jamk.fi

Implementation of security best practices on AWS Cloud

Case: Vulnerability scanning of EC2 instances and networks

Jukka Veijanen

Master's thesis
May 2020
School of Technology
Degree Programme in Information Technology
Cyber Security

jamk.fi

Description

Author(s)	Type of publication	Date
Veijanen, Jukka	Master's thesis	May 2020
		Language of publication: English
	Number of pages: 53	Permission for web publication: x

Title of publication

Implementation of security best practices on AWS Cloud

Case: Vulnerability scanning of EC2 instances and networks

Degree programme

Information Technology, Cyber Security

Supervisor(s)

Kotikoski, Sampo; Hautamäki, Jari

Assigned by

Polar Electro Oy

Abstract

The thesis was assigned by Polar Electro, a company which manufactures sport instruments and heart rate monitoring equipment. Polar wants to improve the security of its cloud services and implement best practices for security in its own services. The first step is to perform vulnerability scans for services installed on Amazon AWS.

The master's thesis studied and implemented the first phase of Amazon AWS security best practices. Here a vulnerability scan for the company's cloud-based instances and networks was selected. Amazon Inspector was chosen as the tool, since it can be easily deployed to all accounts. One EC2 instance was tested.

Amazon Inspector was enabled and the rules were created for the scanning tests after which they were run. The results were sparse, with only 7 notable findings, because the Inspector had no visibility inside the instance. After installing the Inspector Agent, the tests were rerun, and the results had significant differences. Inspector reported the total of 284 notable findings, which is more than 40 times than in the first passive scanning. The report had 162 high severity notable findings, which is 57% of all notable findings.

The thesis showed that Amazon cloud security testing is an important part of software development process, as the test results revealed. The assigner got a strong recommendation for implementing security best practices in their environment.

Keywords/tags (subjects HYPERLINK "http://vesa.lib.helsinki.fi/")

Amazon AWS, security best practices, vulnerability scanning

Miscellaneous (Confidential information)

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päiväys
Veijanen, Jukka	Opinnäytetyö, YAMK	Toukokuu 2020
		Julkaisun kieli: Englanti
	Sivumäärä 53	Verkkojulkaisulupa myönnetty: x

Työn nimi

Implementation of security best practices on AWS Cloud

Case: Vulnerability scanning of EC2 instances and networks

Tutkinto-ohjelma

Information Technology, Cyber Security

Työn ohjaaja(t)

Sampo Kotikoski, Jari Hautamäki

Toimeksiantaja

Polar Electro Oy

Tiivistelmä

Opinnäytetyön toimeksiantaja on Polar Electro Oy, yritys, joka valmistaa urheiluinstrumentteja ja sykemittauslaitteita. Polar haluaa parantaa pilvipalveluidensa turvallisuutta ottamalla käyttöön parhaita turvallisuuskäytäntöjä omissa palveluissaan. Ensimmäisenä vaiheena suoritettaan Amazon AWS:ään asennettujen palveluiden haavoittuvuusskannaukset.

Opinnäytetyössä tutkittiin ja toteutettiin Amazon AWS -turvallisuuden parhaiden käytäntöjen ensimmäisenä vaiheena haavoittuvuusskannaus yrityksen pilvipohjaisiin EC2-instansseihin ja verkkoihin. Työkaluksi valittiin Amazon Inspector, joka voidaan helposti ottaa käyttöön kaikille tileille. Yksi EC2-instanssi valittiin testiä varten.

Amazon Inspector otettiin käyttöön ja skannaustesteille luotiin säännöt, jonka jälkeen ajettiin ensimmäiset testit. Tuloksia oli vähän, vain 7, koska Inspectorilla ei ollut näkyvyyttä instanssin sisälle. Inspector Agent asennuksen jälkeen testit suoritettiin uudelleen, ja tuloksissa oli merkittäviä eroja. Inspector raportoi yhteensä 284 merkittävää havaintoa, mikä on yli 40 kertaa enemmän kuin ensin ajettu passiivinen skannaus. Raportissa oli erittäin vakavia havaintoja 162, mikä on 57% osuus kaikista havainnoista.

Opinnäyte todisti, että Amazonin tietoturvatestaus on tärkeä osa ohjelmistokehitysprosessia, kuten testitulokset paljastavat. Toimeksiantaja sai vahvan suosituksen parhaiden tietoturvakäytäntöjen toteuttamiseksi ympäristössään.

Avainsanat (asiasanat)

Amazon AWS, security best practices, vulnerability scanning

Muut tiedot

Contents

Figures

Tables

Terminology

Term	Explanation
Attack	Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset
Availability	Property of being accessible and usable upon demand by an authorized entity
AWS	Amazon Web Services
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes
Data	Collection of values assigned to base measures, derived measures and/or indicators
Information security	Preservation of confidentiality, integrity and availability of information
Integrity	Property of accuracy and completeness
PCI DSS	The Payment Card Industry Data Security Standard. PCI DSS is an information security standard for entities that store, process, and/or transmit cardholder data.
Risk	Effect of uncertainty on objectives
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation
Risk owner	Person or entity with the accountability and authority to manage a risk
SDLC	Software Development Life Cycle
Threat	Potential cause of an unwanted incident, which may result in harm to a system or organization
Vulnerability	Weakness of an asset or control that can be exploited by one or more threats

1 Introduction

The purpose of this thesis is to create guidelines how to take first step on AWS Security Best Practices, explain what its benefits are and discuss the expected results. The focus is on finding the optimal way to implement vulnerability scanning to the company's own instances and networks on Amazon AWS cloud.

The structure of thesis is as follows; first literature review chapter presents what is cloud computing, Amazon AWS and its well-architected framework, then Amazon security services are presented. Then the threats for cloud, tools and controls to protect from them are presented. The last part on the literature review chapter discusses vulnerabilities. Later methodology and results are presented before the last two chapters, conclusions and proposal for further research suggestions.

1.1 Research questions and limitations

The thesis performs vulnerability scans on the selected EC2 instance and analyzes the results. The analysis seeks to determine how well Amazon Inspector finds vulnerabilities and what kind of useful information it provides to users. The analysis also considers whether there are possible false results and what is the reason of them.

There are several third parties' tools available for vulnerability scanning, but they are limited out of this study. The research question is: Can Amazon Inspector find significant vulnerabilities in the client's environment?

Amazon Inspector is selected for a scanning tool and it is evaluated based on the following research sub questions.

1. What preconditions does the implementation of this service require?
2. How is this service enabled?
3. Does this service work as expected, and if yes/no, why?

This master's thesis does not study how to analyze results nor how to fix issues. The OWASP Top 10 vulnerabilities are not explained in this thesis. Other security best

practises than vulnerability scanning are limited out of this thesis. Software development process and its phases are not explained in this thesis.

1.2 Assigner

Polar Electro Oy, the assigner of the thesis employs 1,200 people worldwide and, manufactures all products in its factories. Polar has 26 subsidiaries globally and manages a distribution network supplying over 35,000 retail outlets in more than 80 countries. Polar caters for all levels of fitness by offering a comprehensive product range along with essential support and advice and its product range covers everything from improving an athlete's sports performance to helping people enjoy a healthier lifestyle, and aiding rehabilitation and weight management. (Polar Electro 2019.)

Polar manufactures equipment such as sport watches and sensors. Polar is a family business founded in 1977 by a Finnish professor from the University of Oulu, Seppo Säynäjäkangas. Polar is located in Finland, and its headquarters is in Kempele with the other sites in Jyväskylä, Tampere, and Espoo.

2 Literature review

This chapter contains the background of this master's thesis. The chapter introduces methodology, cloud computing, Amazon AWS and five pillars of Well-Architected Framework. Next are presented Amazon security services, threats, tools and controls to protect from threats, vulnerabilities and how to face and mitigate them. Finally, Amazon Inspector's rules packages are introduced.

2.1 Methodology

This chapter presents the methodology used to find the most optimal tool for implementing the first step of chosen security best practice.

This thesis uses Design Science Research method to define an artefact to solve the problem (Johannesson & Perjons 2014, 3). This artefact is guidelines on how to implement an optimal vulnerability scanning for organization's EC2 instances and networks on Amazon AWS cloud. The solution is analyzed and its results evaluated.

The author's background on software development sector was the reason to select the methodology for the thesis. To develop a guidelines (artefact) was natural choice for the thesis.

The research is carried out primarily with a qualitative research approach, because no quantitative data has been collected in the work, for example by means of a survey, and the qualitative approach is better suited because information is collected mainly from standards, documents, web pages, researches and from similar sources.

2.2 Cloud computing

In the cloud computing model, the customer does not need their own data center but has access to the resources via the Internet. Cloud computing provides resources such as servers, storage, applications, and services everywhere with minimal management. The cloud service has essential characteristics, service models and deployment models. (Mell & Grance 2011, 2.)

2.2.1 Essential characteristics

Mell & al. (2011, 2) have defined essential characteristics as follows.

On-demand self-service means that the customer can choose the resources they want for their use as needed without separate agreements.

Broad network access means that the capabilities are available using thin or thick client platforms through networks. These platforms include e.g. mobile phones, tablets, laptops and workstations.

Resource pooling means that the service provider's computing resources are shared among several customers. The customer can specify the region where the selected resources are used.

Rapid elasticity means that the capabilities are automatically scaled according to demand and are available anywhere, anytime.

Measured service means that the resources are configurable to respond as desired when they reach a certain measurable threshold, and their changes can be monitored as needed. For example, if the storage capacity of the database reaches 80% of the maximum, then the database expansion will be triggered automatically.

2.2.2 Service models

Mell & al. (2011, 2-3) have defined service models as follows.

Software as a Service (SaaS) means that the consumer can access the applications provided by the cloud provider through either a thin client interface or a program interface. The service provider manages the underlying cloud infrastructure.

Platform as a Service (PaaS) means that the service provider manages the underlying cloud infrastructure where the customer can deploy the applications, they create that are made with the tools provided by the service. The customer manages their own applications and possibly the configuration of the applications.

Infrastructure as a Service (IaaS) means that the service provider manages the cloud infrastructure and the customer can install applications, manage operating systems, storage, etc. This model gives the customer the most extensive access.

2.2.3 Deployment models

Mell & al. (2011, 3) have defined deployment models as follows.

Private cloud means that the cloud infrastructure is privately used, managed, and possibly owned by some organization.

