Julkisen pilven sovellustuotteiden kyber-turvan varmistaminen

Juuso Alakoski

Opinnäytetyö, AMK
Toukokuu 2022
Kyberturvallisuus
Insinööri (AMK), tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Alakoski Juuso

Julkisen pilven sovellustuotteiden kyberturvan varmistaminen

Jyväskylä: Jyväskylän ammattikorkeakoulu. Toukokuu 2022, 43 sivua

Kyberturvallisuus. Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Nykypäivänä pilvipalveluiden turvallisuus on elintärkeää niiden yleistymisen johdosta. Käyttäjinä toimii merkittäviä yrityksiä sekä yksityiskäyttäjiä, joiden informaatioita ei haluta vuotaa ulospäin. Pilvipalveluiden tarjoajat ovatkin suuressa vastuussa ympäristöjensä turvallisuuden kanssa.

Toimeksiantona oli Pinja SaaS-pohjaisten testiympäristöjen kyberturvan varmistaminen Palo Alton Prisma Cloud pilvipalveluiden turvallisuuden hallintajärjestelmällä. Työssä perehdyttiin tarkemmin sovellustuotteiden konfiguraatioiden turvallisuuteen, sekä Prisma Cloudin käyttöönottoon.

Työn toimeksiantajana toimi ohjelmistoyhtiö Pinja, joka tarjoaa teollisuuden SaaS-ratkaisuja sekä muita digitalisaation kehittäviä ratkaisuja yrityksille.

Tutkimus suoritettiin integroimalla Palo Alton Prisma Cloud Pinjan käyttämään pilviympäristöön, sekä konfiguroimalla sen käyttöliittymä. Tarkoituksena oli saada selville, miten Cloud Security Posture Management -ratkaisu sai skannattua Pinjan pilviympäristöistä, sekä minkä tasoisia löydöksiä sieltä paljastuisi. Tutkimuksessa oli käytössä Palo Alto Prisma Cloudin Enterprise kahden kuukauden mittainen kokeiluversio, sekä Pinjan tuotteiden aktiiviset kehitysympäristöt. Kaikki havainnot olivat myös kerätty Prisma Cloudin omien oletus standardien sekä kriteeristöjen perusteella, eli itse luotuja hälytyksiä ympäristössä ei ollut.

Opinnäytetyön tutkimuksen perusteella selvitettiin Pinjan testiympäristöjen kyberturvan tila konfiguraatioiden kannalta. Tuloksista löytyi useita eri tasoisia hälytyksiä. Kuitenkin merkittävä osa vakavammista hälytyksistä oli false positive -tyyppisiä hälytyksiä, jotka ovat yleisiä kehitysympäristöissä. Tällaisia olivat esimerkiksi Azuren oman Defender -komponentin pois kytkentä tietokannoista sekä palvelimilta. Työssä syvennyttiin myös Azuren SQL-hälytyksiin, joita oli tullut useita erilaisia sekä eri tasoisia.

Avainsanat (asiasanat)

Pilvipalvelut, CSPM, kyberturvallisuus

Muut tiedot (salassa pidettävät liitteet)

jamk

Description

Alakoski Juuso

Ensuring cyber security for public cloud application products

Jyväskylä: JAMK University of Applied Sciences, May 2022, 43 pages

Cyber security. Degree Programme in Information and Communication Technology. Bachelor's thesis

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

Cloud computing is starting to be more used in the everyday usage in various companies. Securing those services is vital for the users and for the providers. Users for cloud services can be big companies or pri-vate persons. Although the users, cloud computing providers must retain their responsibilities for secure ser-vices.

The assignment was to check security of Pinja's SaaS solutions test environments using Palo Alto's Prisma Cloud trial version of cloud security posture management system. The work was focused on the security of configurations on those test environments and how to introduce it.

The work was commissioned by the software company Pinja which provides industrial SaaS solutions and other digital development solutions to companies.

Palo Alto's Prisma Cloud was integrated to the Pinja's cloud environment which is used to run those test environments. For the full usability Prisma Cloud needed its own user interface which was configured to work with Pinja's cloud environment. Aim was to scan the cloud environments using CSPM -methods and to check security of configurations for the test environments. Prisma Cloud Enterprise was a two-month trial version, which allowed to see what kind of alerts there might be. Prisma Cloud has its own standards for the scans so there weren't any custom rules inside the scans.

Based on this thesis Pinja's test environments included some various of different level alerts. Test environ-ments didn't include any critical alerts and most of the higher level of alerts were false positive alerts. False positive alerts were found due to use of development environment. For example many of the High level alerts were set because of turning off Microsoft Azures own Defender component in the databases and vir-tual servers. In the results of this thesis was also delved into Azure SQL alerts which had come in several dif-ferent status and different levels.

Keywords/tags (subjects)

Cloud computing, CSPM, Cyber security

Miscellaneous (Confidential information)

Sisältö

Kuviot

Taulukot

Lyhenneluettelo

AD	Active Directory
ADS	Advanced Data Security
BSI	Bundesamt für Sicherheit in der Informationstechnik
BYOK	Bring Your Own Key
CSA	Cloud Security Alliance
CSPM	Cloud Security Posture Management
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
Katakri	Kansallisen turvallisuusauditointikriteeristö
LAN	Local Area Network
NIST	National Institute of Standards and Technology
Paas	Platform as a Service
PiTuKri	Pilvipalveluiden turvallisuuden arviointikriteeristö
Saas	Software as a Service
SOC	Security Operational Center

SQL	Structured Query Language
TDE	Transparent Data Encryption
WAN	Wide Area Network

1 Johdanto

Viimeisen vuoden aikana kyberturvallisuuden näkyminen medioissa on kasvanut radikaalisti. Puhutaan kyberiskuista, tietomurroista ja muista rikoksista verkkoinfrastruktuuria kohtaan. Pilvipalveluiden yleistyessä, niiden käyttäjämäärät kasvavat reilusti ja sitä kautta markkinat paisuvat suuremmiksi. Julkisen pilven sovellustuotteet ovat nostaneet koko ajan päätään uusien verkkosovellusten tulossaan markkinoille, ja näin ollen niistäkin on löydetty erilaisia haavoittuvuuksia ja vikoja.

Pilvipalveluiden markkinoilta löytyy useita erilaisia vaihtoehtoja, joilla pystyy tarjoamaan vahvempaa turvaa omalle tuotteelleen erilaisia tieto- ja kybermurtoja kohtaan. Pilvipalveluiden tarjoajilla on omat vaihtoehtonsa tähän ongelmaan, mutta markkinoilta löytyy myös laajasti erilaisia kolmansien osapuolien tarjoamia sovelluksia. Kolmansien osapuolien sovellusten käyttömahdollisuudet ovat tietenkin laajemmat, koska niiden avulla pystytään usein seuraamaan kokonaisuudessaan käytössä olevan pilvi-infrastruktuurin toimintaa. Näin ne eivät rajoitu ainoastaan palveluntarjoajan myytyyn ympäristöön.

Pilvipalveluiden turvallisuuden hallinta (CSPM) -ratkaisut ovat nostaneet päätään myös viime vuosina palveluiden yleistymisen johdosta. Useat toimijat myyvät tuotettaan osakseen juuri tähän tarkoitukseen, tai sitten vaihtoehtoisesti huomattavasti laajemmalle käytölle. Niiden käyttö perustuu ihmisten luomiin virheellisten konfiguraatioiden valvontaan, jotka ovat inhimillisiä virheitä, mutta voivat olla kuitenkin yritykselle kohtalokkaita menetyksiä. CSPM-ratkaisut voivat valvoa tehokkaasti jo valmiina olevia julkisen pilven ympäristöjä, sekä niiden luomisvaihetta, jossa iso osa konfiguraatiovirheistä tapahtuu.

Automatisoinnilla on myös merkittävä vaikutus CSPM-toiminnan kanssa, koska yhä useammin kaikki halutaan tehdä mahdollisimman nopeasti ja vähällä manuaalisella työllä. CSPM-ratkaisut voivat edistää automatisoitujen pilveen lisättävien järjestelmien kyberturvaa tehokkaasti, koska ne käyvät sen luonnin aikana läpi kaikki käyttöjärjestelmästä haavoittuvuuksiin. Näin ollen myös luontitiedostoihin määritetyt konfiguraatiot testataan ja tarkastetaan erilaistan haavoittuvuuksien ja standardien mukaisesti. Tämän avulla voidaan vähentää merkittävästi automatisoituihin pilven käyttöjärjestelmien konfiguraatiovirheitä ihmisen puolesta. Käyttäjälle tämä näkyy merkittävästi

ajankäytössä, koska sen avulla voidaan välttää jokaisen binääripaketin haavoittuvuuksien selvittäminen, minkä ansiosta tuotteesta tulee tehokkaammin huomattavasti turvallisempi.

1.1 Tutkimuksen tavoite

Pilvipalveluiden turvallisuuden hallintajärjestelmien tuleminen markkinoille on saanut luotua kulttuuria turvallisemmista pilvipalveluista. Sen vuoksi erilaisten CSPM-ratkaisujen käyttäminen on laajentunut. Tutkimuksessa perehdytään niiden vaikutuksiin pilvipalveluiden turvallisuudessa julkisen pilven sovellustuotteiden kanssa. Miksi niiden käyttöä suositellaan ja mitä ne tekevät luodakseen turvallisemman pilviympäristön?

Työn toimeksiantajana toimi ohjelmistoyhtiö Pinja, jonka sovellustuotteita työssä käytettiin. Työssä perehdyttiin kahden Pinjan ylläpitämän julkisen pilven testiympäristön tietoturvaan, käyttäen Palo Alton Prisma Cloud CSPM-ratkaisua. Tarkoituksena oli selvittää ympäristöjen turvalliset konfiguraatiot, sekä miten Prisma Cloud huomaa ja toteuttaa kyseiset skannaukset. Tavoitteena on saada opinnäytetyön avulla tietoon testiympäristöjen konfiguraatioiden tila, liittyen sen mahdollisiin haavoittuvuuksiin tai konfiguraatiovirheisiin. Pinjan molemmat ympäristöt käyttävät Azuren pilvi-infrastruktuuria toimiakseen, joka on yksi Prisma Cloudin tukemista pilviympäristöistä. Tutkimuksen mahdollistamiseksi Prisma Cloud tuli integroida toimimaan Pinjan Azure -ympäristöissä, jonka lisäksi Prisma Cloudin oma käyttöliittymä täytyi konfiguroida yhteensopivaksi juuri kyseisten ympäristöjen kanssa. Tutkimus suoritettiin kahden kuukauden ajaksi saadulla Prisma Cloud Enterprise version kokeiluversiolla, joka on tarkoitettu juuri julkisen pilven kyberturvan valvomiseen ja tehostamiseen.

Tutkimuksen tavoitteena oli selvittää, voidaanko Palo Alton Prisma Cloud tuotteilla kehittää Pinjan ympäristöjen turvallisuutta. Koska Prisma Cloud on pilvipalveluihin keskittyvä sovellus, valittiin Pinjan testiympäristöistä siihen sopivat julkisen pilven testialustat. Tarkoituksena oli saada käsitys siitä, mitä uutta Prisma Cloud voisi tuoda Pinjalle kyberturvaan liittyen. Työssä päätettiin keskittyä tarkemmin juuri heidän CSPM-ratkaisuunsa, joka tarkastelee sovellukset tarkemmin haavoittuvuuksien ja konfiguraatiovirheiden kannalta.

Julkisen pilven sovellustuotteiden konfiguraatioiden merkitys on todella laaja toiminta, jonka johdosta niihin tulisi panostaa aina. Tutkimuksessa haluttiinkin perehtyä siihen, miksi konfiguraatioiden merkitys on niin suuri, ja varsinkin niiden muokkaaminen. Joissain tilanteissa saatetaan ajatella, että valmiiksi luodut konfiguraatiot ovat riittävät omaan tarkoitukseen, eikä niitä tarvitse enää muokata. Kuitenkin niiden merkitys saattaa olla huomattavasti suurempi, jos oletuskonfiguraatiot ovat määritelty muutama vuosi sitten. Kyseisen määrityksen jälkeen on oletettavasti tullut uusia versioita eri osista käyttöjärjestelmiä tai binäärejä. Ne ovat tulleet mahdollisesti vain parannusten takia, mutta hyvin todennäköisesti myös haavoittuvuuksien takia. Näin ollen vanhat oletusmääritykset konfiguraatioissa voivat olla merkittävän haavoittuvaisia, eikä niiden tarkastamiseen käytetä kiireen johdosta aikaa.

2 Teoreettis-käsitteelliset lähtökohdat

2.1 Pilvipalvelut

Pilvipalvelu tarkoittaa verkon yli saavutettavaa tietojenkäsittelypalvelua ja -kapasiteettia, jossa voidaan hyödyntää sen mahdollistamaa joustavien ja skaalautuvien resurssien malli, joka on osakseen automatisoitu itsepalveluperiaatteella tuotettavaksi. Valtiovarainministeriön julkisen hallinnon pilvilinjauksien käyttämiin käsitteisiin, sekä Natonal Institute of Standards and Technology (NIST) -määritelmiin. (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020)

Pilvipalvelut mahdollistavat kaikille sen käyttäjille pääsyn jaettuun verkkoon, joka voi pitää sisällään erilaisia palvelimia, tallennustiloja tai sovelluksia. Tämän ansiosta jaettujen verkkojen sisälle pääsemin vaatii ainoastaan verkkoyhteyden kyseiseen verkkoon, eikä se näin ollen vaadi läsnäoloa tietyn laitteen ääressä. NIST:n määritelmien mukaan pilvipalveluiden toimintamalli perustuu viidestä välttämättömästä ominaisuudesta, kolmesta erilaisesta palvelumallista sekä neljästä eri käyttömallista, joita käsitellään tarkemmin kappaleissa 2.1 ja 2.2. (Mell, P. & Grance, T. 2011)

