervisor. The online Meeting details as mentioned in the below table.

Meeting description	**Date**
Discussion about the identify the project tittle and what type of topic I should select and what are the points to be considered.	15-May-2021
Topic selection and body of the contents.	10-June-2021
Discussion of the points which I have completed and the doubts clarification.	12-July-2021
What are the extra contents to be added in the project?	12-August-2021
Amending the contents with the proper headings.	20-August-2021

Appendix B – Project Presentation





- Aims and Objectives

1. Major cyber attacks happened in the year 2021.
2. How to keep the information more secure.
3. Different types of attacks and technique.
4. Selecting the Leading vulnerability assessment tools.
5. Explain about the Tools (CrowdStrike, Acunetix ,Qualys)
6. Report generation and Meeting with as per the industry standard with respect to audit compliance.
7. Discussion of Change management with respect of a new software implementation.
8. Periodically Security Audit meeting.

- Relevant Works

This project is an Unique one and no one had conducted the same research on my topic until now, however there are various research has had been conducted on cyber security.[1] Human Aspects of Cyber Security, [2] The Level of Social Engineering Attacks and Awareness on Small Business, [3] Monitoring Analyssts' Performance at Security Operation Centre as Services, [4] The Effect of Information Security Awareness Training delivery Methods on Employees to Mitigate Insider Threats .

- Overview of Methodology

1. Discuss main reasons for Cyber attack.
2. Latest types of Cyber threats and technique.
3. Discussion of key features of CrowdStrike, Acunetix ,Qualys.
4. Comparison of tools CrowdStrike, Acunetix ,Qualys with other tools available in market.
5. Report generation as per the Audit perspective.
6. Installtion steps and working pattern of tools.

- Progress

1. Identified the Various types of technique and cyber attacks.
2. Analyzing of Security weakness and strength area of an organization.
3. After running the tools when the vulnerabilities are identifies, how to address to closure.
4. Which are all the teams are important for an organization for making the organization more secure.

- Remaining task

1. Collate installation, configuration and report generation screenshot.

- Conclusion

- How to mitigate the cyber risk.
- Proof of Concept tools done with this configuration by using these tools (CrowdStrike, Acunetix ,Qualys).
- Conducting Internal and External audit for align with the industry security standards.

Overall this project is success and all the goals has been achieved. By doing this project, got an opportunity to know three different types of latest vulnerability tools in detail.

References I

1. 8 Information Security Objectives to Manage Risk | ThreatModeler Soft. (2019, October 23). ThreatModeler Software, Inc. https://threatmodeler.com/identifying-security-objectives/
2. CISCO. (2019, October). Cyber Attack - What Are Common Cyberthreats? Cisco. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#~types-of-cyber-attacks
3. dcomisso. (2019, March 7). Different types of cyber crime. Nibusinessinfo.co.uk. https://www.nibusinessinfo.co.uk/content/different-types-cyber-crime
4. Dunham, R. (2018, July 26). Information Security Policies: Why They Are Important to Your Organization. Linford & Company LLP. https://linfordco.com/blog/information-security-policies/
5. Melnick, J. (2018, May 15). Top 10 Most Common Types of Cyber Attacks. Netwrix.com. https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

References II

1. Merrit, D. (n.d.). S DOS DOS. https://www.splunk.com/pdfs/ebooks/top-50-security-threats.pdf
2. Nadkarni, S. (2021, June 18). Major Cyber Attacks in 2021. Www.linkedin.com. https://www.linkedin.com/pulse/major-cyber-attack-2021-sanil-nadkarni/
3. Noam Erez. (2018, June 22). Cyber attacks are shutting down countries, cities and companies. Here's how to stop them. World Economic Forum. https://www.weforum.org/agenda/2018/06/how-organizations-should-prepare-for-cyber-attacks-noam-erez/
4. Top 10 Cyber Security Threats. (2019, July 22). ProWriters. https://prowritersins.com/cyber-insurance-blog/top-10-cyber-security-threats/
5. Trustwave Contact Us. (n.d.). Trustwave. Retrieved August 12, 2021, from https://www2.trustwave.com/rs/815-RFM-693/images/Ebook_OnceandFuture%20Threats_Final.pdf


THANK YOU

Appendix C – Certificate of Ethics Approval

Certificate of Ethical Approval

Applicant:	Maneesh Arippa Parayil
Project Title:	Analysis of various vulnerability scanner tools for preventing cyber threats in an organization based on customer requirement.

This is to certify that the above named applicant has completed the Coventry University Ethical Approval process and their project has been confirmed and approved as Low Risk

Date of approval:	07 Jun 2021
Project Reference Number:	P123129