Manažment bezpečnostných informácií a udalosti pre akademický informačný systém

Autor práce: Bc. Eva Marková

Vedúci práce: RNDr. JUDr. Pavol Sokol, PhD.

Motivácia

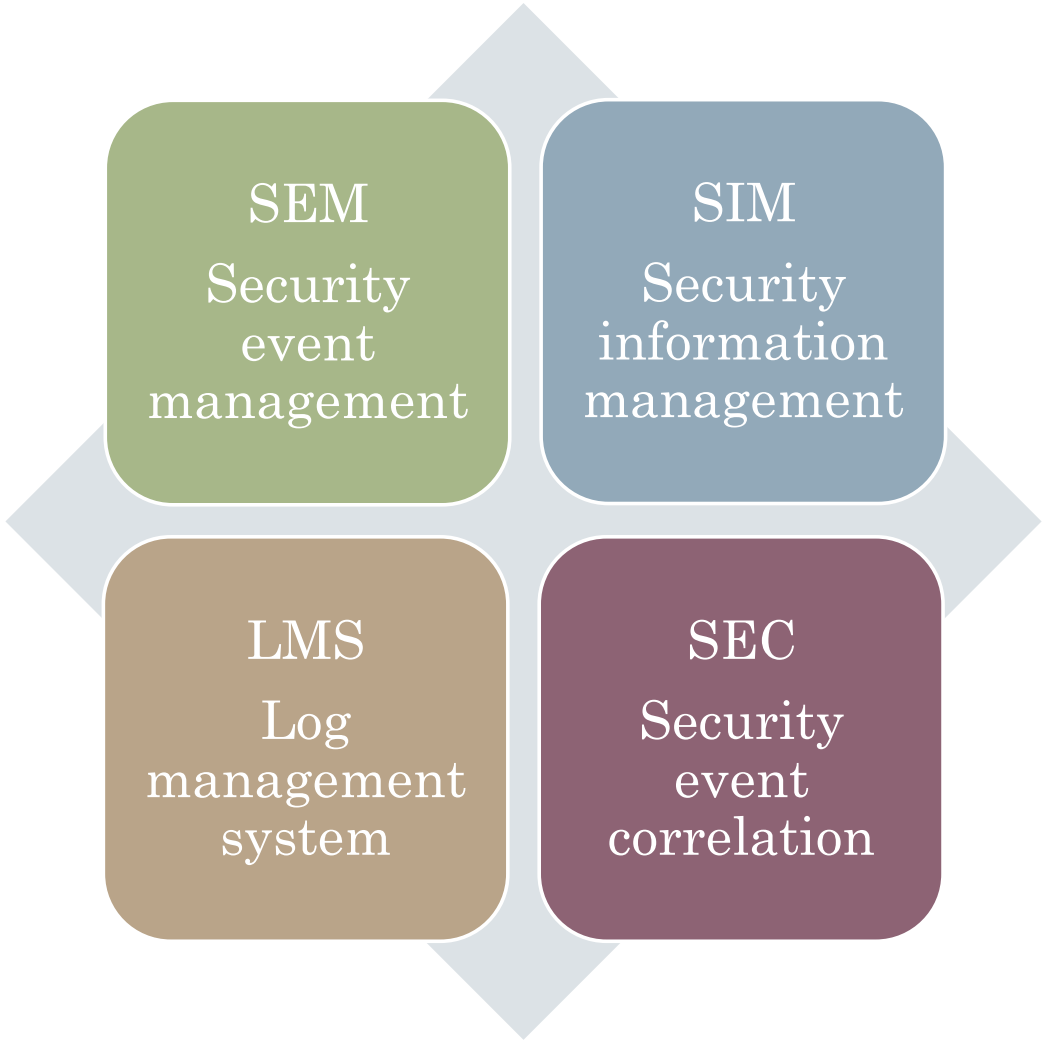
- S postupujúcimi a rastúcimi organizáciami sa zvyšuje úroveň útoku
- Mnoho aktív generuje mnoho bezpečnostných udalostí
- Hrozby sú ťažšie detekovateľné a to vedie k narušeniu bezpečnosti
- Incidenty sú často odhalené až po dlhšej dobe alebo sú úplne nepovšimnuté
- Akademický informačný systém
  - Najkritickejšia infraštruktúra v rámci univerzity
  - Kumulácia množstva osobných údajov