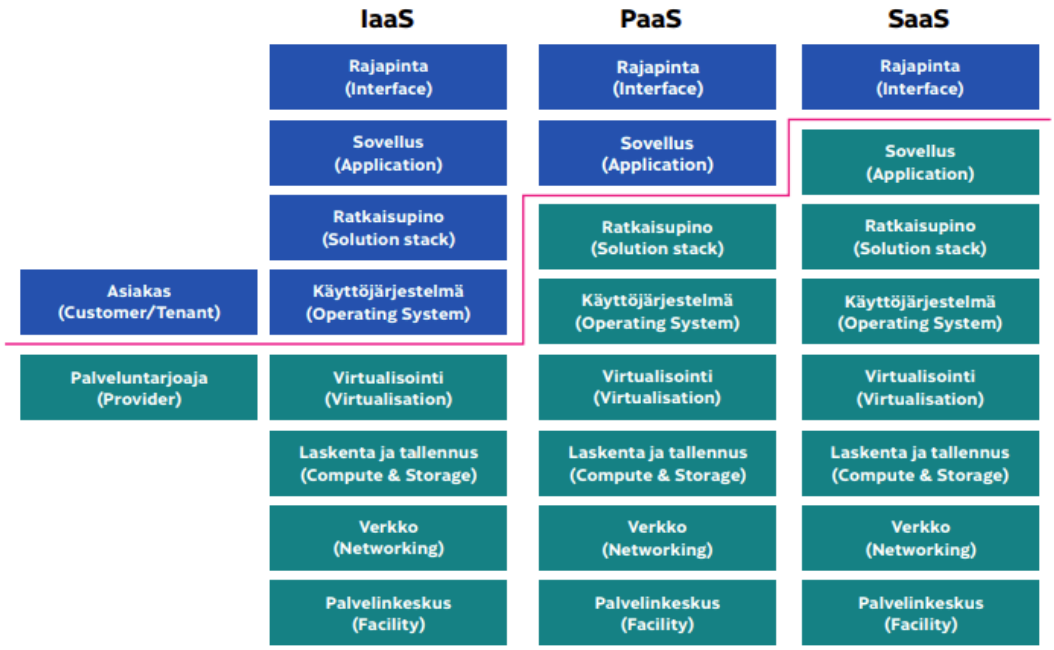
Myös pilvipalveluteknologioiden tuomat edut ovat suuri syy, miksi niiden pariin yritetään siirtyä. Näitä ominaisia etuja on valtiovarainministeriön mukaan kustannustehokkuus, skaalautumiskyky, tietoturva, energiatehokkuus, joustavuus ja innovatiivisuus (Valtiovarainministeriö 2018). Pilvipalvelut myös mahdollistavat pienemmille yrityksille mahdollisuudet hankkia konesaleilta tehokasta

palvelintilaa omaan käyttöönsä, ilman että sen täytyy hankkia kokonaista konesalia itselleen. Tämän ansiosta kulut eivät nouse niin suuriksi, koska ostettaessa pilvipalveluita, kuluttaja maksaa vain siitä mitä se käyttää. Oman konesalin kanssa tulevaisuuden suunnitelmat ovat huomattavasti kriittisempiä. Käyttäjän tulee suhteuttaa tulevaisuuden tarpeet kyseisen hetken käyttötarpeeseen, jolloin laitteiden skaalaus on tärkeää. Heikompi tehoisten palvelinten ostaminen alkuun on hyvä ratkaisu, jos yrityksen käyttökapasiteetti ei tule nousemaan merkittävästi lähivuosina. Yritys voi ostaa konesaliin liian tehokkaat palvelimet, mutta niiden suhteellinen käyttökustannus saattaa olla liian iso. Tällöin käyttäjä on ajatellut mahdollisesti liian pitkälle tulevaisuuteen. Pilvipalveluissa tämä tilanne on poistettu, koska suurista konesaleista saa usein ostettua nopeastikin lisää palvelin- tai tallennustilaa, joka mahdollistaa järkevänä pysyvän nousun myös sen kustannuksissa.

2.2 Palvelumallit

Yleisimmin käytetyt pilvipalveluiden palvelumallit ovat Infrastructure as a Service (IaaS), Platform as a Service (PaaS) ja Software as a Service (SaaS). Jokainen näistä palvelumalleista toimii erilailla asiakkaan ja palveluntarjoajan välillä, mutta käyttötarkoitus on kuitenkin hyvin samanlainen. Erilaisia palvelumalleja on myös tullut markkinoille viime vuosina, joissa on pieniä muutoksia asiakkaan ja palveluntarjoajan hallitsevissa kohteissa. PiTuKri:ssa (Pilvipalveluiden turvallisuuden arviointikriteeristö) määritellään asiakkaan ja palveluntarjoajan välistä vastuunjakomallia tyypillisellä tasolla Suomessa, joka on näkyvissä kuviossa 1. Siinä kerrotaan tarkemmin kuinka eri palvelut ja osa-alueet jakautuvat yleisimpien pilven palvelumallien mukaisesti asiakkaan ja palveluntarjoajan välillä.

(Pilvipalveluiden turvallisuuden arviointikriteeristö 2020)



Kuvio 1. Vastuunjakomalli (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020)

IaaS-mallissa palveluntarjoaja tarjoaa asiakkaalle pilvi-infrastruktuurin, johon asiakkaalla ei ole hallintaa. Kuitenkin asiakkaalla on mahdollisuus itse perustaa tallennustilaa, käytössä olevia sovelluksia, palvelimia sekä verkkoyhteyksiä. Palveluntarjoajalle jää siis vastuulleen fyysiset resurssit, joista kapasiteettia tarjotaan, sekä mahdollisesti jotain osia asiakkaan hallitsemista osuuksista, joita se ei voi itse toteuttaa. IaaS-mallissa asiakas on myös itse vastuussa konfiguraatioista, ohjelmistoista sekä käytettävistä resursseista. (Mell, P. & Grance, T. 2011)

PaaS-malli on IaaS-malliin verrattuna hieman kevyempi asiakkaalle. Asiakas ei hallitse tässä mallissa juuri mitään muuta kuin omia luomiaan tai hankittuja sovelluksiaan, sekä rajapintaa. Usein PaaS-mallia käytetäänkin erilaisten sovellustuotteiden luomisessa koodin kirjottamisvaiheessa. PaaS:ssa palveluntarjoaja tarjoaa asiakkaalleen infrastruktuurin, sekä IaaS-malliin eroten käyttöjärjestelmänkin valmiiksi. (Mell, P. & Grance, T. 2011)

SaaS-malli on asiakkaan kannalta heidän ylläpidettävään kaikista helpoin. Siinä palveluntarjoaja vastaa koko pilvi-infrastruktuurista. Tähän kuuluvat myös verkko, palvelimet, käyttöjärjestelmät, tallennustila sekä yksittäiset sovellukset. Asiakkaan ei tarvitse siis valvoa tai hallita näistä mitään, vaan he voivat keksittyä omaan rajapintaansa ainoastaan. SaaS-malliset palvelut toimivat usein

verkkoselaimessa olevalla käyttöliittymällä, tai sitten omalla ohjelmakohtaisella käyttöliittymällä. Myös tässä opinnäytetyössä käytetyt Pinjan sovellukset ovat molemmat SaaS-mallisia sovelluksia. (Mell, P. & Grance, T. 2011)

2.3 Pilvipalveluiden toteutusmallit

Pilvipalvelut jaetaan sekä NIST:in, että PiTuKri:n mukaisesti neljään yleisimpään toteutusmalliin. Näitä malleja on yksityinen pilvi (private cloud), yhdistelmäpilvi (hybrid cloud), yhteisön yhteisöpilvi (community/government cloud) sekä julkinen pilvi (public cloud). Kuviossa 2 on kuvattu kaavamaisesti, miten pilvipalveluiden toteutusmalleja todellisesti käytetään. (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020)

	Infrastructure Owned By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third-Party Provider	Third-Party Provider	Off-Premises	Untrusted
Private/ Community	Organization / Third-Party Provider	Organization / Third-Party Provider	On-Premises / Off-Premises	Trusted
Hybrid	Both Organization & Third-Party Provider	Both Organization & Third-Party Provider	Both On-Premises & Off-Premises	Trusted & Untrusted

Kuvio 2. Pilven toteutusmallien kaavio (Security guidance for critical areas 2017)

Ruparelia (2016) kertoo, että yksityisen pilven käyttö vaatii usein oman laaja-alaisen verkon (WAN) tai sitten lähiverkon (LAN). Näin ollen niiden käyttö on yleistä yritysmaailmassa, joka voi helposti rajoittaa oman WAN-verkkonsa yrityksen ulkopuolisilta henkilöiltä esimerkiksi palomuurin avulla. LAN-verkkona voi toimia esimerkiksi yrityksen toimiston sisäverkko, tai sitten yksityisen henkilön kotiverkko. Yksityisen pilven ylläpitäjänä voi toimia organisaatio itse, tai sitten vaihtoehtoisesti kolmas osapuoli. Näin ollen sen infrastruktuuri voi sijaita joko organisaation omassa paikallisessa konesalissa, tai sitten vaihtoehtoisesti kolmannen osapuolen ulkopuolisessa konesalissa. Esimerkkinä voi olla myös oma kotiverkko, jossa yksityisellä henkilöllä on oma yksityinen pilvi, joka yhdistää esimerkiksi varmuuskopiopalvelimen, synkronointipalvelun sekä suoratoistopalvelimen käyttämällä

langatonta lähiverkkoa. Yksityistä pilveä voidaan käyttää myös rajoitetuissa olosuhteissa internetin kautta, mutta silloin niihin pitää lisätä tehokkaat pääsyrajoitukset, jotta vain halutut henkilöt voivat palveluiden sisälle. (Ruparelia 2016)

Hybridipilvi on kahden tai useamman pilven käyttöönottomalli, jossa käytetään kapselointia. Siinä voi olla yhdistettynä mitä tahansa pilvipalveluiden muita toteutusmalleja (julkinen, yhteisö tai yksityinen). Hybridipilven voi myös muodostaa esimerkiksi muutamasta erillisestä julkisesta tai yksityisestä pilvestä, joten siihen ei tarvitse sekoittaa välttämättä erilaisia toteutusmalleja. Hybridipilveksi voidaan myös kutsua tilannetta, jossa pilviympäristö on yhdistetty suoraan perinteiseen konesaliin. (Ruparelia 2016)

Yhteisöpilvissä on useamman eri organisaation välille jaettu pilvi-infrastruktuuri, joka sisältää yhteiset tavoitteet tai vaatimukset pilven ympäristöstä. Erona tässä periaatteessa on internetin kautta toimitetut pilvipalvelut, jolla se eroaa yksityisestä pilvestä. Yhteisöpilvissä voidaan rajata myös sen toiminta-aluetta. Esimerkiksi sillä voidaan luoda vain Euroopan unionin oma yhteisöpilvi, joka toimii EU-maissa. Näin ollen sinne ei voi päästä muualta. Yhteisöpilven toimintaa voidaan myös rajata monella eri muulla tavalla. Esimerkiksi terveydenhuollon tarjoajilla voi olla yhteiset pilvipalvelut, joihin pääsee heidän omilla tunnuksillaan. (Ruparelia 2016)

Ruparelian mukaan julkisen pilven toimintatapa perustuu sen saatavuuteen yksityisen tai rajoitetun verkon sijaan internetin kautta. Tässä tapauksessa palveluntarjoaja omistaa kyseisen pilviympäristön, mutta sitä voidaan jakaa asiakkaille internetin kautta. Julkinen pilvi on internetin peruskäyttäjälle se yleisin vaihtoehto pilven toteutusmalleista, koska ne tarjoavat usein valmiin infrastruktuurin, alustan, ohjelmistot sekä tietoja ja liiketoimintaprosesseja valmiina palveluina. Kuitenkin julkiseen pilveen liittyy usein jonkinlainen kuukausimaksu, jos sitä käyttää internetin kautta suoraan. Tällaisia palveluja ovat muun muassa Microsoft Office 365, Amazon EC2 ja Google Docs. Kaikilla näillä palveluilla on yhteinen kuukausittainen käyttökustannushintamalli, jonka mukaan asiakkaan käyttämien palveluiden perusteella hänelle määritetään juuri oikea kuukausimaksuhinta. (Ruparelia 2016)

3 Pilvipalveluiden turvallisuuden hallinta

Pilvipalveluiden turvallisuuden hallinta on prosessi, jonka avulla voidaan automatisoida, valvoa ja tarkastella monipilviympäristöjä. Niiden toiminta on perustunut kykyyn analysoida jokainen havaittu haavoittuvuus, sekä arvioida sen riskit. Nykyään haavoittuvuuksia on niin paljon erilaisissa tietokannoissa, joten kaikkien niiden havainnointi ja arviointi on mahdotonta. Ongelmana on myös avoimen lähdekoodin haavoittuvuudet, joilla ei esimerkiksi ole minkäänlaista CVE-merkintää. Näin ollen CSPM on muuttunut viime vuosien aikana perehtymään enemmänkin ihmislähtöisiin ongelmiin sekä haavoittuvuuksiin. CSPM mahdollistaa sovelluksen suojauksen sen kehityksestä aina pilvipalvelussa käyttöönottoon, jonka ansiosta se toimii hyvin juuri julkisen pilven kehitystuotteiden kanssa. Sen avulla on pääsy erilaisiin tietoturvaprosesseihin, joiden avulla voidaan seurata haavoittuvuuden hallintaa sekä konfiguraatioiden tilaa. (Bulut, M., Hwang, J. 2021)

Gilliksen (n.d) määritelmän mukaan CSPM käytetään nykyisin yrityksissä, jotka ovat siirtäneet palvelujansa pilvipalveluihin. Sen automatisoitu toiminta kyberturvan puolella mahdollistaa resurssien siirtämisen jatkuvasta tarkastamisesta ympäristön rakentamisen ja ohjelmoinnin aikana. DevOps kehittymisen ansiosta lopullisen tuotteen virheiden pääsy tuotantoon vähenee, mikä tulee myös vähentämään tuotannon korjaamista tietoturvan takia (Puzas, D. 2021). Pääsääntöisesti käytössä on erilaiset hybridi- ja yhteisöpilvet, joiden kyberturvallisuuden valvominen toimii helposti CSPM-sovelluksen avulla. CSPM on yleisesti suunniteltu IaaS-ympäristölle, mutta sitä voidaan myös konfiguroida toimimaan SaaS- ja PaaS-ympäristöille. (Gillis, A. n.d)

Cloud Security Posture Managementin tarjoaa usein tärkeitä osia yritysten kyberturvan ylläpitoon. Useimman tarjoajan sivuilta löytyy hyvin samanlaiset tärkeimmät pointit, joita he tarjoavat palvelullaan:

- Näkyvyys ja vaatimustenmukaisuus
- Uhkien havaitseminen
- Tietoturva
- Monitorointi

Näiden avulla voidaankin rakentaa laajasti eri tarkoituksiin sopivia sovelluksia, joiden käyttötarkoitukset saattavat hieman poiketa toisistaan, mutta lopputulos on kuitenkin sama.

