Ministerul Educației Culturii și Cercetării al Republicii Moldova

Universitatea Tehnică a Moldovei

FACULTATEA Calculatoare, Informatică și Microelectronică

Departamentul Informatică și ingineria sistemelor

Admis la susținere

Șef departament: conf, univ., dr. Sudacevschi Viorica

"09" 01 2019

Analiza și gestiunea incidentelor cibernetice în baza SIEM

TEZĂ DE MASTER ÎN

Calculatoare și Rețele Informaționale

Masterand: A. Gromic (Gromic)

Conducător: O. Negruța (Negruța)

Chișinău – 2019

ADNOTARE

La teza de master: „Analiza și gestiunea incidentelor cibernetice în baza SIEM”, elaborat de Gromic Andrei, Chișinău, 2019.

Cuvinte cheie: analiză, gestionare, incident cibernetic, securitate, informaţii, AlienVault.

Lucrarea de față are drept scop pregătirea și detectarea, restrângerea, eradicarea și recuperarea incidentelor cibernetice, gestiunea diferitor tipuri de incidente cibernetice, cât și utilizarea Managerului de informații privind securitatea informațională Open Source AlienVault.

Tehnologiile utilizate sunt: AlienVault, care oferă funcționalitatea unui SIEM tradițional. Dispozitivul include capabilitățile esențiale de securitate necesare pentru a monitoriza eficient rețeaua locală într-o singură platformă unificată, ușurează utilizarea și implementarea, este perfectă pentru organizațiile cu resurse limitate; SIEM, principiul de bază al acestuia este că informațiile relevante despre securitatea unei întreprinderi sunt produse în diverse surse, iar datele sunt corelate și văzute dintr-o locație centrală. Acest proces facilitează studiul modelelor și tendințelor care nu sunt permise. SIEM este o combinație de gestionare a informațiilor de securitate (SIM) și funcții de gestionare a evenimentelor de securitate (SEM) într-un singur sistem de management al securității. În detaliu, segmentul SIM accentuează în principal analiza datelor istorice care intenționează să îmbunătățească performanța stocării pe termen lung și eficiența infrastructurilor de securitate a informațiilor.

Memoriul explicativ conţine: Introducere, 3 capitole, concluzii, bibliografie cu 52 titluri, dintre care 84 pagini text de bază, 26 figuri, 6 tabele.

Capitolul 1 definește pașii de analiză a diferitor tipuri de incidente cibernetice, activitățile ce trebuie realizate în cazul depistării unui incident cibernetic și clasificarea incidentelor cibernetice.

Capitolul 2 definește sistemul de gestionare a incidentelor cibernetice, precum și gestionarea incidentelor cibernetice neautorizare de acces și a incidentelor bazate pe cod malițios (malware).

Capitolul 3 prezintă informații de securitate și gestionare a evenimentelor, precum și despre managerul de informații privind securitatea Open Source. În acest capitol al tezei este prezentat planul de implementare al AlienVault, sunt definiți pașii concreți privind configurarea și utilizarea eficientă a AlienVault.

ANNOTATION

In the master thesis "Analysis and management of cyber incidents based on SIEM", elaborated by Gromic Andrei, Chisinau, 2019.

Keywords: analysis, management, cyber incident, security, information, AlienVault.

This paper aims to prepare and detect, restrict, eradicate and recover cyber incidents, manage various types of cyber incidents, and use the Open Source AlienVault Information Security Information Manager.

The technologies used are: AlienVault, which offers the functionality of a traditional SIEM. The device includes the essential security capabilities required to efficiently monitor local network in a single unified platform, ease of use and deployment, and is perfect for organizations with limited resources; SIEM, its basic principle is that relevant information about an enterprise's security is produced in various sources, and the data is correlated and viewed from a central location. This process facilitates the study of patterns and trends that are not allowed. SIEM is a combination of security information management (SIM) and security event management (SEM) functions in a single security management system. In detail, the SIM segment mainly emphasizes the analysis of historical data that aims to improve long-term storage performance and the efficiency of information security infrastructures.

The explanatory memo contains: Introduction, 3 chapters, conclusions, bibliography with 52 titles, of which 84 basic text pages, 26 figures, 6 tables.

Chapter 1 defines the steps of analyzing different types of cyber incidents, the activities to be performed in the event of a cyber incident and the classification of cyber incidents.

Chapter 2 defines the cyber incident management system, as well as the management of cyber-incidents, unauthorized access, and malware-based incidents.

Chapter 3 provides security and event management information, as well as the Open Source Security Information Manager. In this chapter the thesis presents the implementation plan of AlienVault, the concrete steps for configuring and efficient use of AlienVault are defined.

CUPRINS

.