Community cloud means that the cloud infrastructure is intended for use by a specific community of concern.

Public cloud means that the cloud infrastructure is intended for public use, it is under the control and premises of the service provider.

Hybrid cloud means that the cloud infrastructure is a composition of the above-mentioned cloud infrastructures. These clouds are configured with each other so that the transferability of data and applications between them is enabled.

2.3 What is AWS?

Amazon AWS provides cloud services such as servers, storage, networks, and security. The operational security of these services is ensured in several separate regions, which are divided into availability zones. Regions are located globally and, if desired, geographic restrictions and physical locations of data can be defined. The cost of using Amazon's services is based on their actual utilization rate and they are scalable as needed. Scalability enables flexible use of services, reducing the need for the client to maintain traditional servers or mainframes. (Cloud computing with AWS.)

2.4 Well-Architected Framework

Amazon AWS Well-Architected whitepaper (2019, 6-33) explains how the AWS Well-Architected Framework is based on five pillars, which are presented only at a very generic level as follows:

Operational Excellence means “the ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures”.

Security means “the ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies”.

Reliability means “the ability of a system to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues”.

Performance Efficiency means “the ability to use computing resources efficiently to meet system requirements, and to maintain that efficiency as demand changes and technologies evolve”.

Cost Optimization means “the ability to run systems to deliver business value at the lowest price point”.

2.5 Amazon Security

Amazon AWS is approached in this thesis from a bird's-eye perspective, going deeper into security and moving towards the selected service. This way the importance of security can be highlighted in Amazon's overall architecture. The thesis focuses on the Security pillar part of AWS Well-Architected Framework.

Amazon requires the client to take care of the security in the cloud and offers the security of the cloud. This is illustrated in the Responsibility model Figure 1.

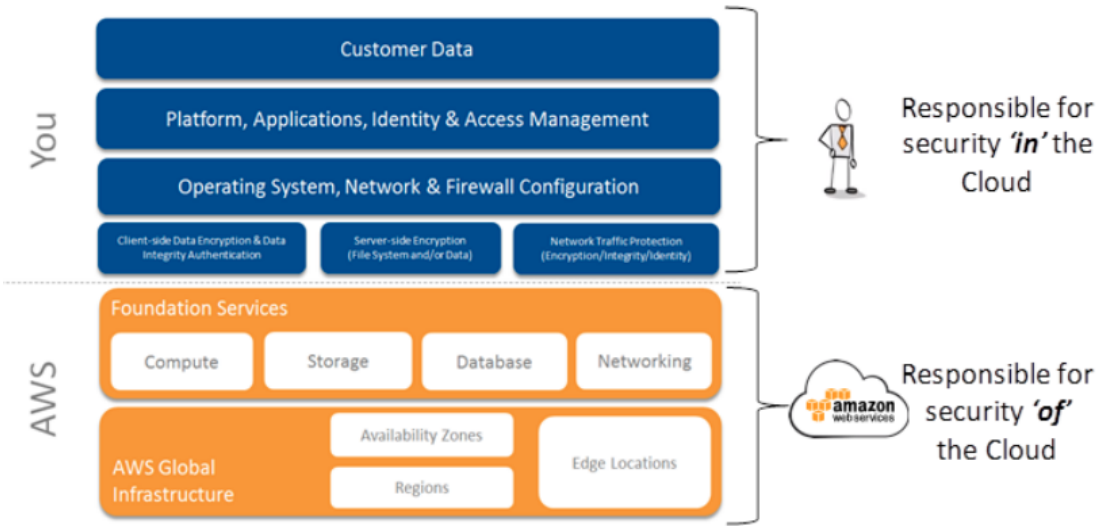

Figure 1. Responsibility model

Figure 2 describes AWS services enhancing security investigations. Customer can configure these services in own infrastructure to improve the security.

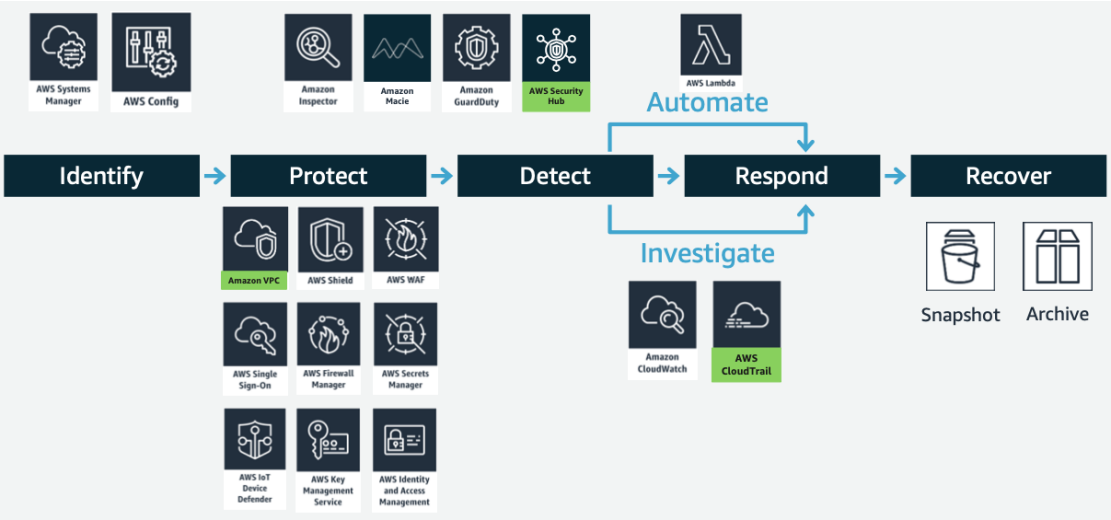

Figure 2. AWS services enhance security investigations

Here is just a brief overview of the security services shown in the Figure 2. These are presented at this stage only superficially; however, Amazon Inspector is discussed in more depth in the Results chapter.

2.5.1 AWS Systems Manager

AWS Systems Manager is a scalable and secure solution which gives a visibility into entire infrastructure. AWS service that maintain security and compliance. It can be used to manage and operate securely across entire infrastructure. AWS Systems Manager is a group of services which allows customers to have a better visibility and control of the infrastructure such as; Run Command, Parameter Store, Sessions Manager and Patch Manager. The basic idea behind the Systems Manager is that there will be an SSM agent installed in the EC2 instances, and the customer can provide specific tasks to the installed agent from the systems manager console. With AWS Systems Manager user can connect directly to EC2 instance from the web browser. (AWS Systems Manager User Guide 2019.)

2.5.2 AWS Config

AWS Config keeps the track of inventory as well as inventory changes. AWS Config works on region wide, not global wide. It shows e.g. relationships between resources as well as configuration changes of their life cycle. If changes are done to resources which have been attached to AWS Config, they are reflected in AWS Config history. This history data comes from AWS CloudTrail logs. This is very clever service e.g. in such situation where the infrastructure cost has spiked suddenly, and the boss wants to know the reason for it. Another example is that last night a website was working fine but, in the morning, website is not accessible. With the AWS Config administrator can check what exactly has changed from last night to this morning. (What Is AWS Config?.)

2.5.3 Amazon Inspector

Amazon Inspector is a security tool developed by Amazon to assess instances vulnerabilities, security threats and deviations of best practices. It relies on the agent installed on the server to scan the server. AWS Inspector has certain pre-defined templates based on which customer can scan the system. Once the assessment is completed, a report will be created according to the severity. (What is Amazon Inspector?)

2.5.4 Amazon Macie

Amazon Macie is a security service that protects sensitive data stored on AWS. The service uses machine learning, which can automatically classify and detect data stored on Amazon S3. Macie is supported in the following areas; US East (N. Virginia) (us-east-1), and US West (Oregon) (us-west-2). (What Is Amazon Macie?)

2.5.5 Amazon GuardDuty

Amazon GuardDuty is a security monitoring tool based on VPC Flow Logs, AWS CloudTrail event logs, and DNS logs, which are analysed to identify signs of unauthorized or malicious activity using machine learning. These include, for example, compromised EC2 instances used for unauthorized activities and security breaches. GuardDuty monitors only the Route 53 for DND Logs. (What Is Amazon GuardDuty?)

2.5.6 AWS Security Hub

Security Hub gives a comprehensive view of high-priority security alerts and compliance status across AWS accounts. The idea of Security Hub is to have a centralized dashboard where all the security alerts are visible. This way the auditor can use this dashboard to check what is missing or what alerts have been raised. Security Hub can also generate its own findings by running automated and continuous checks against the rules in a set of supported security standards. These supported standards are; CIS AWS Foundation and, PCI DSS. (What Is AWS Security Hub?) Figure 3 gives an overview of Security Hub.

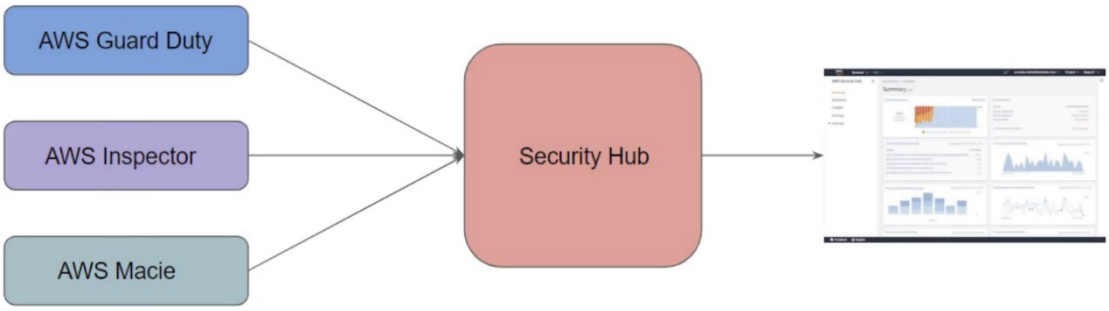

Figure 3. Overview of Security Hub

2.5.7 AWS Lambda

Lambda is a computing service that lets you run code without a server. Lambda automatically manages background computing resources. The customer only pays for the computational time they consume and not for the running code. The code run in AWS is stateless and is called a lambda function. (AWS Lambda.)

2.5.8 Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) is a virtual network like the traditional network where you can run your own AWS resources. Its significant advantage is its scalable infrastructure. Traffic between resources and VPC remains internal to the Amazon network and is invisible to outside. (What Is Amazon VPC?)