3.1 CSPM toiminta

CSPM-toiminta perustuu vahvasti konfiguraatiovirheiden löytämiseen. Muita olennaisia osia siinä ovat haavoittuvuuksien havaitseminen sekä monitorointi. CSPM-sovellusta voidaan käyttää myös esimerkiksi jo sovellustuotteen luontivaiheessa, koska useissa eri CSPM-vaihtoehdoissa on valmiiksi sisään rakennettuja DevSecOps integraatiota. Nämä integraatiot helpottavat kehittäjän työtä luoda tietoturvallista koodia, sekä välttää merkittäviä konfiguraatiovirheitä. Konfiguraatiovirheiden luomat haitat voivat olla todella vakavia erilaisille julkisen pilven tuotteille, joten niiden turvaaminen on hyvin olennainen osa tietoturvaa. Ihmisen luomat kontit ja järjestelmät vaativat aina useiden eri määritysten asettamista, ja sitä kautta niissä voi jäädä virheellisiä tai haavoittuvia konfiguraatioita tuotantoympäristöihin, jotka voivat tuottaa merkittäviä datan menetyksiä. Tällaisia virheitä voi jäädä esimerkiksi tietokantoihin, käyttäjätileihin, verkkoasetuksiin, virtuaalikoneisiin tai pilvitallennustiloihin. (Gillis, A. n.d.) Tähän liittyen on myös alkanut tapahtumaan muutosta ympäristöjen luonnin kanssa, koska on alettu käyttämään Infrastructure as Code (IaC) tyyppisiä tiedostoja, jotka luovat automaattisesti niihin määriteltyjen määreiden mukaisia käyttöjärjestelmiä tai kontteja (Puzas, D. 2021). Useat CSPM-sovellukset pitävät sisällään myös omanlaisen version SOC-toiminnasta (security operational center), jonka avulla voidaan ympäri vuorokauden tarvittaessa seurata sovelluksen käyttäjiä, toiminta-aikaa sekä tiedonsiirtoa. (Gillis, A. n.d)

Useat suuret pilvipalvelujen tarjoajat myyvät omia CSPM tuotteitansa samalla, kun he myyvät asiakkailleen muita palveluita. Niiden kanssa toimiessa täytyy kuitenkin muistaa, että he tarjoavat toimintaa ainoastaan omiin pilviympäristöihinsä. Näin ollen heidän tuotteensa ei pysty esimerkiksi skannaamaan IaC koodia, tai sen toimintaa. Ne perustuvat usein täysin omien pilviympäristöjensä tenanttien seurantaan, sekä siellä niiden konfiguraatioiden ja haavoittuvuuksien skannaamiseen. Kuitenkin jos asiakkaalla on käytössään esimerkiksi hybridi- tai yhteisöpilvi usean eri tarjoajan kanssa, joutuu se mahdollisesti ostamaan jokaisen tarjoajan oman sovelluksen ympäristöjensä valvontaan. Näin ollen muiden markkinoiden tarjolla olevien kolmansien osapuolien CSPM-sovellukset voivat tulla huomattavasti halvemmaksi, koska he tarjoavat usein yhden sovelluksen, johon voi kerätä tarvittavat datat kaikilta eri pilvipalveluilta, joita yritys mahdollisesti käyttää.

CSPM-ratkaisuissa on tarjolla lukuisia erilaisia standardi- ja sääntökokoelmia, joiden perusteella se luo omat hälytyksensä konfiguraatioiden kanssa. Näiden avulla se pystyy tehdä jatkuvaa tarkastelua eri ympäristöille, sekä seurata niille asetettuja säännöksiä. Yrityksillä voi olla omia lupauksiansa

omasta tietoturvastaan asiakkailleen, jolloin he pystyvät myös luomaan omia sääntöjänsä CSPM-ratkaisuunsa, jotka laukaisevat hälytyksen. Näin ollen niiden valvonta on huomattavasti helpompaa, sekä niistä saadut tulokset näkyvät suoraan esimerkiksi CSPM-ratkaisun konsolissa, ilman että sitä täytyy mennä tarkistamaa suoraan koodista, vaikkapa GitHubista. Jotkin CSPM-sovellukset voivat myös tarjota automaattisia korjauksia, jos ne huomaavat merkittäviä konfiguraatiovirheitä sääntöjensä pohjalta.

3.2 Julkisen pilven sovellustuotteet ja kyberturva

Julkisen pilven sovellustuotteella tarkoitetaan kaupallista tuotetta, jonka toiminta perustuu julkisen pilven kautta jaettuun verkkoon, johon voi päästä käsiksi melkein mistä vain internetin kautta. Tämä mahdollistaa siis esimerkiksi useiden eri paikoissa sijaitsevien toimipisteiden käyttää samaa sovellusta siten, että kaikki tieto tallentuu heidän yhteisille palveluillensa. Yleisesti nämä tuotteet ovat SaaS-mallisia, jonka ansiosta jokaiseen koneeseen ei tarvitse erikseen asentaa kyseistä ohjelmistoa, vaan ne toimivat verkkoselaimessa.

Julkisen pilven tietoturvassa on myös oleellisena osana IT-maailmassa tunnettu CIA-kolmio. Tämä muodostuu englanninkielisistä sanoista luottamuksellisuus (Confidentiality), eheys (Integrity) sekä saatavuus (availability). Julkisessa pilvessä on tärkeää pitää siitä kiinni, koska se perustaa toimintansa juuri siihen toimintaperiaatteeseen, joka on käytössä julkisen pilven tuotteissa.

Luottamuksellisuudella mahdollistetaan esimerkiksi oleellisen tiedon salassapito. Informaation saa nähdä ainoastaan ne henkilöt tai prosessit, joille se on tarkoitettu. Esimerkiksi palveluun kirjautuessa sinun tulee esittää pääsyoikeutesi palveluun, eli mahdollinen käyttäjätunnus sekä salasana. Nykyään erilaisten brute force kyberhyökkäysten takia on myös alettu ottamaan laajaan käyttöön kaksivaiheinen tunnistautuminen (two-factor authentication) -ominaisuutta, jossa palveluun sisälle kirjautuvan tulee pystyä todentamaan kirjautumisyrityksensä esimerkiksi puhelimeen lisätyllä sovelluksella. Tässä tapauksessa se voi olla vaikka jokin erillinen pääsykoodi puhelimen sovelluksessa, joka tulee syöttää koneelle. Kun palvelu lukee sen ja toteaa, että tämä tulee todellakin oikean käyttäjän kirjautumisyrityksestä, se voi päästää tämän sisälle palveluunsa. (What is the CIA Triad? 2021)

Eheydellä viitataan datan oikeellisuuteen. Dataan, jota palvelusta saadaan, tulee voida luottaa täysin melkein joka tilanteessa. Sen tulisi pysyä samanlaisena koko ajan, sekä se tulisi säilyttää siten, ettei sitä päästäisi manipuloimaan. Tärkeintä on siis pitää data aitona, oikeana ja luotettavana. Datan eheydestä voi pitää esimerkkinä verkko-ostoksia, jossa ostoskorissasi ja tililläsi näkyy sama ostos, ja voit ottaa yhteyttä kyseisen verkkokaupan edustajiin, jos huomaa eroja niiden välillä. (What is the CIA Triad? 2021)

Saatavuudella tarkoitetaan palvelun käyttämistä sille oikeutetuilta käyttäjiltä koska vain he haluavat. Palveluun oikein kirjautuneiden käyttäjien tulee olla mahdollista tarkistaa sen data heidän haluamassaan paikassa ja ajassa. Tämä tarkoittaakin sitä, että kyseisen palvelun verkot, laitteet ja muut tarvittavat infrastruktuurin osat toimivat ja pysyvät päällä jatkuvasti, tai sovitusti. Tässä voidaan käyttää myös esimerkkinä sitä, että on myös mahdollista ottaa palveluntarjoajaan yhteyttä koska vain, jos palvelun toiminnan ja päällä olemisessa aletaan huomata merkittäviä puutteita. (What is the CIA Triad? 2021)

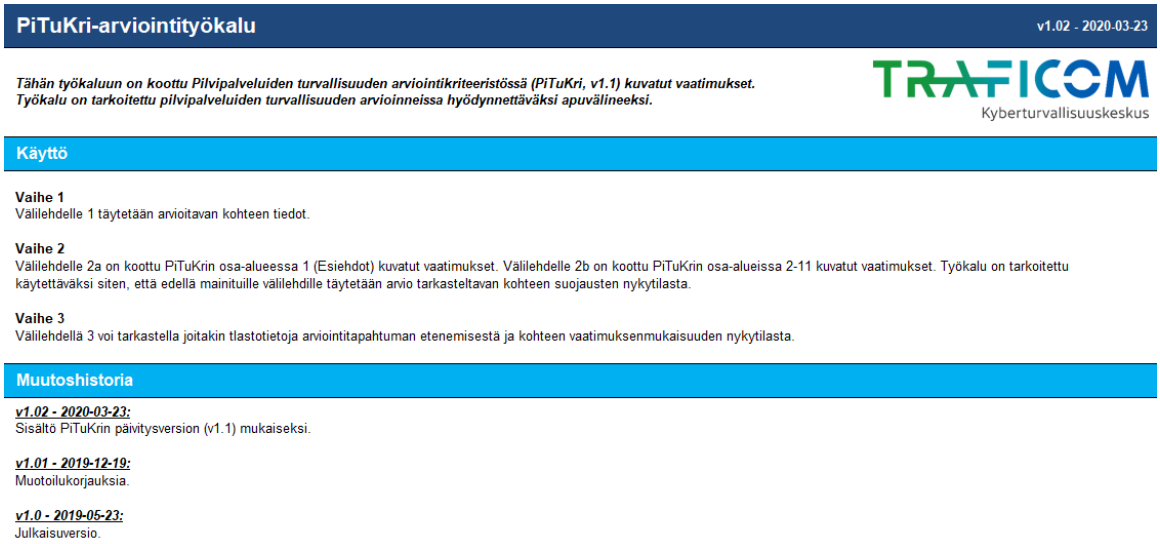
Wu, Zhang ja Wang (2019) pitävät artikkelissaan suurimpana huolena julkisen pilven turvallisuusuhkana tietovuotoja. Tietovuodoilla voidaan tarkoittaa ohjelmistovirheestä johtuvaa datan häviämistä bittiavaruuteen, tai sitten mahdollisesti datan varastamista internetin välityksellä. Tähän liittyykin toinen yleinen uhka julkisen pilven toiminnalle, joita on henkilöllisyyden väärentämishyökkäykset eli spoofing -hyökkäykset. Näissä haittaohjelma tai haitallinen käyttäjä esittää väärää identiteettiä järjestelmässä, jolloin se näyttää järjestelmälle, että tämä muokkaa, lukee tai poistaa dataa. Kuitenkin todellisuudessa hyökkäyksen tekijä voi saada sillä aikaa järjestelmän hallintaansa sen haavoittuvuuden kautta, jonka johdosta se voi myöhemmin hallita, tai jopa keskeyttää palvelun toiminnan. Yhtenä yleisimmistä kyberhyökkäyksistä julkisen pilven tuotteita voidaan myös pitää palvelunestohyökkäksiä (DDoS), joissa tarkoituksena on lamauttaa järjestelmä, kuluttamalla suuria määriä sen järjestelmäresursseista. Järjestelmäresursseihin kuuluvat mm. prosessorit, muisti, levytila sekä verkon kaistanleveys. (Wu ym. 2019.) Palvelunestohyökkäyksessä käytetään usein bottikoneita, jotka voivat olla tavallisia ihmisten tietokoneita (Nagpal, Sharma, Chauhan & Panesar, 2015). Ne on saatu haltuun jonkinlaisen viruksen tai haittaohjelman kautta, jolloin niitä voidaan käyttää ihmisten tietämättä yrittämään pääsyä jollekin tietylle sivustolle tai palveluun. Suuren käyttäjämäärän takia ne hidastuvat merkittävästi, tai mahdollisesti sammuttavat järjestelmän, jolloin sen oikeat käyttäjät eivät voi kirjautua palveluunsa. (Wu ym. 2019)

3.3 Vaatimuksia pilvipalveluiden tietoturvaan

Pilvipalveluiden turvallisuus Suomessa perustuu erilaisiin kriteeristöihin, joiden perusteella Traficomin kyberturvallisuuskeskus on kuvannut erilaisia vaatimuksia pilvipalveluille. PiTuKri pitää sisällään vielä erilaisia kriteeristöjä, joita on kerätty erilaisista yleisistä tietoturvaan perustuvista lähteistä. Kriteeristön osana on lainsäädäntö, jonka mukana on tullut kaksi lakia: laki julkisen hallinnon tiedonhallinnasta (L 906/2019) sekä valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (A 1101/2019). PiTuKri on saanut myös paljon kriteerejä Saksan liittovaltion tietoturvaviraston pilviturvallisuuskriteeristöstä (BSI) sekä Cloud Security Alliance (CSA) pilviturvallisuusmatriiseja Myös ISO27001 ja ISO27017 ovat olleet merkittäviä standardeja Kansallisen turvallisuusauditointikriteeristön (Katakri) ohella, joka edesauttaa ja tukee Valtiovarainministeriön julkisen hallinnon pilvipalveluiden linjausten käyttöönottoa. (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020)

Kyberturvallisuuskeskus tarjoaa sivuillansa arviointityökalua, joka perustuu heidän luomiinsa arviointikriteeristöihinsä (Ks. kuvio 3.). Kriteeristöt perustuvat laajasti tietoturvan kautta tehtyyn selvitykseen. Näiden avulla yritykset tai käyttäjät voivat tarkistaa oman ympäristönsä tilanteen, sekä saada siitä kuvauksen listamuodossa. Lista pitää sisällään 9 erilaista osa-aluetta vaatimuksista, joita tulisi noudattaa sekä pystyä todentamaan. Osa-alueita ovat:

- Turvallisuusjohtaminen
- Henkilöstöturvallisuus
- Fyysinen turvallisuus
- Tietoliikenneturvallisuus
- Identiteetin ja pääsyn hallinta
- Tietojärjestelmäturvallisuus
- Salaus
- Käyttöturvallisuus
- Siirrettävyys ja yhteensopivuus



PiTuKri-arviointityökalu v1.02 - 2020-03-23

Tähän työkaluun on koottu Pilvipalveluiden turvallisuuden arviointikriteeristössä (PiTuKri, v1.1) kuvatut vaatimukset. Työkalu on tarkoitettu pilvipalveluiden turvallisuuden arvioinneissa hyödynnettäväksi apuvälineeksi.

TRAFICOM Kyberturvallisuuskeskus

Käyttö

Vaihe 1
Välilehdelle 1 täytetään arvioitavan kohteen tiedot.

Vaihe 2
Välilehdelle 2a on koottu PiTuKrin osa-alueessa 1 (Esiehdot) kuvatut vaatimukset. Välilehdelle 2b on koottu PiTuKrin osa-alueissa 2-11 kuvatut vaatimukset. Työkalu on tarkoitettu käytettäväksi siten, että edellä mainituille välilehdille täytetään arvio tarkasteltavan kohteen suojausten nykytilasta.

Vaihe 3
Välilehdellä 3 voi tarkastella joitakin tlastotietoja arviointitapahtuman etenemisestä ja kohteen vaatimuksenmukaisuuden nykytilasta.

Muutoshistoria

v1.02 - 2020-03-23:
Sisältö PiTuKrin päivitysversion (v1.1) mukaiseksi.

v1.01 - 2019-12-19:
Muotoilukorjauksia.

v1.0 - 2019-05-23:
Julkaisuversio.