Ciele

1. Analýza aktuálnych prístupov k manažmentu bezpečnostných informácií a udalosti (SIEM)
2. Návrh dátového modelu a pravidiel detekcie bezpečnostných hrozieb pre akademický informačný systém zohľadňujúc bezpečnostné riziká podľa ISO/IEC 27000 a MITRE ATT&CK rámec
3. Návrh, implementácia a optimalizácia SIEM systému pre akademický informačný systém

SIEM

Security
Information
and
Event
Management



SIEM

- Prístup, ktorý ponúka pozorovanie informačnej bezpečnosti organizácie
- Umožňuje členom SOC (Security Operations Center) vykonávať analýzy založené na upozorneniach a udalostiach s cieľom nájsť hlavnú príčinu incidentov
- Zhromažďuje viac zdrojov údajov vrátane monitorovania siete, zariadení a riešení na ochranu koncových staníc
- SIEM je dôležitý, pokiaľ ide o riadenie bezpečnostných incidentov, ktoré sa vyskytnú v inštitúcii

Čo ponúka SIEM?

- **Nástenka s upozorneniami** - všetky výstrahy sú zlúčené do jedného nástroja
- **Korelácia udalostí** zvyšuje vernosť zistení viacerých podozrivých udalostí na základe spoločných kritérií alebo podivného správania.
- Je schopný **zameriavať sa na viacero súborov údajov**, aby sa stanovila hlavná príčina incidentu
- V závislosti od konkrétneho SIEMu môžeme definovať a **spravovať detekcie** na základe indikátorov a detekčných pravidiel
- Existujú rôzne normy pre rôzne časti odvetvia, v ktorých je riešenie SIEM povinné **dodržiavať zásady a predpisy**

Rôzne implementácie

- IBM QRadar – komerčné
- ArcSight – komerčné
- Splunk Free – 500MB denne
- AlienVault OSSIM – open source
- Elastic Stack – open source

Čo je Elastic Stack?

- Sada nástrojov vyvinutá spoločnosťou Elastic
- Elasticsearch – NoSQL databáza
- Logstash – nástroj na agregáciu prichádzajúcich logov a správ, ich spracovanie
- Kibana – vizualizácia dát
- Beats nástroje – Metricbeat, Winlogbeat, Packetbeat, Libbeat
- Zadarmo, open source, skvelé na fulltextové vyhľadávanie
- Alerting

AiS2

- 3 typy serverov – produkčný, vývojový a testovací
- Apache 2 → Tomcat → Java servlety

```
158.197.62.76 : - : - : [16/Jan/2018:15:08:10 +0100] : GET
/ais/start.do HTTP/1.1 : 200 : 2857 : - : Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/63.0.3239.132 Safari/537.36 : 158.197.62.76 : 2857 : - :
57518 : proxy:balancer://aiscluster/ais/start.do : HTTP/1.1 : 0 :
GET : - : - : 443 : 10814 :  : GET /ais/start.do HTTP/1.1 : proxy-
server : 0 : /ais/start.do : + : 1021 : 9497
```

▸ April 15th 2020, 17:20:22.940 path: ff02::1:ff1d:8894 @timestamp: April 15th 2020, 17:20:22.940 bytes_in: 24 ip: ff02::1:ff1d:8894