2.5.9 AWS Shield

AWS Shield Standard is a security service for DDoS attacks that provides additional protection in addition to other AWS services. For AWS Shield Advanced service customer must pay a fee to get more comprehensive protection, which, when combined with other services, provides the best protection for organizations. With the Shield Advanced the customer can have a near-real-time visibility for protection against large and sophisticated DDoS attacks. (AWS Shield.)

2.5.10 AWS WAF

AWS WAF is a web application firewall for managing HTTP(S) requests. The firewall can also be used to protect applications on the AWS network. WAF concepts contain Rules, Rule Statements, and association. Rule Statements define basic characteristics that would be analysed within a web request. These can be custom-defined or ready-made from AWS and marketplace. WAF provides two primary rule types: Regular

Rule & Rate-Based Rule. Association defines to which entity WAF is associated to. (AWS WAF.)

2.5.11 AWS Single Sign-On

Amazon-hosted single sign-on service to manage SSO permissions for all AWS accounts and cloud applications, as well as commonly used third-party software. The service supports SAML (Security Assertion Markup Language) 2.0. User do not have to re-authenticate when login to other application or AWS account. SSO users can authenticate via CLI (Command Line Interface), and they will be able to perform the CLI operations without having to add keys in their credentials file. (What Is AWS Single Sign-On?)

2.5.12 AWS Firewall Manager

AWS Firewall Manager simplified maintenance and management of security group accounts and resources. Defined security rules are available automatically for all accounts in the organization. (AWS Firewall Manager.)

2.5.13 AWS Secrets Manager

AWS Secrets Manager is a service for managing various types of data requiring encryption. The account administrator does not have to worry about access credentials because the service will hide them securely and cannot be accessed by other users. Compliance like PCI DSS requires secrets must be rotated and audit on who does what with secrets. There is a Built-In integration for rotating MySQL, PostgreSQL and Aurora on RDS. There is also a fine-grained access control to control who has access to secrets with help of IAM and Resource based policies. (What Is AWS Secrets Manager?)

2.5.14 AWS IoT Device Defender

AWS IoT Device Defender is a security service that can audit the entire configuration of AWS IoT hardware and detect abnormal behaviour. The Administrator can monitor the security policies of IoT devices, which reduces security risks. (AWS IoT Device Defender.)

2.5.15 AWS Key Management Service

AWS KMS is an easy-to-use service for managing encryption keys, master keys, encryption material, key lifecycles, and related encryption tasks. ASW KMS is integrated for use with other AWS services that implement encryption, which makes it easy to manage the encrypted data used in AWS. It does not have any upfront cost and is pay as you go model. (What is AWS Key Management Service?)

2.5.16 AWS Identity and Access Management (IAM)

IAM is a user and group management service that can grant access to specific resources. IAM has four components: users, groups, roles, and policies. Permission is granted to a user group associated with a user by associating that group with a policy defining the access to a resource. (What Is IAM?)

2.5.17 Amazon CloudWatch

Amazon CloudWatch is a real-time AWS resource and application monitoring service. The Administrator can create dashboards displaying collections of metrics as well as automatic alarms and events based on exceeding specified resource thresholds. (What Is Amazon CloudWatch?)

2.5.18 AWS CloudTrail

AWS CloudTrail is a service that allows to record every API call that takes place in an AWS account. CloudTrail is recommended to be enabled at the first phase when creating account because it cannot get past events before enabling. It's also recommended to apply it to all regions. Auditor can check who has done, what, and when from CloudTrail logs. Auditor can view the last 90 days of events in Event history. After 90 days the events are stored in S3 bucket. (What Is AWS CloudTrail?)

2.5.19 VPC Flow Logs

VPC Flow Logs allows to see, what type of traffic is coming to a particular interface. AWS allows interface level Flow Logs to check on what type of traffic is accepted or rejected by the security group. Flow Logs works at a network interface level. This service can capture IP traffic on networks and store it on Amazon CloudWatch Logs and Amazon S3. (VPC Flow Logs.)

2.6 Cloud security threats

Chen (2019) refers to a Gartner report that states the rate of growth in public cloud services is really significant, leading to more companies sharing resources with each other. This development is also attracting more criminals specializing in cloud services. (Chen 2019, 130-131.) Chained vulnerabilities are another potential issue. By default, vulnerability scanners rate each vulnerability in isolation. But this is not how the attackers target assets. They can use any combination of vulnerabilities to accomplish their attack. Two or more combined low score vulnerabilities may be a greater risk to the organization than one critical vulnerability. (Williams 2019, 4.)

2.7 MITRE ATT&CK Framework

Various cyber security organizations can use the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) tool to develop threat models and methodologies. MITRE aims to help communities solve cyber security issues with its tool. (Pennington 2019, 41.) Figure 4 shows an example how to plan an exploit of such chained vulnerabilities for an attack.

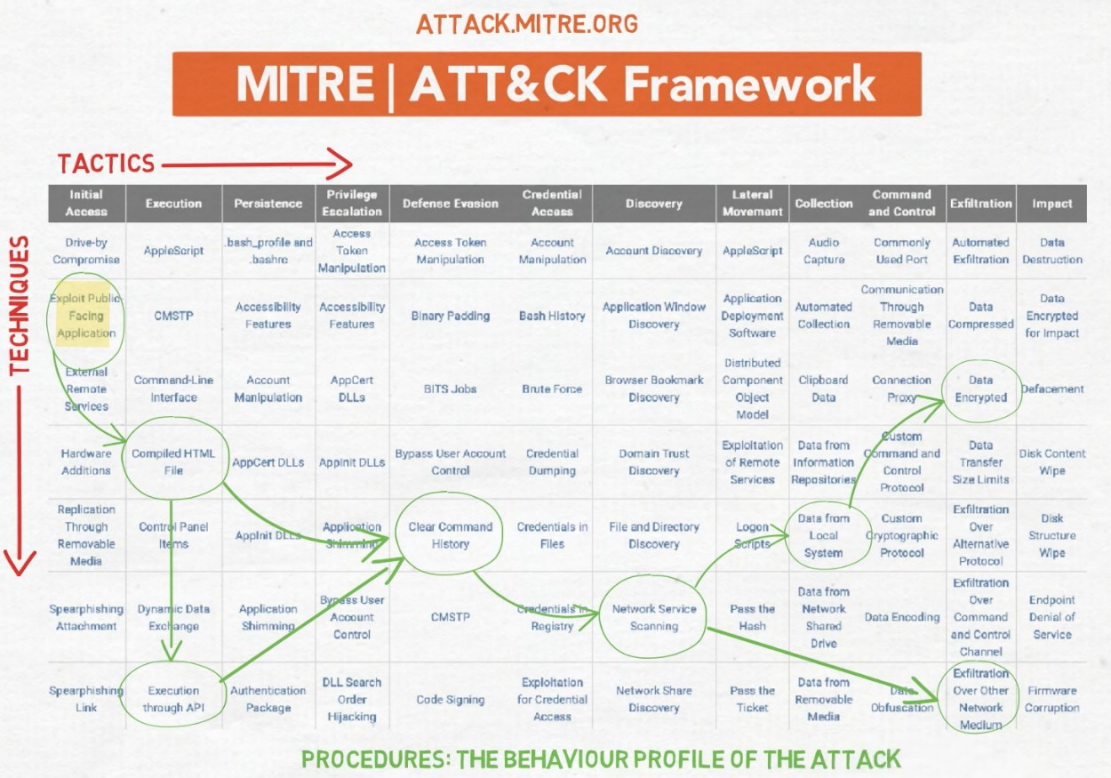

Figure 4. ATT&CK Matrix: The Enemies Playbook

2.8 OWASP

The Open Web Application Security Project (OWASP) is a non-profit foundation dedicated to improving software security. The community is leading open source projects that are being used globally with the goal of making the Internet safer for all users. OWASP develops and maintains tools that can be used to improve the security of your organizations. OWASP provides training and resources to improve security. (Who is the OWASP Foundation.)

2.9 Center for Internet Security

The CIS Controls, a globally accepted security best practice, has been developed by the IT community to support cyber defence. These are used to defend against the most common attacks against systems and networks. (Center for Internet Security 2019, 1.)

2.9.1 CIS Control 2: Inventory and Control of Software Assets

Active management of all software on your network is a critical step as attackers are constantly looking for vulnerable software to remotely exploit it. If obsolete software is found on an organization's network, an attacker could gain access to it and perform unauthorized activity, causing problems for the organization. (Center for Internet Security 2019, 12.)

2.9.2 CIS Control 3: Continuous Vulnerability Management

Constant checking for vulnerabilities and shortages is an important step in protecting against attacks. Possible conflicting priorities can cause nasty side effects that pose particular challenges for the maintenance team. (Center for Internet Security 2019, 15.)

2.9.3 CIS Control 4: Controlled Use of Administrative Privileges

Managing administrators' processes and tools is critical because malicious use of administrative privileges is the primary way for attackers to exploit vulnerabilities. (Center for Internet Security 2019, 18.)

2.9.4 CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

Active updating of default security configurations prevents attackers from exploiting vulnerabilities. Instead of security, manufacturers make their products easy to use, which often leaves the default usernames and passwords used by attackers. Preinstallations may contain unnecessary software and services that can be exploited by attackers. Organizations should use well-established security guides and checklists to improve their security. (Center for Internet Security 2019, 21-22.)

2.9.5 CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services

Attackers scan for remote services that are vulnerable to exploitation. Unnecessary and poorly configured servers increase the risk of exploitation. Administrators should make sure that automatic installation packages do not enable unnecessary services or open unnecessary ports. There is a large amount of ready-made code on the Internet that can be used to exploit software and services. (Center for Internet Security 2019, 34.)

2.10 Vulnerabilities

Vulnerability testing requires a strong security background and the highest level of trustworthiness. Even the best automated vulnerability tools produce misinterpreted alarms that are prevented by other actions. An environment can have two or more vulnerabilities that have a lower severity level than one high-level vulnerability, but when combined create a more serious threat to the organization. Some vulnerabilities may remain undetected by the tool, which may present a risk of exploitation. (Harris & Maymí 2016, 866.)