Kuvio 3. Kuvakaappaus arviointityökalusta (PiTuKri-arviointityökalu 2020)

Olisikin siis hyvä verrata muidenkin hallinnollisten järjestöjen kriteeristöjä suomalaisia pilvipalveluiden turvallisuusvaatimuksia läpi käydessä. Esimerkiksi BSI:n sekä CSA:n kriteeristöt ovat huomattavasti laajempia PiTuKriin verrattuna, mutta pääosin ne sisältävät samat aiheet. Kuitenkin kaikki perustuvat laajasti samaan tarkoitukseen, jossa halutaan luoda selkeät vaatimukset pilvipalveluille sekä niiden toiminnalle. Tämä mahdollistaa myös helpommin kansainvälisen kaupan, jonka ansiosta voidaan ostaa tai myydä esimerkiksi konesalista pilvitilaa muihin maihin. Kriteeristöjen yhdistäminen ja sitä kautta vertaaminen onkin olennainen osa sen kannalta. (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020)

CSA:n julkaisemassa artikkelissaan Top Threats to Cloud Computing (2019) kerrotaan yleisistä konfiguraatiovirheistä, joita erilaisissa pilviympäristöissä usein ilmenee. Yleisiä konfiguraatiovirheitä ovat suojaamattomat tallennustilat, liialliset käyttöoikeudet, tunnistautumistietojen oletustunnusten käyttö sekä järjestelmien omien turvatoimintojen pois kytkeminen. Kyseisten virheiden väärinkäyttö voi johtaa esimerkiksi tietomurtoihin, tietojen muokkaamiseen tai poistamiseen sekä palveluiden häirintään tai keskeyttämiseen. Erilaisten pilviympäristöjen konfiguraatiot voivat usein ollakin monimutkaisia, jonka johdosta ympäristöihin voi jäädä helposti inhimillisiä virheitä. Automaation käyttäminen pilviympäristöjen luonnissa voi vähentää riskien määrää, mutta usein automaatiokin tarvitsee ihmisen luoman pohjan siitä, mitä se on luomassa. (Top Threats to Cloud Computing 2019)

3.4 Palo Alto Prisma Cloud

Prisma Cloud on Palo Alton itse kehittämä CSPM-sovellus, joka soveltuu myös auditointityökaluksi. Palo Alto TechDocs (2022) dokumentaatiot tarjoavat laajat käyttö- ja konfigurointiohjeet käyttäjälleen. Niiden avulla käyttäjät pääsevät hyvin alkuun, kuinka sovellus toimii, sekä mitä se tarvitsee käyttöönsä. Palo Alto Prisma Cloud on luotu pilvi-infrastruktuurin tietoturvaratkaisuksi, joka sisältää myös oman SOC-työkalun (Security Operational Center), jonka avulla voidaan käsitellä riskejä ja suojata työkuormia hybridi- tai yhteisöpilviympäristöissä yhdellä Käyttöliittymällä. Prisma Cloudissa on myös lukuisia muita ominaisuuksia, jonka avulla se pystyy esimerkiksi tehdä käyttäjän seurantaa, liittyen siihen kuka palveluun kirjautuu ja millaisesta IP-osoitteesta. Prisma Cloud toimii suurimpien pilvipalveluidentarjoajien kanssa, jonka ansiosta sitä pystyy käyttämän laaja-alaisesti. Prisma tukee mm. Azurea, Amazon Web Serviceä, Google Cloud Platformia, Alibaba Cloudia sekä Oracle Cloud Infrastructurea. Näiden kanssa Prisma pääsee asiakkaan omaan pilviympäristöön suoraan integraatiolla. (Palo Alto TechDocs 2022)

Prisma Cloudissa on myös lukuisia muita integraatioita, joiden avulla sen käyttöä voidaan yksinkertaistaa ja tehostaa. Tämä mahdollistaa esimerkiksi suorat järjestelmän huomaamat hälytykset pikaviestinä Slackiin, Teamsiin tai vastaavaan palveluun. Prisman voi myös integroida suoraan konteja tai järjestelmiä luovaan sovellukseen, esimerkiksi Jenkinsiin, jossa se ilmoittaa jo mahdollisista haavoittuvuuksista ja ongelmista sen käynnistämisen aikana omassa konsolissaan. Näin ollen pilvityöntekijä voi saada välittömästi omaan tietoonsa mahdolliset konfiguraatiovirheet sekä haavoittuvuudet, joita Prisma havaitsee sen luonnin aikana. Mahdollisuudet luoda tietyille henkilöille kohdistettuja hälytyksiä, onnistuu Prismassa Cloudissa sen roolien luonnilla. Tämän ansiosta pystyy määrittämään tarkastikin henkilöitä, joille mitkäkin hälytykset menevät esimerkiksi Slackiin tai sähköpostiin. Näin ollen eri tuotteiden kanssa toimivat henkilöt eivät saa hälytyksiä tuotteesta, jonka kanssa heillä ei ole mitään tekemistä. Tämä myös helpottaa tilannetta, jossa esimerkiksi sovelluksen koodaaja ei saa hälytyksiä siitä, että pilviympäristö olisi kaatunut, jos hänet on asetettu näiden hälytysilmoitusten ulkopuolelle. Näin ollen turhista hälytyksistä johtuvat häiriöt eivät vaikuta niin paljoa kunkin työntekijän omiin tehtäviin. (Aropaltio 2022)

Prisma Cloud tarjoaa myös turvallisen koodin (code security) skannauksia osana sovelluksen toimintaa. Palo Alto on saanut tähän mukaansa Bridgecrew nimisen yhtiön ja sitä kautta saaneet käyttöönsä heidän koodin katselmointityökalun. Se tekee IaC-skannauksia käytetyn koodiympäristön kautta. Se tekee skannauksensa kontin tai käyttöjärjestelmän luonnin aikana, tarkastamalla sieltä käyttöjärjestelmän, sekä muiden määriteltyjen osien haavoittuvuudet ja lisenssit. Se voidaan liittää suoraan Virtual Studio Codeen heidän omalla lisäosallaan, joka automaattisesti ehdottaa muutoksia koodiin sen kirjoittamisen aikana. Automaattiset ehdotukset perustuvat Prismassa määriteltyihin sääntöihin ja standardeihin. Code Securityyn voi myös luoda omia säännöksiään, jotka hälyttävät koodin kirjoittamisen aikana, tai sitten järjestelmän luonnin aikana. Prisman Cloudin kautta sen voi myös integroida suoraan asiakkaan käyttämään koodinhallintajärjestelmään, johon se pystyy tehdä myös omia muokkausehdotuksiaan koodin katselmoinnin yhteydessä. Prisma Cloud tukee GitHubia, Bitbucketia, GitLab Self-managed, GitLab, GitHub Server, Bitbucket Server sekä Azure Repos hallintajärjestelmiä, joihin sen voi asentaa integraation avulla. (Aropaltio 2022)

3.5 Muita palveluiden tarjoajia

Muita CSPM-ratkaisuja on useita erilaisia, sekä eri hintaisia. Jokaisella pilvipalvelun tarjoajalla on omat CSPM-järjestelmänsä luotuna suoraan omiin ympäristöihinsä, jotka saa helposti käyttöönsä. Kuitenkin haittana näissä on jo aikaisemmin mainitut käyttömahdollisuudet oman pilvipalvelun ulkopuolella. Kuitenkin kolmansien osapuolien tarjoamia, laajamittaisia CSPM-ratkaisuja on useita erilaisia. Niiden erot saattavat olla osassa hiuksen hienoja, mutta toisaalta niissä saattaa olla toiminnallisuuksiltaan suurehkojakin eroja. Myöskin niiden lisäominaisuuksien käyttötarkoituksesta riippuen niiden toiminta ja käytettävyys voivat vaihdella huomattavasti.

Falcon Horizon on Crowdstrike nimisen yrityksen CSPM-ratkaisu. Crowdstrike on amerikkalainen yritys, jonka päämarkkina-aluetta on ollut pilvipalveluiden tietoturva, uhkien tiedustelutoiminta sekä käyttäjälähtöinen tietoturva (Crowdstrike n.d.). Heidän Falcon Horizon on suunniteltu yhteisöpilvien käyttöön, ja se tuo näkyvyyden sekä turvallisuusvalvonnan samaan konsoliin. Se tarjoaa konfiguraatiovirheiden jatkuvaa seurantaa, sekä korjausehdotuksia niiden ilmetessä. Säännöstöjen seurantaan heillä on käytössään jatkuva monitorointi sen Falcon Horizon kautta luotuihin ympäristöihin, minkä avulla se seuraa merkittävimpien standardien ja säännöstöjen kirjastoja, kuten esimerkiksi PCI:tä tai NIST:iä. Falcon Horizonissa on hyvin samantyyppinen roolien jako kuin Prisma

Cloudissa. Se mahdollistaa hälytysten osoittamisen juuri oikeille henkilöille, eikä kaikki tule saamaan samoja hälytyksiä. Näin ollen esimerkiksi muiden sovellusten kanssa työskentelevät henkilöt eivät saa häiritseviä hälytysilmoituksia toisista sovelluksista, jotka eivät vaikuta heidän työnkuvaansa ollenkaan. (Crowdstrike Falcon Horizon CSPM n.d.)

CloudGuard on CheckPointin tarjoama pilvipalveluiden tietoturvaan perustuva ohjelma, joka pitää sisällään heidän oman CSPM-sovelluksensa. Se toimii automaattisesti tietoturvan kanssa ja se hallitsee ja räätälöi asiakkaalleen heidän vaatimustensa mukaisen ympäristön seurannan. Heidän päätoimisia ympäristöjään on AWS, Azure, Google Cloud, Alibaba Cloud ja Kubernetes. CloudGuard on hyvin pitkälti heidän sivujensa mukaisesti samankaltainen sovellus kuin Falcon Horizon, joka mahdollistaa omien säännöstöjen luonnin, sekä useiden erilaisten roolien luomisen. CloudGuardissa on osanaan täysin muokattava konsolinäkymä, johon saa asetettua haluamiansa palikoita. Kuitenkin merkittävänä erona muihin vastaaviin tuotteisiin on se, ettei CheckPoint myy CSPM-ratkaisuaan omana osana, vaan silloin täytyy ostaa koko CloudGuard sovellus, joka takaa huomattavasti laajemmin kaiken pilvipalvelun turvaamiseen. (CheckPoint CloudGuard n.d.)

4 Tutkimusvaihe

Työn tutkimusvaiheessa perehdyttiin Palo Alto Prisma Cloudin toiminnallisuuksiin, ja siihen kuinka sen CSPM-toiminnot vaikuttaisivat Pinjan toimintaan sekä sen tietoturvaan. Tutkimuksessa Prisma Cloud integroitiin kahteen Pinjan julkisen pilven testiympäristöön.

4.1 Tutkimuskohteet

Prisma Cloud suoritti skannauksensa Pinjan testialustojen pilviympäristöihin Azuren pilvipalvelussa. Tarkoituksena oli selvittää jo valmiiksi pilvessä pyörivien sovellusten konfiguraatioiden tietoturva. Tutkimuksen aikana myös suoritettiin erillisiä ympäristöjen luonteja kehityspuolella, jossa saatiin enemmän tietoa juuri ympäristöjen pystyttämisen ajalta. Näin ollen tuloksia saatiin jo valmiista ympäristöistä, sekä uusista luoduista ympäristöistä. Kuitenkin kaikki skannaukset tehtiin kehitysympäristöihin, eikä niitä suoritettu yhtään tuotantoympäristöihin. Tutkimus suoritettiin kahden kuukauden mittaisella trial Prisma Cloud Enterprise -versiolla.

Testiympäristö 1 on SaaS-pohjainen järjestelmä, jonka toimintatarkoitus on käyttäjälleen ympäristön, jossa voi suorittaa maksullisia tarkastustehtäviä. Se säilöö ja siirtää tietonsa myös suoraan julkisiin tietokantoihin. Testiympäristö 1 pitää sisällään varauspalvelun, maksupalvelun, siirtopalvelun sekä tietokannan. Azuren pilviympäristössä palvelut ovat kahdennettu, koska kyseisessä ympäristössä pyörii kaksi eri kielistä versiota.

Testiympäristö 2 on SaaS-järjestelmä, jonka pääasiallinen tarkoitus on asiakirjojen säilytys- ja välitysympäristönä. Se toimintaperiaatteena on siirtää asiakirjoja tietokannan sekä käyttäjien välillä nopeasti. Testiympäristö pitää sisällään tietokannan sekä asiakirjojen siirtopalvelun.

4.2 Prisma Cloud integrointi

CSPM-toimintaa varten Prisma Cloud integroitiin suoraan molempien tuotteiden käyttämiin Pinjan Azure pilviympäristöihin. Prisma Cloudin integroinnissa, käyttäjän tulee pystyä antamaan sille oikeudet datan lukemiseen sekä hallintaan halutussa pilviympäristössä. On myös suotavaa luoda Prismalle oma mukautettu rooli, jolla se pääsee käsiksi flow lokeihin. Tässä tapauksessa se toteutetaan Pinjan hallinnoimassa Azuren pilviympäristössä. Prisma Cloudin integrointi voidaan toteuttaa helposti muutamalla eri vaiheella Cloudin selkeiden ohjeiden mukaisesti. Käyttäjällä on hyvä olla admin-tason käyttäjäoikeudet pilviympäristöihin, jotta integraatioon tarvittavat määreet saadaan helposti selville, sekä niitä saadaan lisättyä Azuren pilviympäristöihin.

1. Valitaan pilvipalvelun tuottaja, sekä valitaan käyttäjälle nimi, käyttötarkoitus (tenant vai subscription) ja tila (Monitor tai Monitor & Protect)
2. Määritetään Azuren ympäristön ID johon integraatio suoritetaan.
3. Tarkempien määritysten ja ID:iden hakemista Azuresta, joko Terraform muodossa AzureBashin kautta tai sitten manuaalisesti Azuren pilviympäristöstä
4. Valitaan käyttäjäryhmä, joka vastaanottaa kyseisen ympäristön hälytykset.

Integrointia suoritetaan mahdollisesti useassa eri paikassa, ja tässä tapauksessa se tehtiin Prisma Cloudin omassa käyttöliittymässä, sekä Azuren pilviympäristöissä. Laajempaa integrointia tehdessä, Prisma Cloud voidaan lisätä esimerkiksi suoraan CI/CD -putkeen, jossa se voi suorittaa skannauksiaan. Tällöin Prisma Cloud tulee integroida suoraan sovellukseen, jonka putkessa järjestelmiä luodaan. Tutkimuksen ohessa tehtiin integroinnin Jenkinsiin, joka on Pinjalla käytössä joidenkin

testiympäristöjen sovelluksen luonnissa. Tähänkin tehtävään löytyi selkeät ohjeet Prisma Cloudin omista tukidokumenteista, jonka avulla integraatio saatiin tehtyä riittävien oikeuksien kanssa.

4.3 Miten tulokset saatiin?

Prisma Cloudin CSPM-toiminto alkoi välittömästi käydä läpi sen saamia pilviympäristöjä, sekä niiden tilaa. Tässä tutkimuksessa aloimme saada tuloksia seuraavana päivä Prisman integroinnin jälkeen. Asiantuntijoiden mukaan Prisma Cloud alkaa antamaan tuloksia noin neljän tunnin päästä, kun se on saatu integroitua oikein järjestelmiin. Kaikki kuitenkin riippuu pilviympäristöjen koosta ja niiden käyttömäärästä. Tässä tutkimuksessa oli käytössä kaksi erillistä pilviympäristöä, sekä niiden sisällä kehitysversio molemmista testiympäristöistä.