kibana

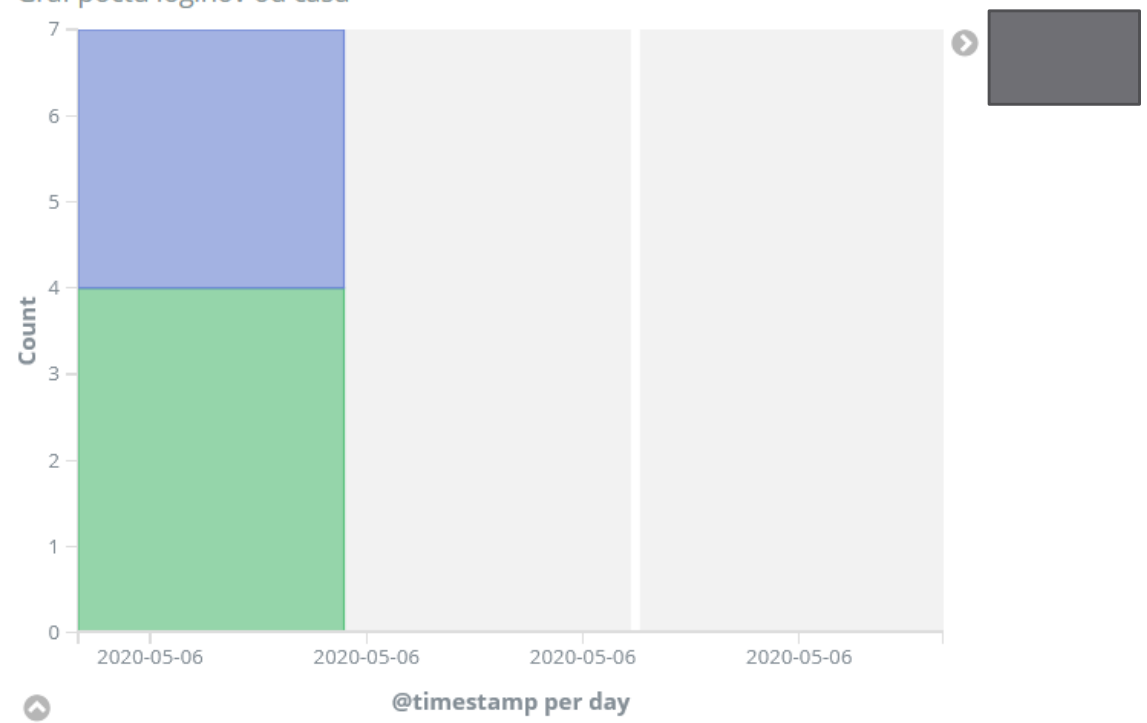
3,597 hits

New Save Open Share Last 15 minutes

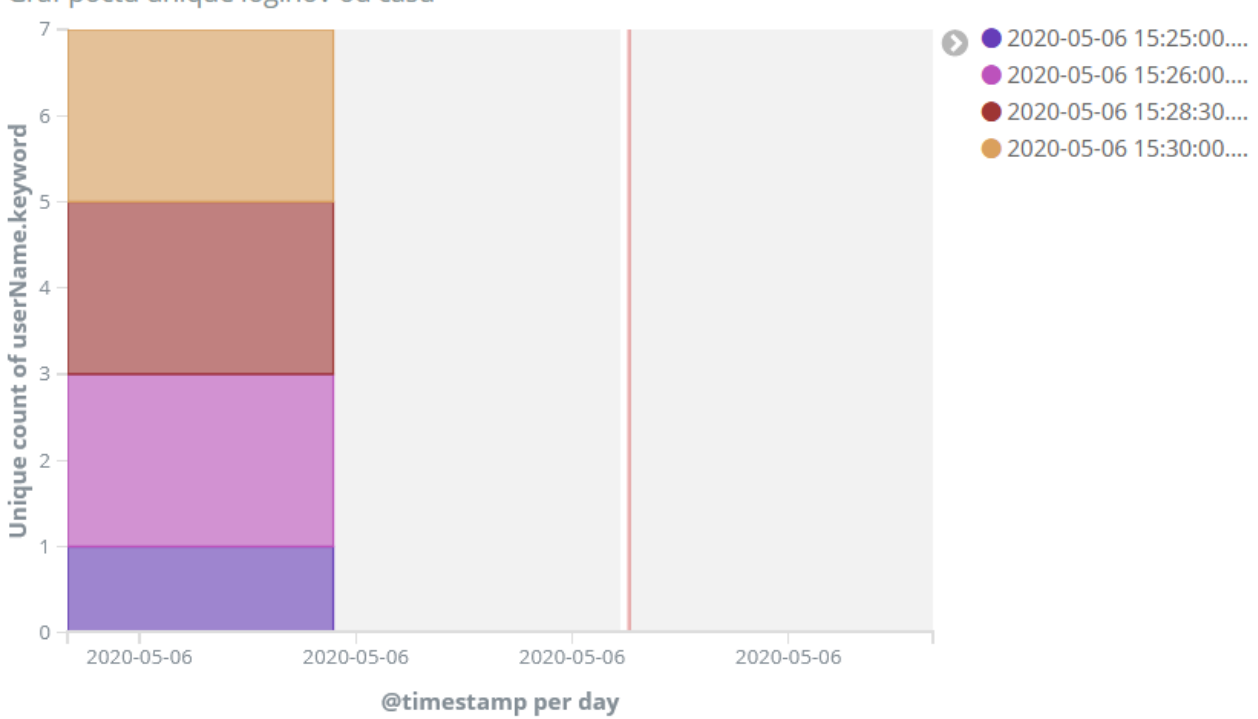
Search... (e.g. status:200 AND extension:PHP)