Zhang (2017) reports that Amazon EC2 on Windows and Linux operating systems contains outdated software with critical vulnerabilities. Amazon EC2 cloud has several Common Vulnerabilities and Exposures (CVE) in public images. (Zhang 2017, 30.)

2.10.1 Common Vulnerabilities and Exposures

Common Vulnerabilities and Exposures (CVE), established in 1999, maintains a list of the most common cyber security vulnerabilities. It has standardized identifiers for vulnerability notation, e.g. "CVE-1999-0067" refers to 1999, followed by a sequential number, which is reset annually. Various actors can refer to this identifier in their mutual communication. (MITRE.)

2.10.2 Common Vulnerability Scoring System

The Common Vulnerability Scoring System (CVSS) can be used to report the severity of a vulnerability. CVSS consists of three metrics groups: the Base group represents the unchangeable vulnerability properties, the Temporal group the variable properties, and the Environmental group represents the user environment. The Base score is between 0.0 and 10.0, and it can be presented as a vector string as following format: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N which is stands for: (FIRST 2019.)

- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: High
- User Interaction: None
- Scope: Unchanged
- Confidentiality: Low
- Integrity: Low
- Availability: None

CVSS is related to CVE so that it gives an indicator of the severity of each item of CVE. CVSS answers to question: Is this risky? However, it does not mean it is risky to every organization.

2.11 Preparation

There is so much data that it sets prioritization the biggest challenge. Here CVSS can be used to create the remediation plan. (Hammons 2015.)

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have published the security standards. The purpose of the ISO / IEC 27000 series is to define the ISMS family of standards. The accepted life cycle of security management is to plan, do, check, act to prevent security incidents. This comprehensive set of standards can be applied to organizations of all sizes. (Chen 2019, 193 -194.)

2.11.1 ISO 27000-series instructions

Information security must be part of project management methods. This way risks can be identified and addressed in a timely manner (SFS-EN ISO/IEC 27002:2017:en 2017, 13).

SFS-EN ISO/IEC 27002:2017:en guides that the organization needs responsible parties to monitor the vulnerabilities, assess the risks involved and take the necessary corrective action. Technical Vulnerability Management is part of a change management project. (2017, 53 - 54.)

SFS-EN ISO/IEC 27017:2015:en complements that the cloud client is responsible for managing some of the technical vulnerabilities. The client must identify these vulnerabilities and define their management processes. (2015, 16.)

An information system project should include security requirements at an early stage, as well as the identification and management of their processes. This can lead to a more cost-effective end result. (SFS-EN ISO/IEC 27002:2017:en 2017, 61.)

There are ready-made automated tools for security auditing that organizations should take advantage of. These include e.g. code analysis tools and vulnerability scanners. (SFS-EN ISO/IEC 27002:2017:en 2017, 68).

Security should be taken into consideration at the management level, and the developing teams should be encouraged to perform security tests during the development process. As defined by SFS-EN ISO/IEC 27002:2017:en, managers should ensure that the security requirements defined in the standards are met and that security tests are used regularly throughout the software development process. (2017, 84.)

Penetration tests or vulnerability scans can compromise the security of systems and should be treated with the utmost caution. These tests must be carefully documented. (SFS-EN ISO/IEC 27002:2017:en 2017, 84.)

SFS-EN ISO/IEC 27004:2016:en explains that many security incidents are done by exploiting known vulnerabilities. The longer a known vulnerability is not patched, the more likely it is to be exploited and the greater the risk involved. (2016, 14.)

2.11.2 Security Testing in the Development Workflow

Security tests performed during the software development lifecycle can provide the first assurance that software components are secure as seen in Figure 5. Source code analyses inform whether the source code is safe and written based on the required standards. The functionality of the software components can also be verified during runtime before integration into the main component. (Testing Guide Introduction.)

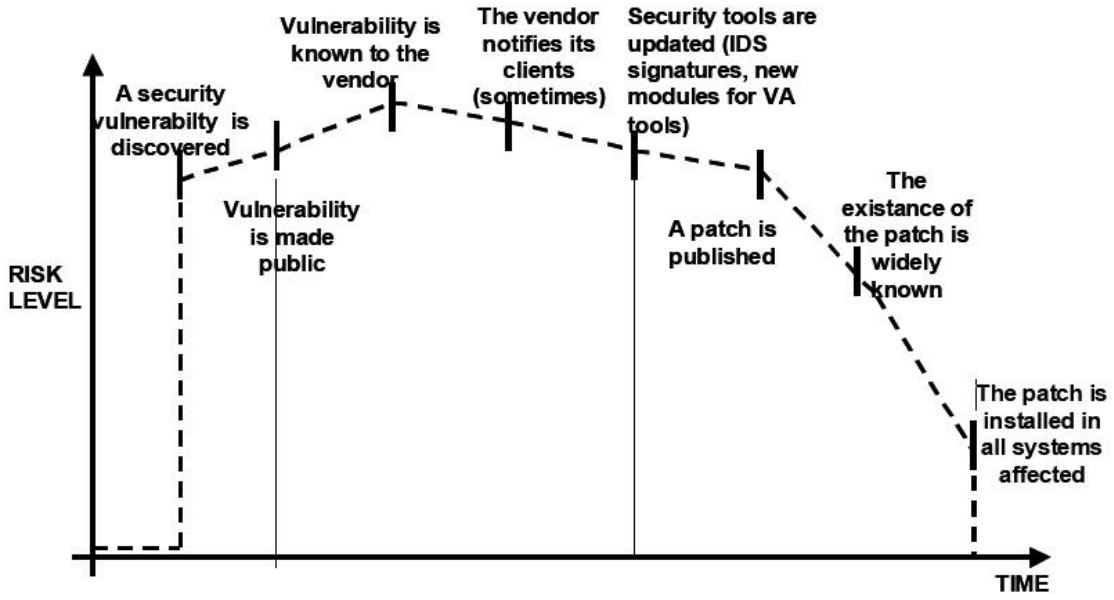

Figure 5. Window of vulnerability

2.12 Scanning tools

It is the customer's responsibility to install the latest security patches for the AWS environment. Vulnerability scanners on traditional networks do not work as efficiently on cloud networks as on local area networks and may not find all crucial vulnerabilities. Administrators should make sure all security patches are up to date and use the tools available to detect potential vulnerabilities. (Martinez 2019.)

Nessus is a vulnerability scanning program that works in various operating systems. It consists of a daemon, nessusd, which performs the scan int the target system, and nessus, the client that shows the progress and reports on the status of the scans. (The Nessus Family.)

Amazon has detailed instructions for customers to take security tests. For vulnerability scanning, Amazon offers its own service, Amazon Inspector. Amazon maintains and develops this service, which guarantees its continuity and supports its deployment within the organization. (What is Amazon Inspector?)

The idea of Amazon Inspector is similar to Nessus vulnerability scanner. In both the agent is installed into target instance where it performs a scan. It produces results according to the selected rules package.

Zhang (2017) clarifies that the Amazon Inspector security agent is installed on the virtual machines, where it monitors the operation of the instance from inside. The agent uses the CVE database to identify threats and investigates potential system vulnerabilities and security threats. (Zhang 2017, 47.) The author does not see this as an issue on this case because scanning is first run on pre-production instances, which gives comparable reports to compare with production instances. This requires that necessary vulnerability fixes are conducted in pre-production instances before provisioning to production.

2.13 Real risk of vulnerabilities

The biggest challenge is finding the most threatening vulnerabilities in their own environment. It is not advisable to start patching all vulnerabilities found in the environment but to try to focus on which are currently being exploited. This is illustrated in Figure 6. (Pokorny 2019, 45-46.)

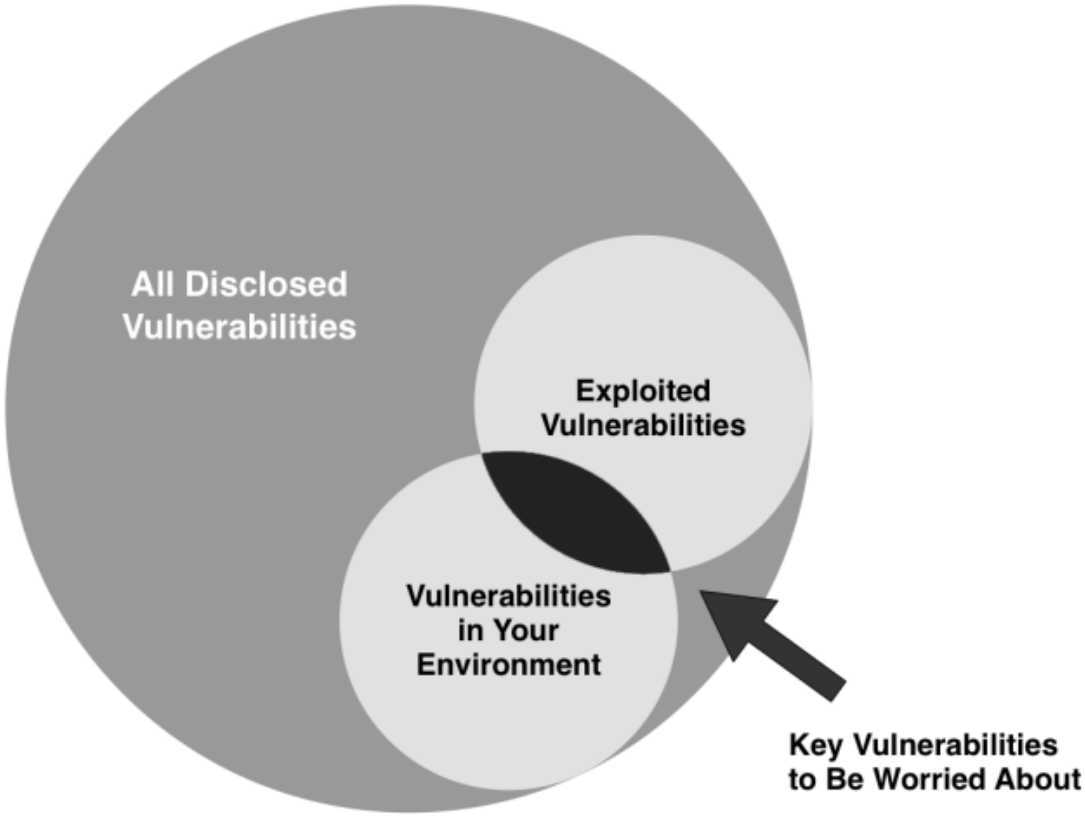

Figure 6. Vulnerabilities currently being exploited

An effective way to identify the actual risk is to look at its life cycle, which is illustrated in Figure 7 (Pokorny 2019, 50).