Prisma Cloud alkaa skannauksien aikana käymään omia prosessejaan läpi, ja alkaa sitä kautta tutkimaan puutteellisia konfiguraatioita erilaisten vaatimusstandardien ja lisenssien kautta. Se pitää sisällään yleisimmät vaatimusstandardit aina GDPR:stä ISO standardeihin. Tällä hetkellä Prisma Cloud tarkastaa automaattisesti 52 eri vaatimusstandardilta sen CSPM-toiminnan. Kaikki käytössä olevat standardit ovat listattuna liitteessä 1. Prisma Cloudiin voi myös itse muokata omia vaatimusstandardejaan joidenkin valmiiden pohjalta, tai sitten täysin oman asiakaskuntansa vaatimusten perusteella.

5 Tulokset

Konfiguraatioihin perustuvat löydökset pysyivät molemmissa testiympäristöissä hyvin samankaltaisina, jos peilaa niitä löydösten prosentuaaliseen määrään taulukossa 1. Lukumäärä vaikuttaa suurelta, mutta kuitenkin kriittisten haavoittuvuuksien puuttuminen antaa tuotteiden tilasta hyvää kuvaa. Myös High-tasoisia havaintoja oli suhteessa huomattavasti vähemmän kuin Medium-tasoisia, ja hieman vähemmän kuin Low-tasoisia. Nämä kaikki tulokset saatiin kerättyä kahden kuukauden mittaiselta trial ajanjaksolla. Kuitenkin kaikkien konfiguraatioiden johdosta, itse skannauksiin käytetty aika on ollut lyhyempi. Trial ajanjakson aikana havaintoja oli kertynyt useita erilaista vaatimusstandardeihin liittyvää poikkeusta, jotka on Prismaan asetettu oletuksena. Niistä noin 18% oli SQL-ympäristöihin perustuvia löydöksiä, joita käydään läpi hieman tarkemmin kappaleessa 5.2.

Taulukko 1. Prisma Cloud havaintojen prosentuaalinen määrä

	High (%)	Medium (%)	Low (%)
Testiympäristö 1	5	87	8
Testiympäristö 2	10	74	16

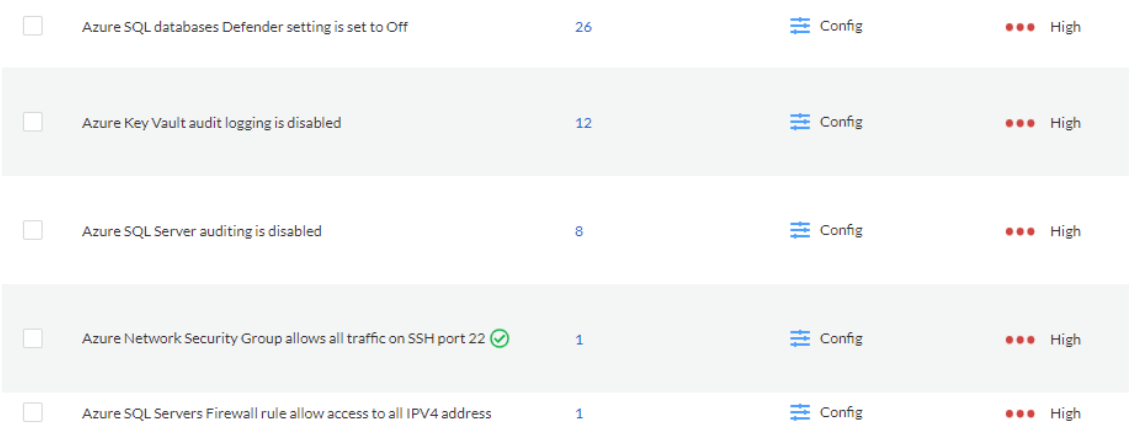
Testiympäristöjen erilaisten havaintojen määrät olivat lukumääräisesti hyvin samankaltaiset. Testiympäristö 1:ssä on prosentuaalisesti huomattavasti enemmän löydöksiä kuin testiympäristö 2:ssa (Ks. taulukko 1), johon vaikuttaa merkittävästi se, että testiympäristö 1 on ollut kehitysympäristössä kaksi samanlaisista versiota pyörimässä. Niissä ainoana erona on ainoastaan niiden käyttämä oletuskieli. Näin ollen testiympäristö 1 löydökset voidaan jakaa kahdella, jos haluttaisiin saada vertauskelpoinen tulos testiympäristö 2 verrattuna.

Prisma Cloudin luomien oletus vaatimusstandardien mukaiset löydökset olivat kuitenkin laadultaan hyviä, vaikka siellä oli reilusti medium-tasoisia havaintoja. Tulosten läpikäynnissä on pitänyt kuitenkin pohtia paljon niiden tarkoitusta, ja sitä, ovatko ne niin sanottuja false positive -havaintoja vai oikeita löydöksiä. False positive -löydöksellä tarkoitetaan havaintoa, jonka toiminta tai koodi muistuttaa jotakin tunnettua haitallista toimintatapaa, kuten virusta, hyökkäystä tai tiedostoa (False Positive n.d.). Näissä tapauksissa kyseessä on konfiguraation puute, mutta se saattaa olla tietoisesti tehty ratkaisu. Kuitenkaan mitään havaintoa ei saa jättää huomioimatta, vaan sen tarkoitus pitää aina selvitettävä. Tiimien kanssa käytyjen palavereiden aikana onkin selvinnyt, että suurin osa löydöksistä on heidän tiedostamiaan, ja niille on jokin oma selityksensä sovellusten käytettävyyden kannalta.

Myös ympäristöllä on merkittävä vaikutus sen konfiguraatioihin ja sitä kautta sen luomiin löydöksiin. Tutkimuksen aikana käytössä on ollut kehitysympäristö, jonka johdosta osa havainnoista johtuu pääsyjen helpottamisesta erilaisiin resursseihin ja paikkoihin. Kuitenkin tuotantoympäristöjen konfiguraatiot ovat tiukemmat, koska siellä liikkuu asiakkaiden merkittävää dataa. Näin ollen sekin tuo osakseen tutkimukseen lisää pohdintaa false positive -havainnoista.

5.1 High-tason havainnot

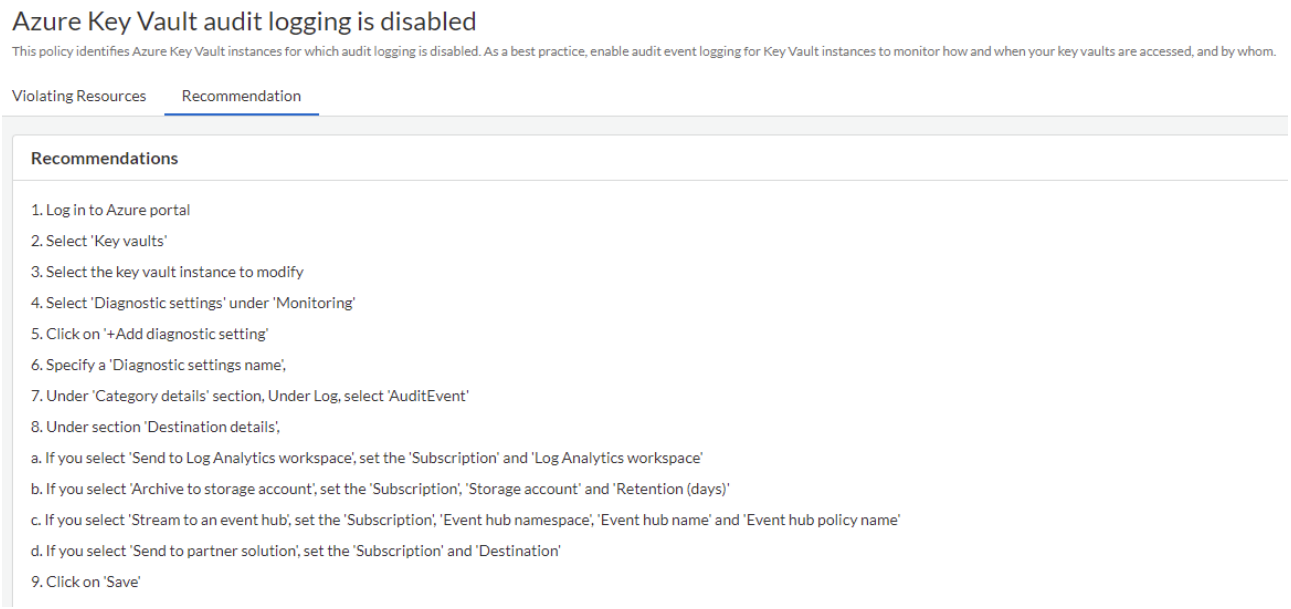
High-tason havainnot ilmenivät Prisma Cloudissa pääosin Azuren omien lokien ja heidän oman CSPM-ratkaisunsa kiinniololla. High-tasoisia hälytystyyppejä ollut vain 5 erilaista (Ks. Kuvio 4.), mutta skannauksien aikana havaintoja on ilmennyt useamman kerran. Eniten löydöksiä on antanut Azuren oman CSPM-ratkaisu Defenderin käyttämättömyys sen SQL-tietokannoissa. Seuraavaksi suurin erillisten löydösten luoja on ollut Azuren salausavainten säilytystilan auditointilokien pois sulkeminen. Myös SQL-palvelimen auditoinnin poissulkeminen on luonut muutamat löydökset. Yksittäiset havainnot SQL-palvelimeen luotujen ryhmien sisältävän säännön, jonka mukaan jokainen IPV4 osoite voi yhdistyä palvelimeen, sekä Azuren verkkoryhmien kaiken SSH-portti 22 kulkevasta liikenteestä sallivan konfiguraation asettaminen. Prisma Cloudin etuna voidaan pitää kehittäjän tai pilviarkkitehdin kannalta työtä edistävänä ominaisuutena sitä, että se tarjoaa jokaiseen havaintoon korjausehdotuksensa, jonka avulla se voitaisiin saada pois näkyvistä. On kuitenkin myös mahdollista luoda omia sääntöjä, joiden avulla false positive -havaintoja saataisiin pois Prisman käyttöliittymästä, mutta ne pitäisi luoda erikseen manuaalisesti.



Kuvio 4. High-tason havainnot Prisma Cloudissa

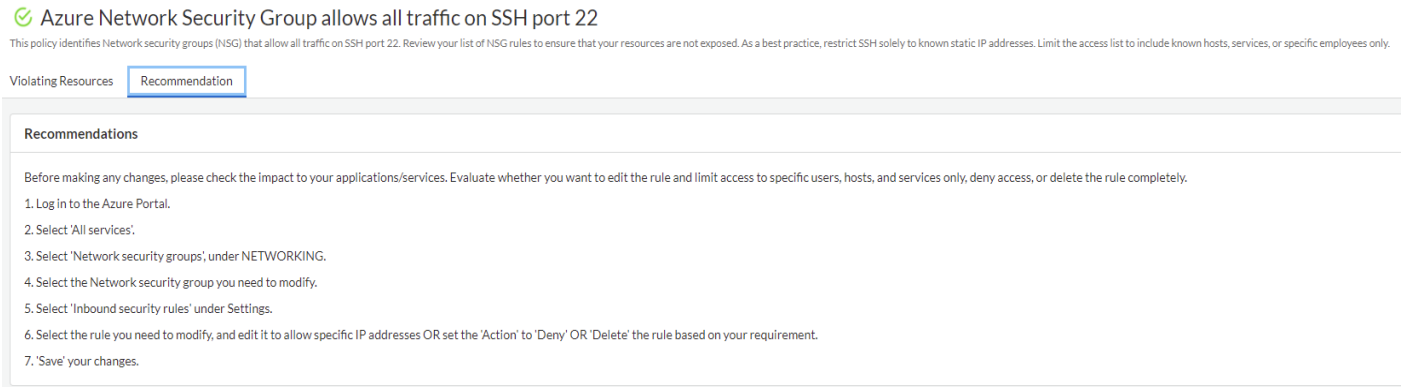
Azuren avainsäilön (key vault) auditoinnin lokituksen pitäminen pois päältä on Prisma Cloudille automaattinen löydös. Tämä suositellaan Prisman mukaan pitämään päällä, jotta voitaisiin monitoroida ja seurata, kenellä on pääsy kyseiseen säilöön, ja ketkä siellä oikeasti käyvät. Tässäkin on viittauksia false positive -havaintoon, koska kyseinen monitorointiloki pitäisi sisällään vääriä kirjautumisia mahdollisen kyberhyökkäyksen aikana. Jos kyseiseen palveluun päästäisiin ulkopuolelta käsiksi, ei ympäristön käyttäjät tietäisi, onko heidän avainsäilössään käyty. Kyseinen löydös

perustuu useisiin Prisma Cloudin oletus vaatimusstandardiin, jonka johdosta se ilmoittaa hälytyksensä. Prisma ehdottaa jokaisesta hälytyksestään oman korjausehdotuksensa, jonka avulla kyseinen löydös lähtisi pois järjestelmästä (Ks. kuvio 5.).



Kuvio 5. Avainsäilön hälytyksen korjausehdotus

Toinen havainto Prisma Cloudissa, joka ei liity SQL-palveluihin oli tutkimuksessa Azuren verkkoryhmien kaiken liikenteen SSH-portti 22 salliminen. Tämä johtuu Prisman oletuskäytänteistä, liittyen sen verkkoryhmien konfigurointeihin. Prisma ehdottaakin korjauksena tälle, että sinne asetetaan staattiset IP-osoitteet, joista kyseistä porttia voitaisiin käyttää (Ks. kuvio 6.). Sen ehdotuksen mukaan olisi suotavaa, että kyseiseen IP-osoitteiden listaan olisi määritetty vain tietyt osoitteet, kuten palvelut ja tietyt työntekijät. Kuitenkin julkisten sovellustuotteiden kanssa toimiessa, jokaista IP-osoitetta ei voi kuitenkaan tietää. Tässäkin tapauksessa IP-osoitteita tulisi olla todella paljon, joka tulisi varmasti tuottamaan ongelmia laitteiden kanssa, jolla sovellusta käytetään. Tämä havainto onkin hyvin vahvasti siinä rajalla, onko tämä false positive -löydös, vai sitten oikea hälytys. Kuvasta 10 voi taas huomata tarkemmin, että tämäkin havainto on usean erilaisen vaatimusstandardin listoilla, jonka johdosta se on aktivoitunut Prisma Cloudissa.



