KOKKUVÕTE

Telegrupp AS-i tegevusvaldkonnast tingituna tegeletakse palju konfidentsiaalse informatsiooniga ja seetõttu on vaja suuremat läbipaistvust töötajate tegevusele ja võimalikele välistele ohtudele. Diplomitöö eesmärgiks oli tagada parem läbipaistvus kasutajate tegevustesse Telegrupp AS infotehnoloogia taristus ja selle eesmärgi täitmiseks juurutada kasutajate käitumispõhise analüütika töörist.

Lõputöös andis autor ülevaate Telegrupp AS-i infotehnoloogia taristule ning kogutavatele andmetele. Sellele järgnes infoturbe ja logide halduse süsteemi kirjeldus enne käitumispõhise analüütika tööriista juurutamist koos selle arhitektuurilise ülevaatega. Töö käigus kaardistati algse süsteemi puudujäägid ja selgitati puudujääkide kriitilisus ettevõtte seisukohast. Enne tööriista juurutamist testiti testikeskkonnas selle sobivust ettevõtte infotehnoloogia taristusse ja samuti veenduti tööriista põhifunktsionaalsuse toimimises.

Kuna enne edasiarendust ei olnud normaliseeritud logidest saadud kasutajad seotud ühe konkreetse töötajaga, siis osa informatsiooni ei olnud ka seotud võimalike intsidentidega ja nende uurimisega, juhul kui intsident hõlmas erinevate kasutajate kasutamist üle IT-taristu. Samuti eeldas uurimine seda, et SIEM süsteem oli tuvastanud intsidendi. Kasutades UBA tööriista koostatud kasutajapõhist riskifaktorit, on võimalik alustada uurimist ennatlikult.

Juurutatud käitumispõhise analüütika tööriist tagab läbipaistvuse ja ülevaate kasutajate tegevusele IT-taristus ja sellest lähtuvalt loeb autor diplomitöö mõlemat eesmärki täidetuks.

SUMMARY

Due to Telegrupp AS's field of activity a lot of confidential information is handled and therefore, there is a need for greater transparency in the activities of employees and possible external threats. The aim of this thesis was to ensure greater transparency in the activities of the users of Telegrupp AS IT infrastructure and to introduce a user behavior analytics tool.

In his diploma work, the author gave an overview of Telegrupp AS's information technology infrastructure and the data collected from different parts of it. This was followed by a description of the security information and event management system, before the introduction of an analytics tool, and its architectural overview. During the thesis, the original system's shortcomings where mapped in regard to their criticality to the business. Before the analytics tool was deployed, it was tested in a test environment for its suitability into the companies' information technology infrastructure and also the basic functionality of the tool was verified.

Before the upgrade, all parsed usernames where handled as separate identities. This meant that information was not tied to a single person and pieces of information where missed during incidents where multiple accounts were used maliciously. It also meant that the only reason to start an investigation was for an incident to happen and register. With UBA there is the possibility of proactive investigations because you have an overview of the risk score of all users.

The introduced behavioral analytics tool provides transparency and insight into the users' activities in the IT infrastructure, and as a result, the author considers both objectives of the thesis to be fulfilled.