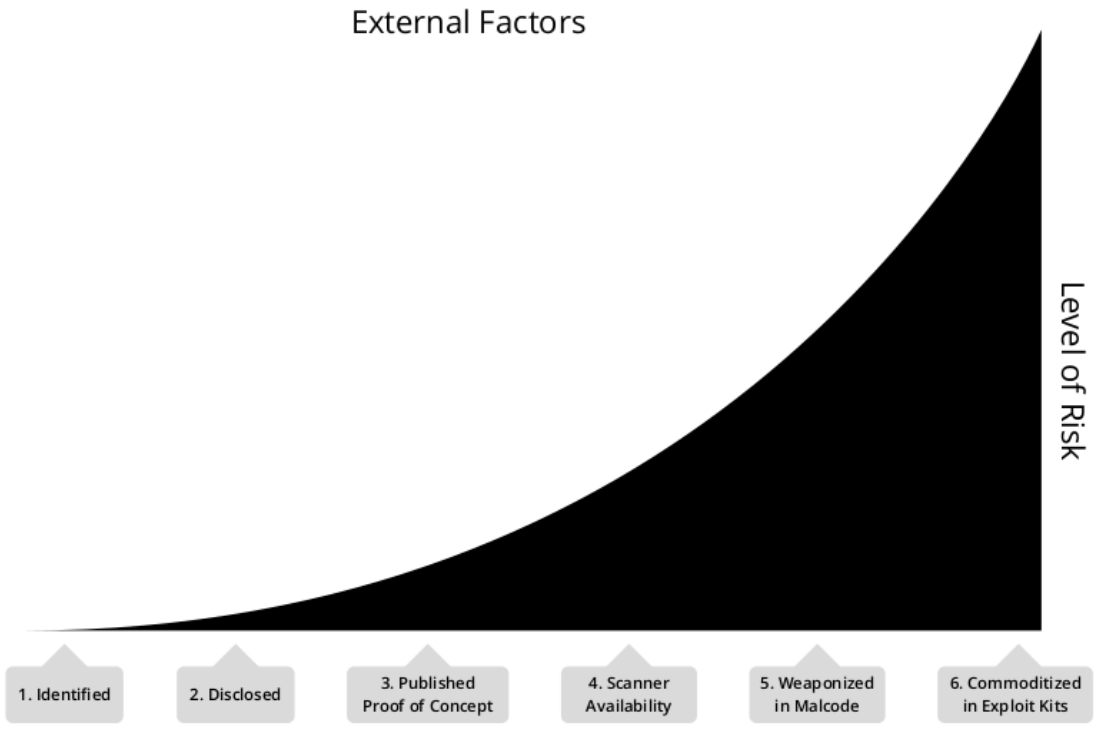

Figure 7. Risk growth factors

2.14 Amazon Inspector Rules Packages

Amazon Inspector uses Rules Packages to define performed tests. These Rules Packages are:

- Network Reachability
- Security Best Practices
- CIS Operating System Security Configuration Benchmarks
- Common Vulnerabilities and Exposures

2.14.1 Network Reachability

Shows findings about the ports that are reachable from the internet through an internet gateway. This rule can help if ports are misconfigured at the security group level. These scans do not require AWS Inspector Agent, so these can be considered more like an external scan. (What is Amazon Inspector?)

2.14.2 Security Best Practices

This is a set of certain rules which Inspector will check against and report of them. The Inspector lists these rules for the following topics: (What is Amazon Inspector?)

- “Disable Root Login over SSH
- Support SSH Version 2 Only
- Disable Password Authentication Over SSH
- Configure Password Maximum Age
- Configure Password Minimum Length
- Configure Password Complexity
- Enable ASLR
- Enable DEP
- Configure Permissions for System Directories”

2.14.3 CIS Operating System Security Configuration Benchmark

This rule checks the operating system against the CIS benchmarks to verify whether the server is following all the best practices mentioned in the CIS Benchmarks. This is a set of certain rules which Inspector will check against and report of them. (What is Amazon Inspector?)

2.14.4 Common Vulnerabilities and Exposures

Inspector rule CVE basically scan all the packages which are installed in the operating system and it verifies if an associated version has any vulnerabilities. If any vulnerabilities are found, they are listed with details in an Inspector console classified by their severities. (What is Amazon Inspector?)

3 Methodology

This chapter describes the method used to evaluate the suitability of Amazon Inspector to perform a vulnerability scan on instances in the Amazon cloud service. The detailed results of the reports were excluded from this thesis because the goal was to evaluate the used tool to scan the vulnerabilities. The contents of the reports are confidential and have been provided to the parties involved. The study addressed only significant findings from the reports, sorted by severity level, not details of the findings.

3.1 Data collection

Studying what vulnerabilities Amazon Inspector finds in the EC2 instance, Amazon Inspector is enabled and then the assessment rules are defined. A separate assessment template is created for each rules package so that each rules package can be run on its own. Scans are first run without Inspector Agent installation. When the first run is complete, the Inspector Agent is installed on the EC2 instance. After the Inspector Agent was installed and the scans re-run, the reported findings were compared to the first run. The vulnerabilities found were listed in the findings grid ordered by severity. The desired reports can be easily downloaded from the dashboard. This revealed how significant the difference is between external scanning and internal scanning.

3.2 Evaluation

The study presents the first step to implementing AWS cloud security best practices. The tool used is Amazon Inspector, which is readily available in the AWS services. Deploying the Inspector is easy and straightforward process. A prerequisite for running the Inspector tests were to get sufficient privileges from the administrator and to tag the EC2 instances properly. Then tagged instances were tested with the vulnerability scans. Installing and running Amazon Inspector itself is a simple process

but the research itself opens up new perspectives on the subject. The results of the report can be used from different perspectives depending on the different departments and roles of the company as discussed in the Conclusions chapter.

4 Results

This chapter presents the process how to prepare EC2 instance for vulnerability tests, how to enable Amazon Inspector, and creation of assessments with rules packages, followed by a description how to run scans, results of reports, and how to use them.

4.1 Select EC2 instance for scan

These instances are listed in EC2 Console where the link Instances is clicked to list all instances. The instances to be tested are selected from the list. These items are marked with tags as shown in Figure 8. The instance is tagged with; key = security, value = Testing.

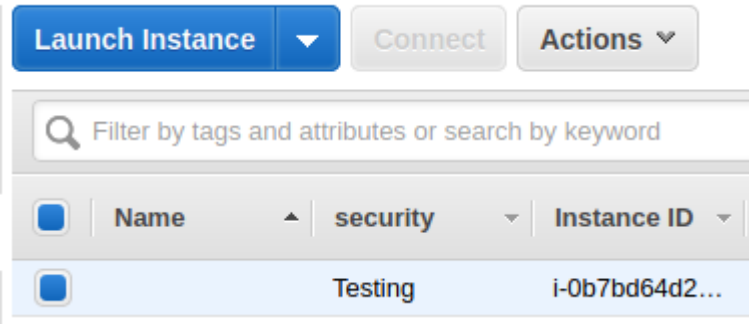

Figure 8. Tag EC2 instance for vulnerability scanning

The method described above informs the inspector that this instance is selected according to the vulnerability scans marked with the same tagging.

4.2 Enable Amazon Inspector

The administrator has granted sufficient privileges for the Inspector to use in order to take the necessary action. As the first action, the Amazon Inspector is opened in Amazon AWS Console and enabled in the Amazon AWS account.

The user starts using the Inspector as shown in Figure 9. The three steps shown in Figure 9, Install, Run, and Analyse, are not explained here. The start using the Inspector is commenced by clicking the button ‘Get started’.

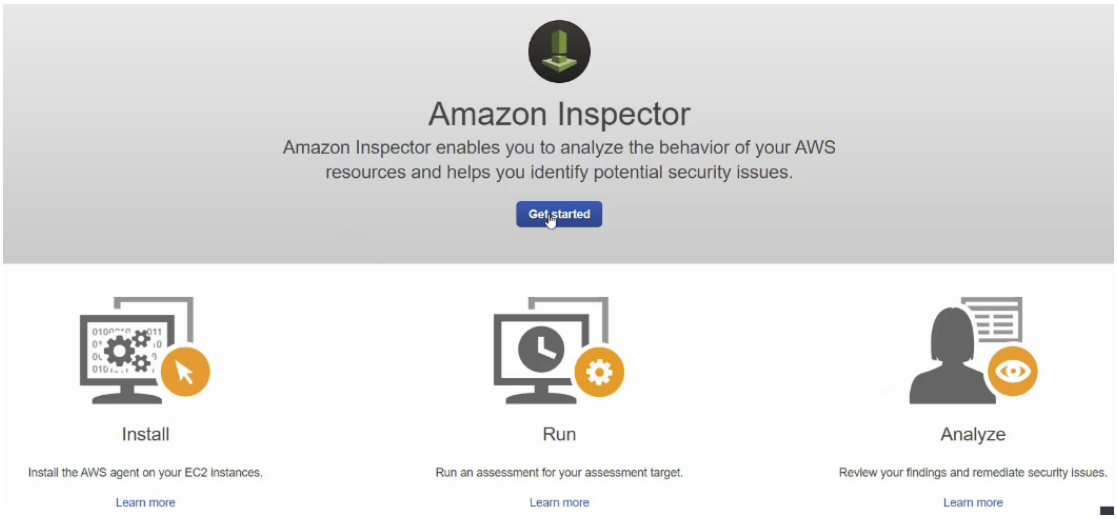

Figure 9. Getting started with the Inspector

On the Amazon Inspector home page, it is possible to schedule assessments, run assessments once, and open advanced setup as shown in Figure 10. These are skipped and taken to the Amazon Inspector dashboard page by clicking Cancel.