Kuvio 6. Verkkoryhmän SSH-portin korjausehdotukset

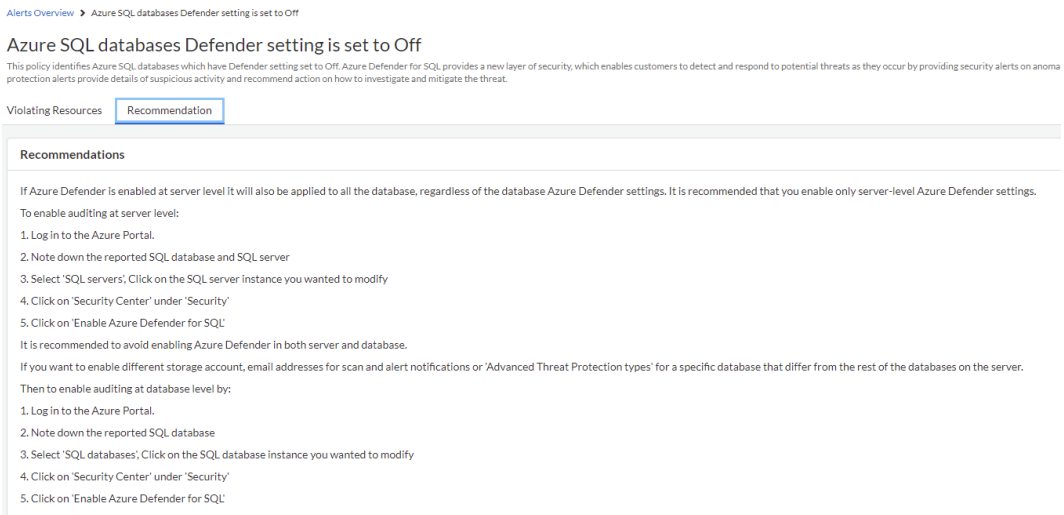
5.2 Azure SQL havainnot

Azuren SQL-palveluista löytyi useampia havaintoja, joiden vakavuus vaihteli (Ks. kuvio 7.). Tässä kappaleessa tarkastellaan tarkemmin näitä SQL-löydöksiä, sekä käydään läpi niiden tarkoitusta. 13:sta erilaisesta havainnosta kolme oli High-tasoista, kuusi Medium-tasoista ja neljä Low-tasoista. Näiden havaintojen lukumäärät vaihtelivat järjestelmän sisällä, ja yhteensä niitä oli tullut Prisma Cloudiin näkyviin muutamia. Eniten löydöksiä oli tuottanut Azuren SQL-tietokannan oman Defender-ohjelman poiskytkentä. Vähiten löydöksiä olivat tuottaneet Azure SQL-palvelimen palomuurin asetusten sallimat kaikki IPV4 osoitteet, sekä SQL-palvelin, jolle ei ole luotu Azuren oman Active Directoryn (AD) admin käyttäjää. Nämä kaksi havaintoa saivat vain yhdet hälytykset koko tutkimuksen aikana.

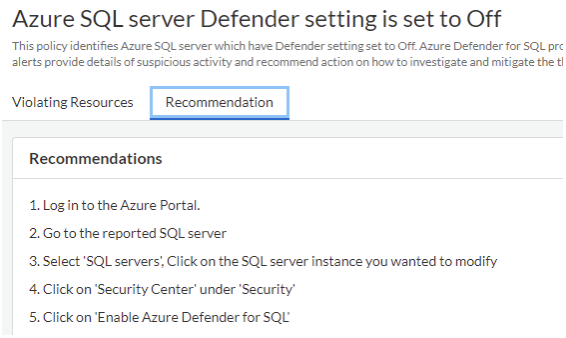
Policy Name	Alerts	Policy Type	Severity
Azure SQL databases Defender setting is set to Off	26	Config	High
Azure SQL Server auditing is disabled	8	Config	High
Azure SQL Servers Firewall rule allow access to all IPV4 address	1	Config	High
Azure SQL database auditing is disabled	19	Config	Medium
Azure SQL server Defender setting is set to Off	14	Config	Medium
Azure SQL server TDE protector is not encrypted with BYOK (Use yo...	14	Config	Medium
SQL Server Firewall rules allow access to any Azure internal resources	11	Config	Medium
Azure Microsoft Defender for Cloud is set to Off for SQL servers on ...	2	Config	Medium
Azure Microsoft Defender for Cloud is set to Off for Azure SQL Data...	2	Config	Medium
Azure SQL Server ADS Vulnerability Assessment is disabled	14	Config	Low
Azure Activity log alert for Create or update SQL server firewall rule ...	2	Config	Low
Azure Activity log alert for Delete SQL server firewall rule does not e...	2	Config	Low
SQL servers which do not have Azure Active Directory admin configu...	1	Config	Low

Kuvio 7. Azuren SQL-havainnot

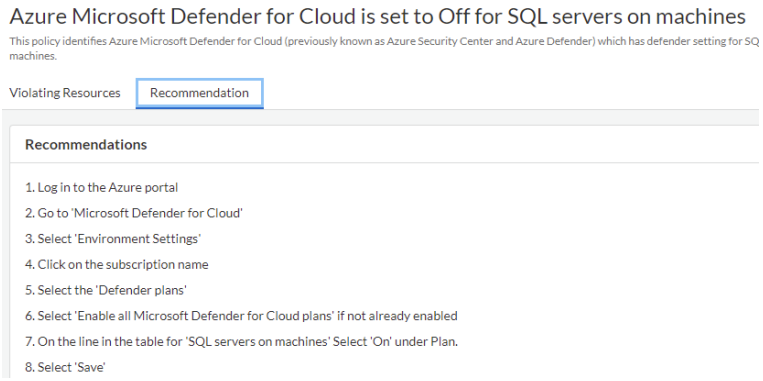
Azuren Defenderin tehtävä tietokannassa on seurata sen käyttäjiä ja reagoida uhkiin antamalla tietoturvahälytyksiä poikkeavista toiminnoista. Näin ollen sen yleinen pois kytkeminen Azuressa nostaa useita erilaisia löydöksiä. Sen tehtävä on kuitenkin suojata toimintaa, sekä luoda siitä omia hälytyksiään, jos se huomaa jotain poikkeavaa. Näidenkin havaintojen laatu on hyvin ailahteleva, koska kyseessä on kuitenkin maksullinen palvelu Azuren sisällä.



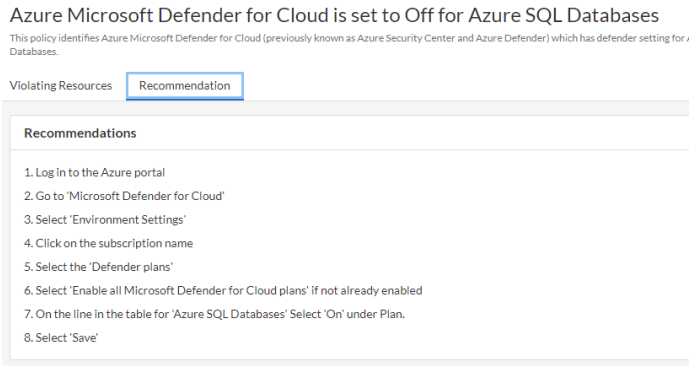
Kuvio 8. Azuren SQL-tietokannan Defenderin puute hälytys ja sen korjausehdotus



Kuvio 9. Azure SQL-palvelimen Defenderin puute hälytys ja sen korjausehdotus



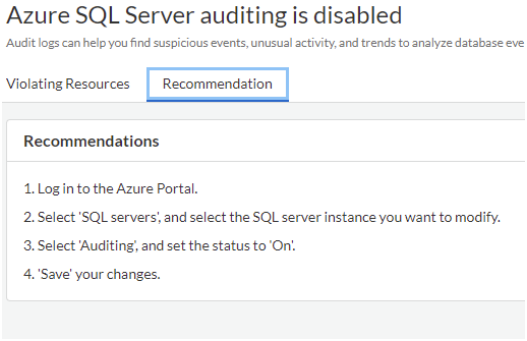
Kuvio 10. Azuren Microsoft Defenderin puute -hälytys SQL-palvelimen koneilla, sekä sen korjausehdotus



Kuvio 11. Azuren Microsoft Defenderin puute -hälytys SQL-tietokannassa, sekä sen korjausehtotus

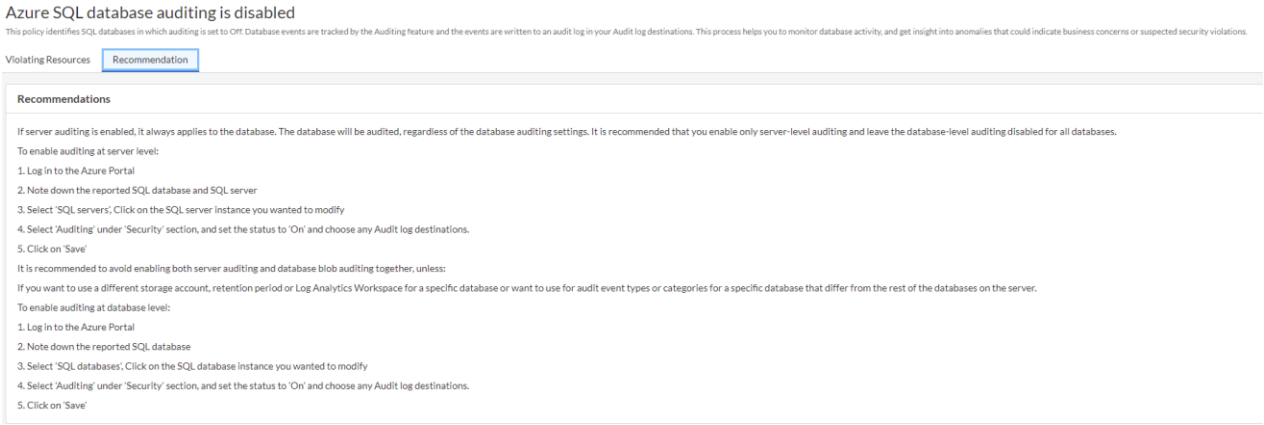
Prisma Cloud onkin nostanut High-tason hälytyksen Defenderin uupumisesta sen tietokannoissa (Ks. kuvio 8.). Kuitenkin se on luonut erilaisia hälytyksiä Defenderin käyttämättömyydestä, kuten Medium-tasoinen hälytys Defenderin puuttumisesta Azuren SQL-palvelimesta (Ks. kuvio 9.), sekä

kaksi Medium-tasoista hälytystä Azuren Defenderin puuttumisesta sen pilviympäristössä SQL-palvelimen koneilla (Ks. kuvio 10.) ja SQL-tietokannassa (Ks. kuvio 11.). Hälytysten määrittely onkin hankalaa sen puolesta, onko se false positive vai ei. Kuitenkin useiden standardien mukaisesti se olisi silti hyvä olla käytössä, koska tietoturvaan voi harvoin panostaa liikaa.



Kuvio 12. Azure SQL-palvelimen auditoinnin puute -hälytys ja sen korjausehdotus

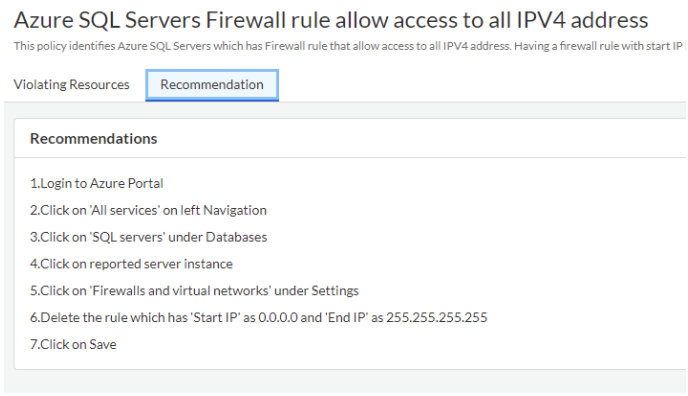
Myös Azuren oman auditoinnin pois kytkeminen on nostanut kaksi erillistä hälytystä. High-tasoinen auditoinnin puuttumisesta sen SQL-palvelimessa (Ks. kuvio 12.) ja Medium-tasoinen hälytys SQL-tietokannan auditoinnin puutteesta (Ks. kuvio 13.).



Kuvio 13. Azure SQL-tietokannan auditoinnin puute -hälytys ja sen korjausehdotus

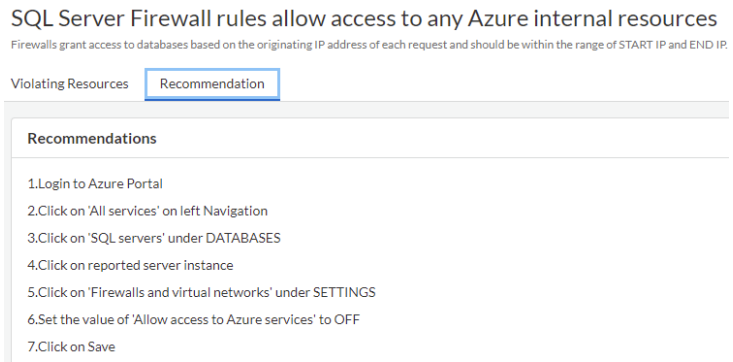
Kuvioiden 12 ja 13 hälytyksissä on taustalla ominaisuus, joka kerää dataa tapahtumista SQL-palvelimessa ja -tietokannassa. Tapahtumilla tarkoitetaan kyselyitä ja talletettuja toimenpiteitä, joita suoritetaan tietokannassa, sekä onnistuneita ja epäonnistuneita kirjautumisia. Prisma

Cloudilla on myös tähän yksinkertaiset ohjeet järjestelmässään, kuinka auditoinnin saa kytkettyä päälle SQL-palvelimella ja -tietokannassa.



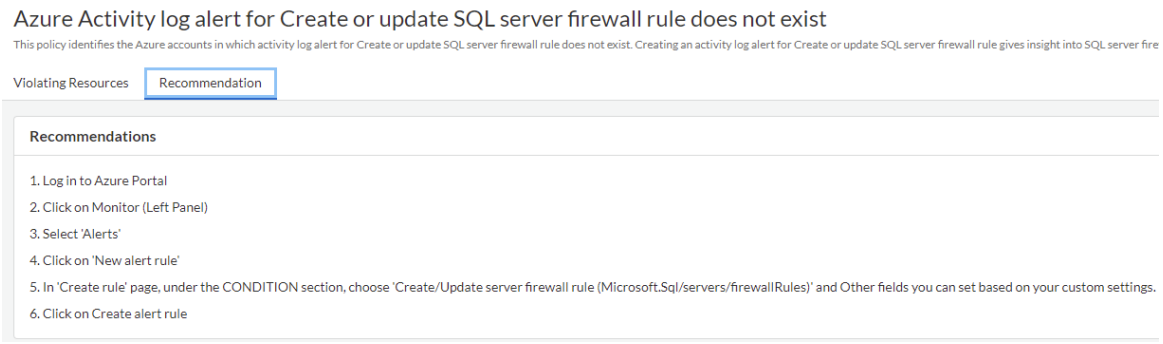
Kuvio 14. Azuren SQL-palvelimen palomuurin sallima liikenne kaikilla IPV4-osoitteilla -hälytys ja sen korjausehdotus

Viimeinen High-tasoinen hälytys on tullut Azuren SQL-palvelimen palomuurin asetuksista, jossa on sääntönä sallia kaikki IPV4 osoitteet (Ks. kuvio 14.). Näin ollen tietokantaan voi päästä sisälle millä IP-osoitteella tahansa internetistä. Sääntö voi olla usein manuaalisesti sinne asetettu, ja sen tarkoituksena on helpottaa tietokantaan pääsyä mistä tahansa paikasta, ilman että käytössä olisi jokin tietty laite, ja sen mukana staattinen IP-osoite. Tällaisilla säännöillä on siis riskit mahdollistaa väärien käyttäjien pääsy tietokantapalvelimelle mahdollisesti erilaisia SQL-haavoittuvuuksia käyttäen. Kuitenkaan kyseistä hälytystä ei löydy monesta oletusvaatimusstandardista automaattisesti, mutta osa standardeista vaatii paremman suojan IPV4 osoitteiden hallinnassa.