Uses lucene query syntax

Graf poctu loginov od casu



Graf poctu unique loginov od casu



Loginy a ich pocet

t host
t instalacia
t instancia
t level
t appId

Collapse

▸ 2020-05-06 15:32:20.915 offset: 124,667 level: DEBUG logger: a.s.conPool logMessage: check connections message: 2020-05-06 15:32:20,915 DEBUG [cpool-CheckingThread] a.s.conPool - check connections type: server instalacia: UPJS-TEST threadName: cpool-CheckingThread path: /opt/ais2-test/ais2-conf/logs/ais.log.2020-05-06_15 instancia: server11 @timestamp: 2020-05-06 15:32:20.915 host: vyvoj2.science.upjs.sk @version: 1 _id: AXHqLt0A7VaovQ31oBNo _type: server _index: logstash-2020.05.06 score: -

pril 15th 2020, 17:20:20.003 last_time: April 15th 2020, 17:19:22.900 flow_id: EQIA////DP////8U//8BAAGErY23Oe7 ///////8AAAAA/////0QAQwA final: true beat.name: evka-pc beat.hostname: evka-pc beat.version: 5.1.1

Analýza rizík

	ID zraniteľnosti	Zdroj zraniteľnosti (aktívum)	Popis zraniteľnosti
ID hroz	V01		

Aktívum	Klasifikácia	Bezpečnostné kritérium	Vlastník aktíva	Hodnota aktíva	Popis

T25		
V23		
V24		
V25		

MITRE ATT&CK

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Command-Line Interface	.bash_profile and .bashrc	Exploitation for Privilege Escalation	Binary Padding	Bash History	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	Bootkit	Process Injection	Clear Command History	Brute Force	Browser Bookmark Discovery	Exploitation of Remote Services	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
Hardware Additions	Graphical User Interface	Browser Extensions	Setuid and Setgid	Compile After Delivery	Credential Dumping	File and Directory Discovery	Internal Spearphishing	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Spearphishing Attachment	Local Job Scheduling	Create Account	Sudo	Connection Proxy	Credentials from Web Browsers	Network Service Scanning	Remote File Copy	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Spearphishing Link	Scripting	Hidden Files and Directories	Sudo Caching	Disabling Security Tools	Credentials in Files	Network Sniffing	Remote Services	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing via Service	Source	Kernel Modules and Extensions	Valid Accounts	Execution Guardrails	Exploitation for Credential Access	Password Policy Discovery	SSH Hijacking	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Supply Chain Compromise	Space after Filename	Local Job Scheduling	Web Shell	Exploitation for Defense Evasion	Input Capture	Permission Groups Discovery	Third-party Software	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service

ATT&CK navigátor

- Vlastný pohľad na Mitre ATT&CK - zvýraznenie dôležitých techník apod.
- https://github.com/mitre-attack/attack-navigator
- https://mitre-attack.github.io/attack-navigator/enterprise/

Príklad: User Execution

Mitigations

Mitigation	Description
Execution	Application whitelisting may be able to prevent the running of executables masquerading as other files
	may be used to conceal malicious files in Obfuscated Files or Information.
User Training	Use user training as a way to bring awareness to common phishing and spearphishing techniques and how to raise suspicion for potentially malicious events.

Detection

Monitor the execution of and command-line arguments for applications that may be used by an adversary to gain Initial Access that require user interaction. This includes compression applications, such as those for zip files, that can be used to Deobfuscate/Decode Files or Information in payloads.

Anti-virus can potentially detect malicious documents and files that are downloaded and executed on the user's computer. Endpoint sensing or network sensing can potentially detect malicious events once the file is opened (such as a Microsoft Word document or PDF reaching out to the internet or spawning Powershell.exe) for techniques such as Exploitation for Client Execution and Scripting.

Odporúčaná literatúra

1. MURDOCH, D. W. SOC, SIEM, and Threat Hunting (V1.02): A Condensed Guide for the Security Operations Team and Threat Hunter. Independent Publishing, 2019.
2. COLLINS, Michael. Network Security Through Data Analysis: From Data to Action. O'Reilly Media, Inc., 2017.
3. STROM, Blake E., et al. Finding cyber threats with ATT&CK-based analytics. Technical Report MTR170202, MITRE, 2017.

Ďakujem za pozornosť