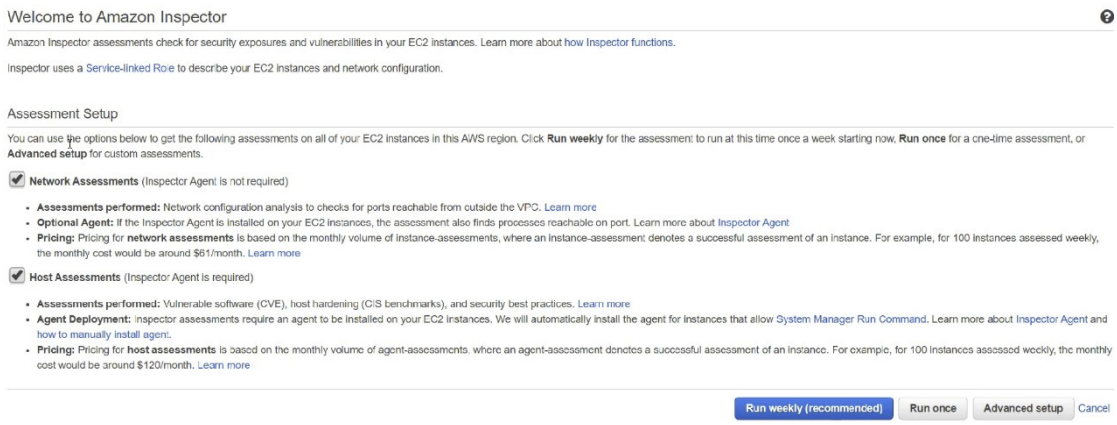

Figure 10. Assessment Setup choices on Inspector start page

Creating of assessments starts in the empty dashboard illustrated in Figure 11.

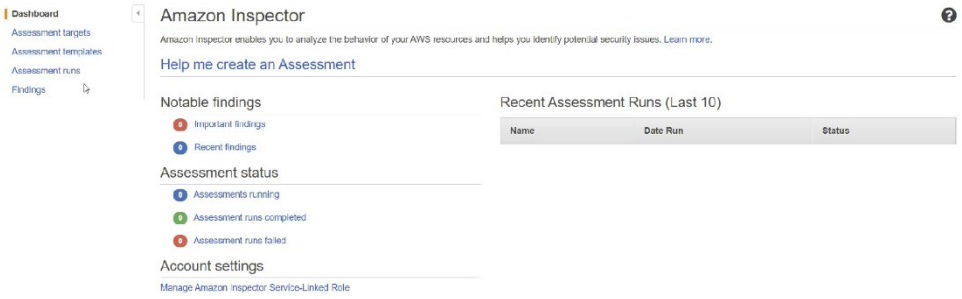

Figure 11. Clean Amazon Inspector Dashboard

4.3 Assessment Target

Assessment targets is opened by clicking Assessment targets link. By clicking Create button, as shown in Figure 12, a new assessment target form is opened.

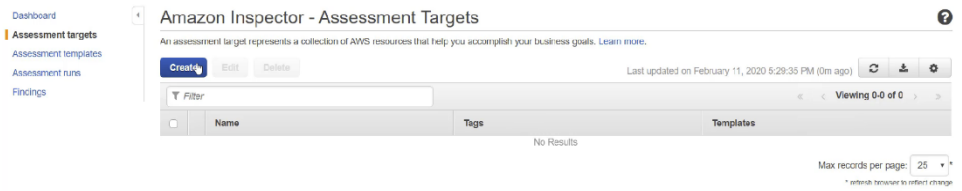

Figure 12. Create Assessment Target

The user creates assessment targets to define which EC2 instances will be scanned. In Figure 13 the option ‘All Instances’ runs all instances of the AWS account and region. This option is not selected, and the instances are selected manually. The form also has another check box that, when selected, installs the Amazon Inspector Agent on all EC2 instances under this assessment using the Run Command. This option is unchecked, and Inspector Agent is installed manually.

Targets are marked with Tags; key = security, value = Testing. These tags must be assigned to EC2 instances which to test as seen before.

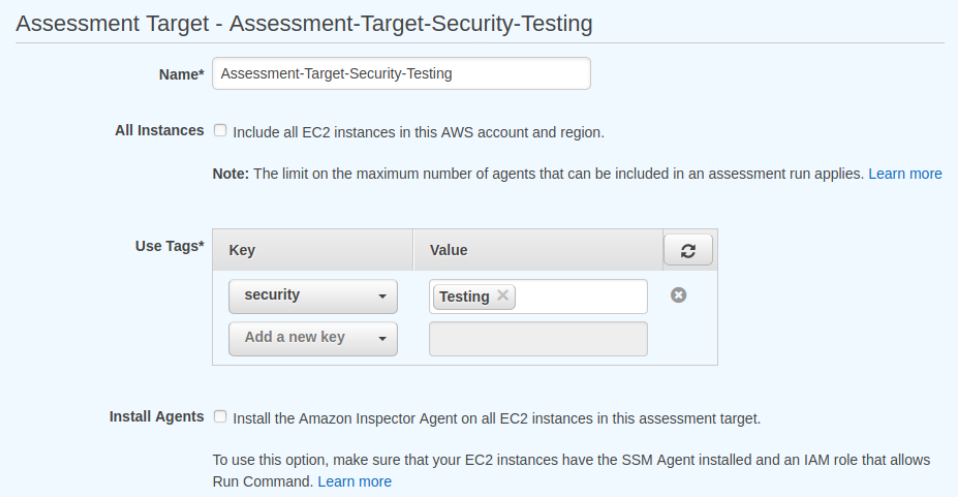

Figure 13. Create assessment target form

As shown above, the assessment target is connected to the EC2 instance marked with the same tag (see select EC2 instance for scanning). The next step is to create an assessment template before scan can be run.

4.4 Assessment Template

Assessment templates use an assessment target for tests. Templates define details for tests. The assessment template is associated with an assessment target which is picked on Target name popup field as shown in Figure 14. For Rules packages popup field, the Common Vulnerabilities and Exposures-1.1 is selected. Duration is one hour, as recommended. No SNS topics are selected. Tags are defined as an assessment target phase.

Findings made by the assessment template can be tagged in the section ‘Attributes added to findings’ to distinguish the reports from each assessment templates. Here tagging with ‘findings’ = ‘Vulnerabilities’. When the form is filled, it is saved and run.

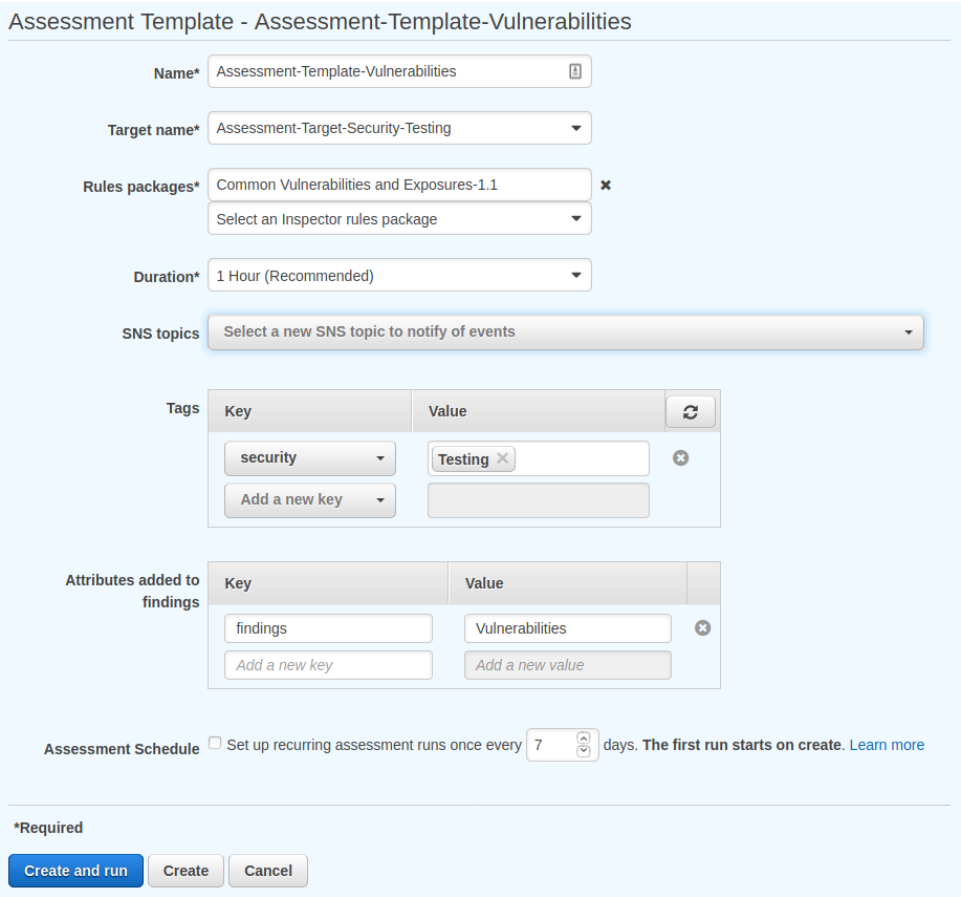

Figure 14. Assessment template definition form

4.5 Findings without Inspector Agent

One assessment template is created and run for each of the rules packages and the result is shown in figure “Amazon Inspector – Assessment Templates” (Figure 15).

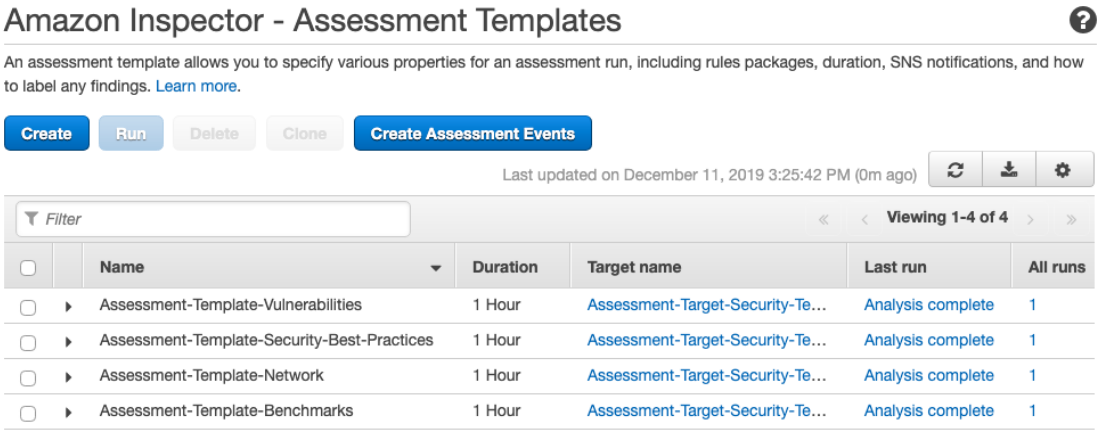

Figure 15. Amazon Inspector – Assessment Templates

It is remarkable that these runs have performed as they have, and they do not give plenty of results. Only Network Reachability reported 7 findings, where 2 was Low level and 5 Informational level severity as seen in Table 1.