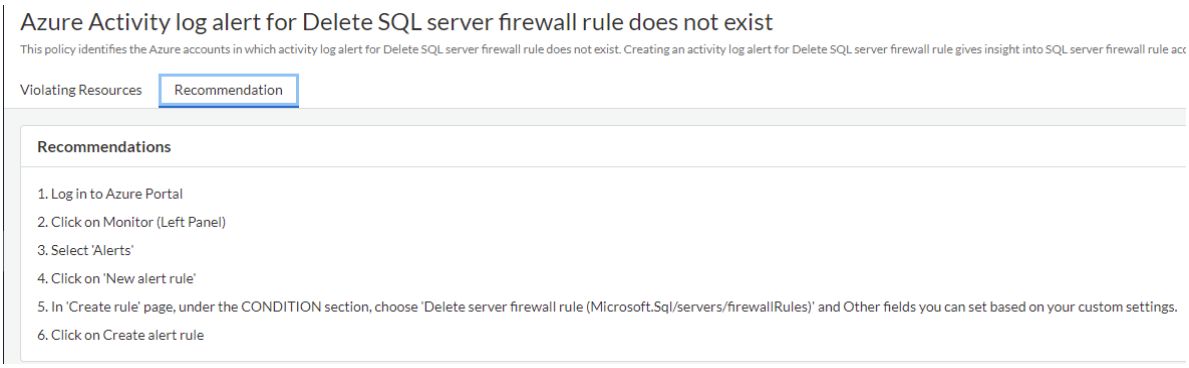
Kuvio 15. SQL-palvelimen palomuurin sallima pääsy kaikkiin Azuren sisäisiin resursseihin -hälytys ja sen korjausehdotus

Toinen palomuuriin liittyvä hälytys on SQL-palvelimen palomuurin sallima pääsy kaikkiin Azuren sisäisiin resursseihin (Ks. kuvio 15.). Se on kuitenkin saanut vain Medium-tasoisen hälytyksen, mutta sen seuraamukset voivat kuitenkin olla pahoja, jos sitä osataan käyttää väärin. Tämä perustuu myös hyvin paljo edeltävään HIgh-tason hälytykseen, koska tässäkin hälytyksessä on sääntönä päästää käytännössä kaikista IP-osoitteista käyttäjä sisäisiin resursseihin. Näin ollen resursseihin voi päästä väärät henkilöt käsiksi, jos he onnistuvat pääsemään SQL-palvelimelle. Tämä vaikuttaa kuitenkin olevan luotu sääntö, jolla tarkoitus on päästä tarkastamaan kehitysympäristön resursseja helpommin, ilman että ne ovat tietyn IP-osoitteen ja laitteen takana piilossa.



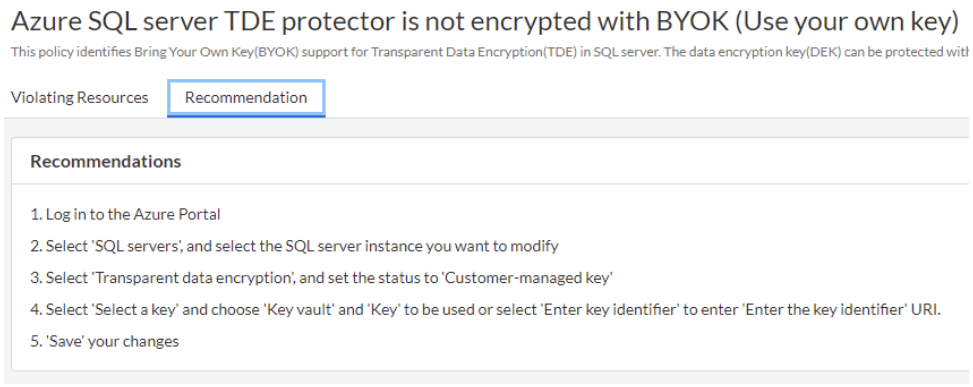
Kuvio 16. Aktiivilokin puute -hälytys palomuurin asetusten luonnille ja muutokselle

Azuren palomuuriin liittyy vielä kaksi erillistä Low-tason hälytystä. Näissä on kuitenkin kyse aktiivisesta lokista, johon tulisi ilmoituksia, jos SQL-palvelimen palomuuriin tehtäisiin tai muokattaisiin sääntöjä (Ks. kuvio 16.).



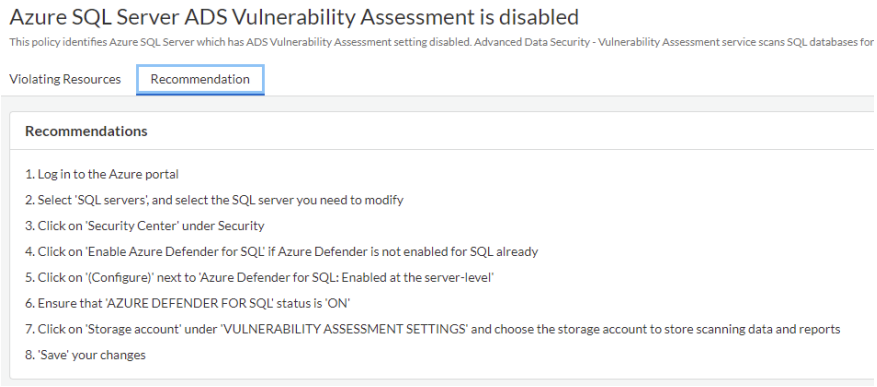
Kuvio 17. Aktiivilokin puute -hälytys palomuurin asetusten poistamisesta

Toinen hälytys Azuren palomuurissa olisi sille, jos sääntöjä poistettaisiin (Ks. kuvio 17.). Näiden hälytysten tarkoituksena on ehdottaa pääkäyttäjää luomaan aktiivisen lokin, josta saisi selville mahdolliset muutokset palomuurin asetuksissa. Tämä myös helpottaisi järjestelmän seurantaa epätavallisesta toiminnasta, koska aktiiviseen lokiin tulisi lisätä Azure käyttäjiä, joilla olisi oikeus tehdä muutoksia palomuuriin. Tänne tulisi siis ilmoituksia, jos siellä olisi jokin epäilyttävä käyttäjä yrittämässä tehdä muutoksia palomuurin asetuksiin ja sääntöihin.



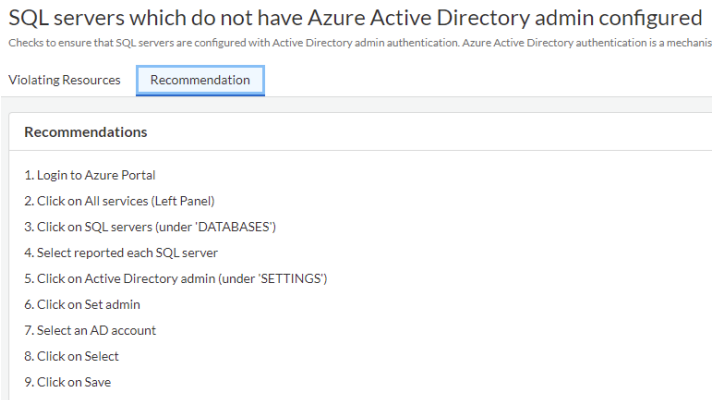
Kuvio 18. Azuren SQL-palvelimen TDE protector ei ole kryptattu omalla avaimella -hälytys ja sen korjausehdotus

Salausavaimien käyttöön on useita erilaisia vaihtoehtoja, ja tässä tapauksessa Azuren SQL-palvelimessa suositellaan käyttämään BYOK (Bring Your Own Key) -metodilla omaa asymmetristä avainta sen avainsäilöstä (Ks. kuvio 18.). Tämä parantaisi käyttäjänhallintaa TDE (Transparent Data Encryption) -kryptattujen avainten käyttöä, sekä rajoituksia siitä kuka niitä saa käyttää ja koska. Tämä tehostaisi taas Azuren palveluiden tietoturvaa, mutta kehitysympäristön kanssa kyseinen käytäntö voisi olla hieman kömpelö.



Kuvio 19. Azuren SQL-palvelimen ADS haavoittuvuusarviointien puute -hälytys ja sen korjausehdotus

Azuren SQL-palvelimella sijaitsee myös sen omat Advanced Data Security (ADS) haavoittuvuusarvioinnit, jotka ovat tämän hälytyksen laukeamisen mukaisesti pois päältä (Ks. kuvio 19.). Näiden arviointien pois päällä pitäminen vaikuttaa tietokannan palveluiden skannaamiseen. Sen tarkoituksena on skannata tietokannasta tiedetyt haavoittuvuudet ja korostaa poikkeamia, kuten konfiguraatiovirheet, liialliset käyttöoikeudet sekä kriittisen datan turvaamattomuutta. Tämä toimii siis Azuren omana skannaustyökaluna Azure Microsoft Defenderin lisäksi. Kuitenkin tämän on tarkoitus toimia vain tietokannoissa, eikä muualla ympäristöissä.



Kuvio 20. SQL-palvelimen Azuren AD adminin puute -hälytys ja sen korjausehdotus

Viimeinen SQL-hälytys perustuu sen palvelimen Active Directoryn (AD) adminin puutteena (Ks. kuvio 20.). Kyseiseen AD:hen ei ole siis konfiguroituna minkäänlaista admin autentikaatiota. Näin ol-

len Azuren omaa AD-ryhmää ei voida käyttää kirjautumisissa, koska sitä ei ole konfiguroitu kunnolla. Tämän ominaisuuden avulla voitaisiin hallita samaa AD-ryhmää Azuren SQL-tietokannan ja SQL-datavaraston välillä. Samaisen AD-ryhmän konfiguraatioilla voitaisiin myös hyötyä muiden Microsoftin palveluiden kanssa. Kuitenkin jos käytössä ei ole AD-kirjautumista, on tämä hälytys hieman turha.

6 Pohdinta

Prisma Cloudin huomiot ympäristöistä kertovat hyvää tilaa Pinjan omista julkisen pilven testiympäristöistä. Prisma Cloud ei löytänyt CSPM-ratkaisullaan merkittäviä tietoturvaongelmia ympäristöistä. Tavoitteena oli varmistaa sovellusten tietoturva, sekä samalla päästä testaamaan Palo Alton Prisma Cloud tuotetta. Vaikka kyseessä oli kuitenkin kehitysympäristö eikä tuotantoympäristö, voidaan tuloksia pitää luotettavina johtuen sovellusten kehityskaaresta. Havaintoja saatiin riittävästi aikaiseksi, mutta ne olivat pitkälti samoja koko kahden kuukauden kokeiluversion aikana. Prisma Cloud antoi useita erilaisia löydöksiä, mutta niiden taso ei ole kuitenkaan kriittinen. Samoja havaintoja on tullut useita kertoja uudestaan ympäristöjen luonnin ja päivittämisen aikana. Löydöksistä 6% oli High-tasoisia, 59% Medium-tasoista, sekä 35% Low-tasoista löydöstä.

Havaintojen laatu oli hyvin pitkälti false positive tyyppisiä havaintoja, jotka ovat yleisiä kehitysympäristöissä, joissa on useita kehittäjiä samaa aikaa toimimassa ympäristön kanssa. Näin ollen ympäristöihin ja palveluihin pääseminen on tehty huomattavasti helpommaksi, kuin esimerkiksi olisi tuotantoympäristöissä. Tämän johdosta löydöksiä on pitänyt pohtia hieman kriittisemmällä tasolla, kuten sitä, että olisiko kaikki konfiguraatiot näin tuotantoympäristöissä. Tämä johtuu siitä, että kehitysympäristöissä halutaan toimia mahdollisimman vaivattomasti ja tehokkaasti, jotta aikaa ei kulu turhaan kirjautumisongelmaan. Vaikka tuotantoympäristöjen tulisi olla usein samankaltaisia kuin kehitysympäristöt, on niissä kuitenkin aina hieman eroja juuri käytettävyyden ja tehokkuuden johdosta.

6.1 Voiko pilvipalveluiden turvallisuuden hallinta edistää turvallisuutta julkisen pilven sovellustuotteissa

CSPM-ratkaisut voivat luoda sen käyttäjilleen pohjan, jolla voidaan edistää julkisen pilven sovellustuotteiden kyberturvaa huomattavasti. Näiden ratkaisujen avulla voidaan päästä käsiksi haavoittuvuuksiin heti sen kehityspolun alussa, ilman että kyseiset ongelmat edes ehtivät tuotantoympäristöihin. Sen johdosta voidaan säästää huomattavasti työaikaa verrattuna siihen, että tuotantoympäristöä pitää alkaa muokkaamaan reilusti erilaisten haavoittuvuuksien johdosta (Puzas, 2021).

CSPM-ratkaisujen keskeinen tarkoitus on keskittyä juuri ihmisen tekemiin inhimillisiin virheisiin. Kyseiset virheet ovat aina läsnä, jos käyttäjä itse luo määrityksiään erilaisten järjestelmien luonnissa. Erilaisten virtuaalikoneiden ja -ympäristöjen luonnin aikana CSPM-ratkaisut voivat tehdä haavoittuvuuksien tarkastamisen huomattavasti nopeammin kuin ihminen. Kyseinen toiminto perustuu CSPM-ratkaisuihin sisällytetyistä kriteeristöistä ja standardeista, jotka määrittelevät erilaiset pilvipalveluihin liittyvät riskitekijät ja haavoittuvuudet. Suomessa on käytössä Traficomin Kyberturvallisuuskeskuksen oma arviointikriteeristö PiTuKri, joka sisältää pätkiä eri maiden omista kriteeristöistä, lainsäädännöstä sekä standardeja (Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri), 2020). PiTuKri sisältää myös oman tarkastustaulukkonsa, jonka avulla kuka tahansa pilvipalveluiden käyttäjä voi tarkistaa oman ympäristönsä tai tuotteensa turvallisuuden tilan. Arviointityökalun avulla voi saada selville myös erilaisten vaatimusten merkityksen pilvipalveluissa, sekä kuinka niitä voitaisiin toteuttaa. Taulukko myös tekee sen täyttämisen perusteella suosituksia tekijälleen, mihin heidän tulisi kiinnittää mahdollisesti enemmän huomiota omassa turvallisuudessaan. (PiTuKri-arviointityökalu 2020.)

Gillis (n.d.) mainitsee myös CSPM-ratkaisujen tuovan käyttäjälleen oman SOC-tyylisen seurantajärjestelmänsä sovellusten mukana. Kyseisten seurantajärjestelmien avulla voidaan seurata liikennettä, kirjautumisia sekä toiminta-aikaa. Kaikki nämä ovat yleisesti nähtävillä aina erilaisissa pilviympäristöissä, mutta usein ne sijaitsevat eri paikoissa järjestelmien kirjastorakenteissa. CSPM-ratkaisuissa ne kaikki siirretään samaan käyttöliittymään, josta niiden seuranta helpottuisi huomattavasti. CSPM-ratkaisujen mahdollistavat myös löydösten lähettämisen eri ryhmille, jotka on myös mahdollista integroida erilaisiin pikaviestisovelluksiin, kuten esimerkiksi viestintäpalvelu

Slackiin tai Microsoft Teamsiin. Näiden avulla voidaan tehokkaasti vähentää sähköpostiin hukkuvien löydösten myöhästymisiä, sekä nopeuttaa havaintoihin reagointia.