Table 1. Vulnerabilities per Rules Packages without Inspector Agent

Rules Packages / Severity	Vulnerabilities	Security Best Practices	Network **Reachability**	Benchmarks
High	0	0	0	0
Medium	0	0	0	0
Low	0	0	2	0
Informational	0	0	5	0
Total	**0**	**0**	**7**	**0**

4.6 Install Inspector Agent

The next step is to install Inspector Agent into EC2 instances. This agent examines EC2 instances from inside and gives a great deal more information about security issues.

Amazon Inspector Agent can be installed from inside of EC2 instance. The following is an excerpt of installation process (The output has been removed for convenience):

Download agent from Amazon AWS:

[centos@ip-xxx-xxx-xxx-xxx ~]$ curl -O https://inspector-agent.amazonaws.com/linux/latest/install

Run installation:

[centos@ip-xxx-xxx-xxx-xxx ~]$ sudo bash install

4.7 Findings with Inspector Agent

After agent installation the vulnerability tests were run again, and the results were totally different as described in table “Vulnerabilities per Rules Packages” in Table 1. The new results can be seen in Table 2. Figure 16 illustrates the results.

Table 2. Vulnerabilities per Rules Packages with Inspector Agent

Rules Packages / Severity	Vulnerabilities	Security Best Practices	Network **Reachability**	Benchmarks
High	74	0	0	88
Medium	95	1	0	0
Low	6	0	3	0
Informational	0	0	8	9
Total	**175**	**1**	**11**	**97**

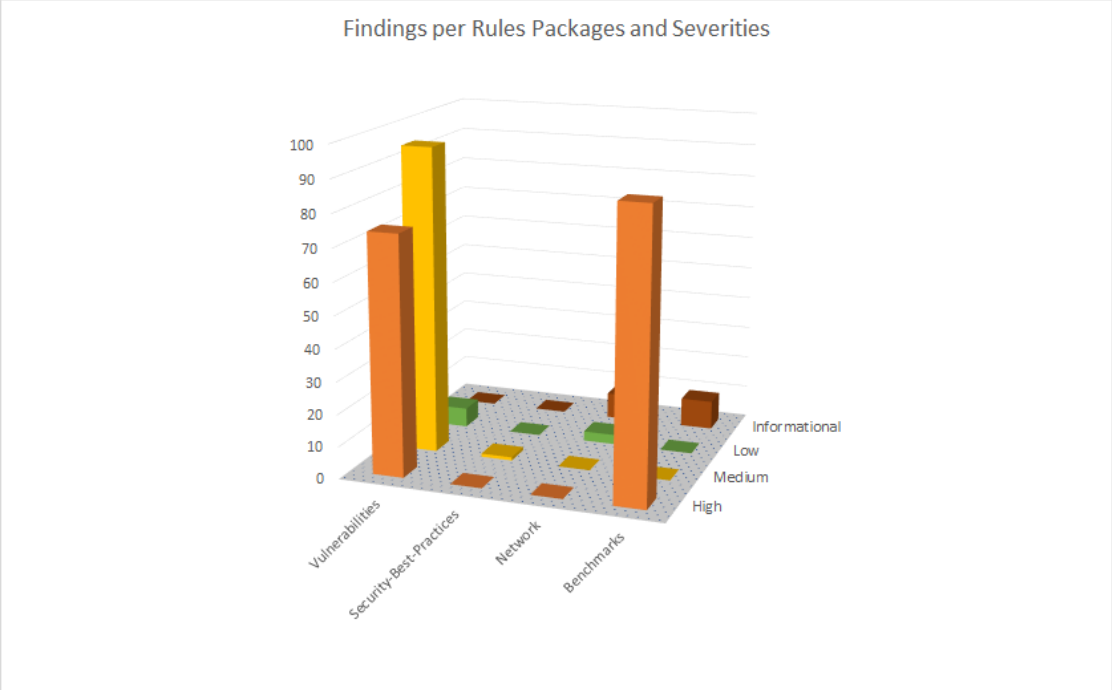

Figure 16. Findings per Rules Packages and Severities

62% of the significant findings are in the Vulnerabilities category and 34% in the Benchmarks rules packages category. The total number of significant observations in the Network Reachability and Security-Best-Practices category is very small, only about 4%. This gives a signal to resolve the significance of the observations of the first two categories for their own environment. Figure 17 shows the total number of findings.

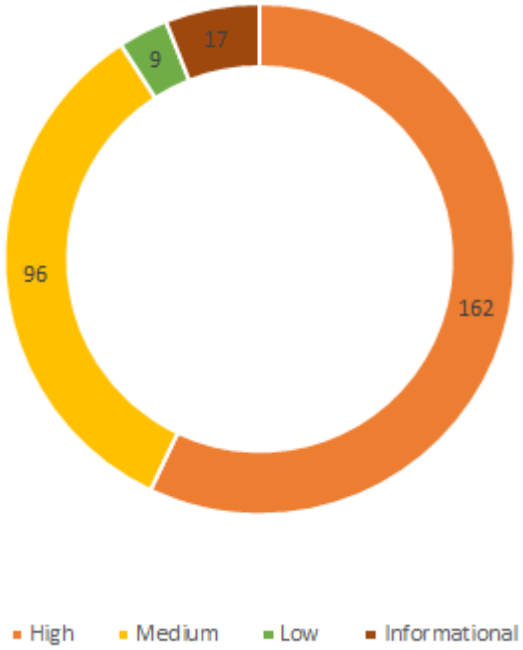

Figure 17. Total amount of Severities

Why are the numbers of findings in these two categories so large compared to the others?

The CVE Home site has information about total amount of CVE Entries which is more than 135,000 at the time of writing the thesis. New vulnerabilities are found continuously. (MITRE.) The existence of potential vulnerabilities has not been considered when configuring EC2 instances, so this explains the large number of vulnerabilities in the report.

The large number of CIS Benchmarks is because CIS Benchmarks supports following operating systems only: (Amazon Inspector)

- Amazon Linux 2 and 2014.09-2015.03
- CentOS Linux 6 and 7
- Red Hat Enterprise Linux 6 and 7
- Ubuntu Linux 14.04, 16.04, and 18.04 LTS
- Windows Server 2008, 2012, and 2016

In the other hand, these EC2 instances have not been selected with Amazon Inspector in mind and therefore the number may be large. If the Linux distribution in the EC2 instance does not support CIS Benchmarks, then it will result in a failed run.

The report is huge and has several issues. Some of them do not need actions to be performed, as mostly on Informational level. The content of the reports is confidential, and they have been provided to stakeholders.

4.8 Does this service work as expected, and if yes/no, why?

The goal was to scan for vulnerabilities from EC2 instances and the network. Amazon Inspector found a lot of significant findings, which was a positive surprise about the tool's operation. On the other hand, it should be noted that if the selected Linux distribution does not support CIS Benchmarks then the result is a failed run, which gives the user the wrong signal. If the selected Linux distribution does not support CIS Benchmarks then those tests will not be run for this instance. Anyway, a more preferred option is to seek to select operating systems that support CIS Benchmarks tests. After these reviews, it can be stated that this service works as expected.

4.9 Excerpt of findings

Below is an example of one of issues to clarify its contents:

ARN *arn:aws:inspector:<region>:xxxx*

Run name *Run - Assessment-Template-Security-Best-Practices - 2019-11-25T13:37:12.988Z*

Target name *Assessment-Target-Security-Testing*

Template name *Assessment-Template-Security-Best-Practices*

Start *11/25/2019 (GMT+2) (14 days ago)*

End *11/25/2019 (GMT+2) (14 days ago)*

Status *Analysis complete*

Rules package *Security Best Practices-1.0*

AWS agent ID *<agent-id>*

Auto scaling group *<AS-Group>*

Finding *Instance <instance-id> is configured to allow users to log in with root credentials over SSH, without having to use a command authenticated by a public key. This increases the likelihood of a successful brute-force attack.*

Severity *Medium*

Description

This rule helps determine whether the SSH daemon is configured to permit logging in to your EC2 instance as root.

Recommendation

*To reduce the likelihood of a successful brute-force attack, we recommend that you configure your EC2 instance to prevent root account logins over SSH. To disable SSH root account logins, set PermitRootLogin to 'no' in /etc/ssh/sshd_config and restart sshd. When logged in as a non-root user, you can use sudo to escalate privileges when necessary. If you want to allow public key authentication with a command associated with the key, you can set **PermitRootLogin** to 'forced-commands-only'.*

This example issue has medium level severity as seen above in *Severity* field. Extending this finding (as shown above) and clicking *"Show Details"* button (below Findings) opens detailed information of a Finding on JSON format. Below are two examples of *Medium* and *High-level* severity details, focused on *numericSeverity* and *severity* tags. *numericSeverity* can be used as an input for CVSS calculator.

Medium severity


```
"numericSeverity": 6,
  "recommendation": {
    "message": "To reduce the likelihood of a successful brute-force attack, we recommend that you configure your EC2 instance to prevent root account logins over SSH. To disable SSH root account logins, set PermitRootLogin to 'no' in /etc/ssh/sshd_config and restart sshd. When logged in as a non-root user, you can use sudo to escalate privileges when necessary. If you want to allow public key authentication with a command associated with the key, you can set **PermitRootLogin** to 'forced-commands-only'."
  },
  "schemaVersion": 1,
  "service": "Inspector",
  "serviceAttributes": {
    "assessmentRunArn": "arn:aws:inspector:<region>:<ID>:<target>",
    "rulesPackageArn": "arn:aws:inspector:<region>:<ID>:rulespackage/<id>",
    "schemaVersion": 1
  },
  "severity": "Medium",
```


The rest of output removed due to space saving.

High severity


```
"numericSeverity": 9,
  "recommendation": {
    "message": "Edit or create the file /etc/modprobe.d/CIS.conf and add the following line:\n
install hfsplus /bin/true"
  },
  "schemaVersion": 1,
  "service": "Inspector",
  "serviceAttributes": {
```

```
    "assessmentRunArn": "arn:aws:inspector:<region>:<ID>:<target>",
    "rulesPackageArn":
"arn:aws:inspector:<region>:<ID>:rulespackage/<id>",
    "schemaVersion": 1
  },
  "severity": "High",
The rest of output removed due to space saving.
```


Amazon Inspector gives a large amount of information in reports, detailing of resources in AWS and issues found. The report created by Inspector Agent is rich and comprehensive. The detailed information identifies the resource tested and the issue it is associated with. The contents of the message field expose the threat and provide guidance on how to fix it.

4.10 Use of Findings

As mentioned earlier, the content of the reports is confidential; however, the results are treated at the level of severity. The number of threats is enormous and should be taken seriously. Vulnerability management is limited out of this study; nevertheless, its rapid design and deployment is recommended to be prepared soon. The results of the report can be used as a tool for the purposes mentioned in Table 3.

Table 3. Utilization of vulnerability scanning

Stakeholder	**Perspective**	**Knowledge Derived**
Internal auditor, management	Artifact as proof of security compliance	What vulnerability scans reveal deviations about security standards
CISO, DevSecOps	Artifact as benchmark of threats	Principles for the construction of secure software and environment
QA, Dev	Artifact as improved security	A better secure software development process

5 Conclusions

The objectives set for this thesis were well defined and achievable. The research questions and the restrictions placed on the research guided the work towards the set goal.

The results show that Amazon Inspector itself does not find nearly all of the issues, but it requires the installation of Inspector Agent for maximum results. As mentioned earlier, even Inspector Agent may not find all the potential issues in the EC2 instance or network, as the resource status is constantly changing.

Deploying Amazon Inspector as a first step in security best practices is a good starting point for deploying other services because it exposes potential threats and vulnerabilities in instances of the organization. Amazon Inspector is part of the Security Hub; hence, the next best practice step could be to deploy Security Hub and its associated services. Managing reports generated by Inspector is a challenging task and managing vulnerabilities in them is also a great option for the next step in improving security.

The large number of issues identified by Inspector needs to be brought to the attention of project managers, product owners, and others to incorporate security testing into the software development process rather than as an extra step. Interpreting reports, prioritizing issues, and mitigating issues is a challenging task that requires a new kind of dedication from the team to achieve a secure result.

This study was very interesting and provided a good understanding of the need to develop security. Amazon's cloud service is a challenging and very engaging environment with a richness of services, which puts development of the security testing to the core of software development process.

6 Proposals for further research

This study raised ideas for possible further research topics to complement the work carried out so far. Adding automation to many tedious routines reduces the risk of errors and frees up employees for the right tasks.

The first challenge was vulnerability management due to the large amount of data provided by the report. This vulnerability management system could use artificial intelligence to go through and prioritize vulnerabilities. Vulnerabilities that threaten the organization need to be identified to gain an idea of the likelihood of their exploitation.

An internal information security audit could be conducted within the organization, which would provide the capability to obtain certification. This would reduce future needs for unexpected change because the organization would be prepared to head software development towards the standards.

The security logging and monitoring system could collect and categorize the information to be logged into its own categories. This logged information could be tracked through a centralized monitoring system, providing a single dashboard for real-time monitoring of all important events. Own applications' security logging could be a part of this system.

References

Amazon AWS Well-Architected whitepaper. 2019. PDF document on Amazon Web Services's website. Accessed on 12 October 2019. Retrieved from https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf

AWS Firewall Manager. Page on Amazon AWS's website. Accessed on 25 November 2019. Retrieved from https://docs.aws.amazon.com/waf/latest/developerguide/fms-chapter.html

AWS IoT Device Defender. Page on Amazon AWS's website. Accessed on 30 November 2019. Retrieved from https://docs.aws.amazon.com/iot/latest/developerguide/device-defender.html

AWS Lambda. Page on Amazon AWS's website. Accessed on 15 November 2019. Retrieved from https://aws.amazon.com/lambda

AWS Shield. Page on Amazon AWS's website. Accessed on 19 November 2019. Retrieved from https://docs.aws.amazon.com/waf/latest/developerguide/shield-chapter.html

AWS WAF. Page on Amazon AWS's website. Accessed on 19 November 2019. Retrieved from https://docs.aws.amazon.com/waf/latest/developerguide/waf-chapter.html

Center for Internet Security. 2019. CIS Controls v7.1. Accessed on 19 October 2019. Retrieved from https://www.cisecurity.org/controls/

Chen, L. 2019. Security, Privacy, and Digital Forensics in the Cloud. Singapore. John Wiley & Sons Singapore Pte Ltd.

Cloud computing with AWS. Page on Amazon AWS's website. Accessed on 2 February 2020. Retrieved from https://aws.amazon.com/what-is-aws/

FIRST. 2019. Common Vulnerability Scoring System, Version 3.1. Accessed on 3 December 2019. Retrieved from https://www.first.org/cvss/user-guide

Hammons, K. 2015. Vulnerability Management Isn't Simple ... (or, How to Make Your VM Program Great). North Texas ISSA. Accessed on 10 December 2019. Retrieved from https://www.youtube.com/watch?v=67Mz_pjlPSk

Harris, S. & Maymí, F. 2016. CISSP All-in-One Exam Guide, 7th Edition. McGraw-Hill Education.

Johannesson, P. & Perjons, E. 2014. An Introduction to Design Science. Springer International. ISBN 978-3-319-10632-8.

Martinez, J. 2019. 8 AWS Security Best Practices to Mitigate Risk. Paloalto Networks. Accessed on 20 November 2019. Retrieved from https://blog.paloaltonetworks.com/2019/02/8-aws-security-best-practices-mitigate-risk/

Mell, P. & Grance, T. 2011. The NIST Definition of Cloud Computing. National Institute of Standards and Technology. Gaithersburg.

MITRE. Page on MITRE's website. Accessed on 2 December 2019. Retrieved from https://cve.mitre.org/about

Pennington, A. 2019. GETTING STARTED WITH ATT&CK. MITRE. Accessed on 5 December 2019. Retrieved from https://www.mitre.org/sites/default/files/publications/mitre-getting-started-with-attack-october-2019.pdf

Pokorny, Z. 2019. The Threat Intelligence Handbook. Second Edition. Moving Toward a Security Intelligence Program. CyberEdge Group, LLC. Annapolis. USA.

Polar Electro. 2019. Who we are? Accessed on 30 October 2019. Retrieved from https://www.polar.com/uk-en/about_polar/who_we_are

SFS-EN ISO/IEC 27000:2017:en. 2017. Information technology. Security techniques. Information security management systems. Standards. Helsinki: Finnish Standards Association SFS.

SFS-EN ISO/IEC 27002:2017:en. 2017. Information technology. Security techniques. Code of practice for information security controls. Standards. Helsinki: Finnish Standards Association SFS.

SFS-EN ISO/IEC 27004:2016:en. 2016. Information technology. Security techniques. Information security management. Monitoring, measurement, analysis and evaluation. Standards. Helsinki: Finnish Standards Association SFS.

SFS-EN ISO/IEC 27017::2015:en. 2015. Information technology. Security techniques. Code of practice for information security controls based on ISO/IEC 27002 for cloud services. Standards. Helsinki: Finnish Standards Association SFS.

Testing Guide Introduction. Page on OWASP Foundation's webpage. Accessed on 8 November 2019. Retrieved from https://www.owasp.org/index.php/Testing_Guide_Introduction

The Nessus Family. Page on Tenable's website. Accessed on 2 September 2019. Retrieved from https://www.tenable.com/products/nessus

VPC Flow Logs. Page on Amazon AWS's website. Accessed on 18 November 2019. Retrieved from https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html

What Is Amazon CloudWatch? Page on Amazon AWS's website. Accessed on 4 December 2019. Retrieved from https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html

What Is AWS Config? Page on Amazon AWS's website. Accessed on 17 October 2019. Retrieved from https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html

What Is Amazon GuardDuty? Page on Amazon AWS's website. Accessed on 23 October 2019. Retrieved from https://docs.aws.amazon.com/guardduty/latest/ug/what-is-guardduty.html

What Is Amazon Inspector? Page on Amazon AWS's website. Accessed on 20 November 2019. Retrieved from https://docs.aws.amazon.com/inspector/latest/userguide/inspector_introduction.html

What Is Amazon Macie?. Page on Amazon AWS's website. Accessed on 22 October 2019. Retrieved from https://docs.aws.amazon.com/macie/latest/userguide/what-is-macie.html

What Is Amazon VPC? Page on Amazon AWS's website. Accessed on 19 November 2019. Retrieved from https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html

What Is AWS CloudTrail? Page on Amazon AWS's website. Accessed on 18 November 2019. Retrieved from https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html

What is AWS Key Management Service? Page on Amazon AWS's website. Accessed on 1 December 2019. Retrieved from https://docs.aws.amazon.com/kms/latest/developerguide/overview.html

What Is AWS Secrets Manager? Page on Amazon AWS's website. Accessed on 28 November 2019. Retrieved from https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html

What Is AWS Security Hub? Page on Amazon AWS's website. Accessed on 15 November 2019. Retrieved from https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html

What Is AWS Single Sign-On? Page on Amazon AWS's website. Accessed on 22 November 2019. Retrieved from https://docs.aws.amazon.com/singlesignon/latest/userguide/what-is.html

What Is AWS Systems Manager? Page on Amazon AWS's website. Accessed on 23 October 2019. Retrieved from https://docs.aws.amazon.com/systems-manager/latest/userguide/what-is-systems-manager.html

What Is IAM? Page on Amazon AWS's website. Accessed on 3 December 2019. Retrieved from https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html

Who is the OWASP Foundation? Page on OWASP Foundation's webpage. Accessed on 10 January 2020. Retrieved from https://owasp.org/

Williams, J. 2019. Whitepaper. Why Your Vulnerability Management Strategy Is Not Working - and What to Do About It. SANS Institute. Accessed on 11 November 2019. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/vulnerability-management-strategy-working-about-38938

Zhang, T. 2017. Detection and Mitigation of Security Threats in Cloud Computing. Dissertation. Princeton University. Electrical engineering.