6.2 Palo Alto Prisman vaikutus Pinjan kyberturvaan julkisen pilven sovellustuotteissa

Palo Alton Prisma Cloudin vaikutukset Pinjan kyberturvaan eivät olleet valtavia CSPM-ratkaisua käyttäessä. Tutkimuksen tavoitteena oli selvittää Prisma Cloudin avulla Pinjan julkisen pilven sovellustuotteiden turvallisuutta, joka osoittautui onnistuneeksi tutkimuksen aikana. Kuitenkin tutkimus herätti laajaa keskustelua Pinjan sisällä heidän omien testiympäristöjensä tilasta, sekä haavoittuvuuksien hallinnasta. Havaintoja läpikäydessä sovellusten kehittäjien ja arkkitehtien kanssa, selvisi sieltä muutamia kohtia, joista he olettivat Prisma Cloud tekevän havaintoja. Kuitenkin niiden merkitys kehitysympäristössä on tiedostettu, eikä niitä sen johdosta päästetä ollenkaan tuotantoympäristöihin. Prisma Cloudin käytöstä oltiin kuitenkin kiinnostuneita sen käyttöliittymän toimivuuden kannalta, joka helpottaisi esimerkiksi arkkitehtien työtä. Sen avulla hän voisi tarkastella helpommin järjestelmien tilaa erilaisten havaintojen johdosta. Myös omien hälytysten ja kriteeristöjen luonti kiinnosti testiympäristöjen työntekijöitä, koska se mahdollistaisi helposti virheellisten konfiguraatioiden huomaamisen. Tämän tarkoituksena olisikin helpottaa juuri arkkitehtien työtä, jotka luovat usein järjestelmät itse. Näin voitaisiin myös jakaa vastuuta laajemmalle käyttäjäkunnalle, koska Prisma Cloud tarkistaisi kuitenkin ympäristön turvallisuuden, jolloin arkkitehti voisi vain kyseisen järjestelmän käynnistyksen lokeista tarkistaa sen tilan.

6.3 Konfiguraatioiden merkitys julkisen pilven kyberturvassa

Konfiguraatioiden merkitystä julkisessa pilvessä ei voi vähätellä yhtään. Niiden avulla sovelluksesta voidaan tehdä turvallinen ja toimiva, tai sitten se voi jäädä haavoittuvaiseksi sisältäen ohjelmointivirheitä. On tärkeä tietää mitä vaatimuksia ympäristöllä tai sovelluksella on, ja minkälaisia haavoittuvuuksia se voi pitää sisällään. Tuotantoympäristöjen kriittisen datan säilyttäminen on elin ehto kaikille kaupallisille sovelluksille nykyään. Pienenkin konfiguraatiovirheen johdosta järjestelmä voi antaa tunkeutujalle mahdollisuuden päästä järjestelmään sisälle, ja viedä sieltä esimerkiksi käyttäjänsä dataa tai sitten henkilötietoja. Gillis (n.d.) mainitsee kehittyvän DevSecOps -käytäntöjen kehittymisen CSPM-ratkaisujen yhteydessä, jossa konfiguraatiovirheiden minimalisointi mahdollistaa myös enemmän aikaa kehittäjille keskittyä uusiin ominaisuuksiin. Näin ollen käytetyn järjestelmän

kehittämiseen mahdollistetaan enemmän aikaa, kuin siihen että sitä jouduttaisiin korjata liian usein haavoittuvuuksien takia.

Erilaisten konfiguraatiovirheiden ymmärtäminen on myös tärkeä osa pilvijärjestelmiä, vaikka käytössä ei olisi erilaisia CSPM-ratkaisuja. Top Threats to Cloud Computing (2019) artikkelin mainitsemat yleisimmät konfiguraatiovirheet tulisi aina tarkistaa ennen järjestelmän luontia. Jos käytössä on jonkinlainen automaatiokäytäntö pilvijärjestelmien luontiin, tulisi sekin tarkistaa säännöllisin väliajoin, jotta vältyttäisiin turhilta haavoittuvuuksilta ja järjestelmävirheiltä. Esimerkiksi käyttäjätietoja luodessa, tulisi aina välttää root-käyttäjän luomista. Konfiguraatiovirheiden tarkastaminen tulisikin siis olla säännöllistä, vaikka se veisikin reilusti aikaa. Järjestelmien haavoittuvuuksilta välttyminen on ydinajatus, joka pitäisi olla aina mielessä, kun luo uutta pilviympäristöä tai -järjestelmää. Haavoittuvien sovellusten tarkastaminen on kuitenkin huomattavasti hitaampaa, jonka johdosta erilaisten ohjelmien käyttäminen niihin on suotavaa. Kuitenkin erilaisten haavoittuvuustietokantojen kautta voi aina käydä tarkistamassa käytössä olevan käyttöjärjestelmän tilanteen, ja sitä kautta varmistaa käytössä olevan version turvallisuus.

CSPM-ratkaisujen tuomia etuja konfiguraatioiden kanssa on olennaista myös ajatella kansainvälisiä kauppasuhteita. Erilaisten kansainvälisten vaatimusstandardien käyttäminen konfiguraatioiden tarkastuksessa voi luoda palveluntarjoajasta luotettavampaa kuvaa, koska he voivat esitellä listaa erilaisista kriteeristöistä, joiden avulla heidän pilvijärjestelmänsä tarkistetaan. Tunnettujen kriteeristöjen maininta luo luotettavuutta myytävään järjestelmään.

Lähteet

A 1101/2019. Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa. Viitattu 25.2.2022. https://www.finlex.fi/fi/laki/alkup/2019/20191101

Aropaltio, A. 2022. Systems Engineer. Palo Alto Networks. Keskustelu aiheesta Prisma Cloud sekä Bridgecrew by Prisma Cloud. Viitattu 18.2.2022

Bulut, M., Hwang, J. 2021. NL2Vul: Natural Language to Standard Vulnerability Score for Cloud Security Posture Management. Konferenssiartikkeli. Viitattu 17.3.2022. IEEE. https://janet.finna.fi, IEEE Xplore.

CheckPoint CloudGuard. N.d. CheckPointin sivusto Cloudguard tuotteesta. Viitattu 18.3. https://www.checkpoint.com/cloudguard/cloud-security-posture-management/

Crowdstrike Falcon Horizon CSPM. N.d. Crowdstriken verkkosivut Falcon Horizon CSPM -tuotteesta. Viitattu 18.3.2022. https://www.crowdstrike.com/cloud-security-products/falcon-horizon-cspm/

Crowdstrike. N.d. Crowdstriken verkkosivut. Viitattu 18.3. https://www.crowdstrike.com/

False Positive. n.d. F-Securen verkkosivun tarkennus termiin false positive. Viitattu 30.3.2022. https://www.f-secure.com/v-descs/false_positive.shtml

FGillis, A. n.d. Cloud Security Posture Management (CSPM). SearchCloudSecurity sivuston määritelmä Cloud Security Posture Management:lle. Viitattu 17.3.2022. https://searchcloudsecurity.techtarget.com/definition/Cloud-Security-Posture-Management-CSPM

L 906/2019. Laki julkisen hallinnon tiedonhallinnasta. Viitattu 25.2.2022. https://www.finlex.fi/fi/laki/alkup/2019/20190906

Mell, P. & Grance, T. 2011. The NIST Definition of Cloud Computing. National Institute of Standards and Technology U.S. Department of Commerce. NIST:in julkaisema ohjeistus pilvipalveluista. Viitattu 7.2.2022. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

Nagpal, B., Sharma, P., Chauhan, N. & Panesar, A. 2015. DDoS tools: Classification, analysis and comparison. Konferenssiartikkeli. IEEE. Viitattu 25.2.2022. https://janet.finna.fi, IEEE Xplore.

Palo Alto TechDocs. 2022. Palo Alton dokumentaatiota Prisma Cloudin käyttöön. Päivitetty 16.3.2022. Viitattu 17.3.2022. https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/get-started-with-prisma-cloud/prisma-cloud.html

Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri). 2020. Traficom, Liikenne- ja viestintävirasto, Kyberturvallisuuskeskus. Traficomin julkaisuja 13/2020. Viitattu 27.1.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf.

PiTuKri-arviointityökalu. 2020. Traficomin Kyberturvallisuuskeskuksen luoma taulukkopohjainen arviointityökalu. Julkaistu 23.3.2020. Viitattu 27.1.2022. https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/pilvipalveluiden-turvallisuuden-arviointikriteeristo-pitukri.

Puzas, D. 2021. What is Cloud Security Posture Management (CSPM)?. Crowdstrike sivuston artikkeli aiheesta Cloud Security Posture Management. Viitattu 17.3.2022. https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-security-posture-management-cspm/

Rupelia, N. 2016. Cloud computing. The MIT Press. Viitattu 7.2.2022. https://janet.finna.fi, IEEE Xplore.

Security guidance for critical areas of focus in cloud computing v4.0. 2017. Cloud Security Alliancen julkaisema PDF-kirja. Viitattu 7.2.2022. https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf.

Top Threats to Cloud Computing. 2019. Cloud Security Alliancen julkaisema PDF-artikkeli. Viitattu 1.5.2022. https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/.

Valtiovarainministeriö. 2018. Julkisen hallinnon pilvipalvelulinjaukset. Valtiovarainministeriön julkaisu – 35/2018. Viitattu 7.2.2022. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161294/VM_35_2018_Julk_hallinnon_pilvipalvelulinjaukset.pdf?sequence=1&isAllowed=y

What is the CIA Triad? Definition and examples. 2021. SecurityScorecard blogi. Julkaistu 1.9.2021. Viitattu 25.2.2022. https://securityscorecard.com/blog/what-is-the-cia-triad#:~:text=Confidentiality%2C%20Integrity%2C%20and%20Availability.,organization's%20security%20procedures%20and%20policies

Wu, W., Zhang, Q. & Wang, Y. 2019. Public Cloud Security Protection Research. Konferenssiartikkeli. Viitattu 25.2.2022. IEEE. https://janet.finna.fi, IEEE Xplore.

Liitteet

Liite 1. Vaatimusstandardit

AWS:

- APRA CPS 234
- Brazilian Data Protection Law (LGPD)
- CIS AWS 3 Tier Arch v1.0
- CCPA 2018
- CIS v1.2
- CIS v1.3
- CIS AWS v.1.4
- CSA CCM v3.0.1
- CSA CCM v4.0.1
- CMMC
- GDPR
- HITRUST v9.3
- HITRUST v9.4.2
- HIPAA
- ISO 27001:2013
- MAS TRM 2021
- MITRE ATT&CKv6.3
- MITRE ATT&CKv8.2
- MPAA Content Protection Best Practice v4.08
- Multi-Level Protection Scheme (MLPS) v2.0
- NIST 800.53 Rev4
- NIST 800-53 Rev5
- NIST 800-171 Rev1
- NIST SP 800-171 Rev2
- NIST SP 800-172
- NIST 800-53 Rev5
- NIST CSF v1.1
- PCI DSS v3.2
- PIPEDA
- Monetary Authority of Singapore (MAS) Technology Risk Management (TRM)
- Risk Management in Technology (RMiT)
- SOC 2
- AWS well architected framework
- CyberSecurity Law of the People's Republic of China
- CIS AWS 3 Tier Arch v1.0
- ISO/IEC 27002:2013
- ISO/IEC 27018:2019
- ISO/IEC 27017:2015
- MITRE ATT&CK v10.0

Azure:

- Azure Security Benchmark (ASB) v2
- APRA CPS 234
- Brazilian Data Protection Law (LGPD)
- CCPA 2018
- CIS v1.1
- CIS v1.2
- CIS v1.3
- CIS v1.3.1
- CIS v1.4.0
- CMMC
- CSA CCM v3.0.1
- CSA CCM v4.0.1
- GDPR
- HITRUST v9.3
- HITRUST v9.4
- HIPAA
- ISO 27001:2013
- MITRE ATT&CKv6.3
- MITRE ATT&CKv8.2
- MPAA Content Protection Best Practice v4.08
- Multi-Level Protection Scheme (MLPS) v2.0
- NIST 800.53 R4
- NIST 800-53 Rev5
- NIST CSF v1.1
- NIST SP 800-171 Rev2
- NIST SP 800-172
- PCI DSS v3.2
- PIPEDA
- SOC 2
- CyberSecurity Law of the People's Republic of China
- ISO/IEC 27002:2013
- ISO/IEC 27018:2019
- ISO/IEC 27017:2015
- MITRE ATT&CK v10.0

GCP:

- APRA CPS 234
- Brazilian Data Protection Law (LGPD)
- CCPA 2018
- CIS v1.0

- CIS v.1.1
- CIS v.1.2
- CIS GKE v1.1
- CSA CCM v3.0.1
- CSA CCM v4.0.1
- CMMC
- GDPR
- HITRUST v9.3
- HITRUST v9.4
- HIPAA
- ISO 27001:2013
- MITRE ATT&CKv6.3
- MITRE ATT&CKv8.2
- MPAA Content Protection Best Practice v4.08
- NIST 800.53 R4
- NIST 800-53 Rev5
- NIST CSF v1.1
- NIST SP 800-171 Rev2
- NIST SP 800-172
- PCI DSS v3.2
- PIPEDA
- SOC 2
- ISO/IEC 27002:2013
- ISO/IEC 27018:2019
- ISO/IEC 27017:2015
- MITRE ATT&CK v10.0

Alibaba:

- Brazilian Data Protection Law (LGPD)
- CIS v1.0.0
- CMMC
- CSA CCM v4.0.1
- HITRUST v9.3
- MAS TRM 2021
- MPAA Content Protection Best Practice v4.08
- Multi-Level Protection Scheme (MLPS) v2.0
- MITRE ATT&CKv8.2
- NIST 800.53 Rev4
- NIST 800-53 Rev5
- NIST CSF v1.1
- NIST SP 800-171 Rev2
- NIST SP 800-172
- PCI DSS v3.2
- MAS TRM
- RMiT
- CyberSecurity Law of the People's Republic of China

- ISO/IEC 27002:2013
- ISO/IEC 27018:2019
- ISO/IEC 27017:2015
- MITRE ATT&CK v10.0

Oracle Cloud Infrastructure

- CIS v1.0
- CIS v1.1
- CSA CCM v4.0.1
- HITRUST v9.4
- MITRE ATT&CKv8.2
- MPAA Content Protection Best Practice v4.08
- NIST SP 800-171 Rev2
- NIST SP 800-172
- NIST CSF v1.1
- PCI DSS v3.2
- ISO/IEC 27002:2013
- ISO/IEC 27018:2019
- ISO/IEC 27017:2015
- MITRE ATT&CK v10.0