Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică şi Microelectronică

Departamentul Ingineria Software și Automatică

**RAPORT**

Lucrarea de laborator nr. 6

*Metode și mijloace tehnice de protecție a informației.*

A efectuat: st. gr. SI-211 Chihai Adrian

A verificat: dr. conf.univ. Colesnic Victor

Chișinău – 2024

**Lucrare de laborator 6**

**Tema:** Bitdefender GravityZone

**Scopul lucrării**: Studierea GravityZone ce oferă o protecție sporită împotriva atacurilor prin folosirea unui set extins de tehnologii de proteсție a sistemelor, de detectare și prevenire a amenințărilor, precum și învățarea automată și analiza comportamentală a componentelor sistemului.

**Analiza soluțiilor oferite de Bitdefender GravityZone**

1. **Soluțiile oferite de GravityZone**

Bitdefender GravityZone este o platformă de securitate completă care oferă o varietate de soluții pentru a proteja organizațiile împotriva amenințărilor cibernetice. Printre aceste soluții se numără:

* **Antimalware**: Protecție împotriva programelor malware, inclusiv viruși, troieni și ransomware.
* **Advanced Threat Control (HyperDetect)**: Tehnologie avansată de detecție a amenințărilor care identifică și blochează atacurile înainte de a afecta sistemele.
* **Advanced Anti-Exploit**: Mecanisme de protecție împotriva exploit-urilor care vizează aplicațiile vulnerabile.
* **Firewall**: Soluție de securitate pentru monitorizarea și controlul traficului de rețea.
* **Network Attack Defense**: Protecție împotriva atacurilor la nivel de rețea, inclusiv atacuri de tip DDoS.
* **Patch Management**: Gestionarea actualizărilor de software pentru a remedia vulnerabilitățile sistemului.
* **Integrity Monitoring**: Monitorizarea integrității fișierelor și configurărilor critice pentru a detecta modificările neautorizate.
* **Device Control**: Controlul accesului la dispozitive externe conectate la rețea, cum ar fi USB-urile.
* **Full Disk Encryption**: Criptarea întregului disc pentru protejarea datelor sensibile în caz de furt sau pierdere a dispozitivului.
* **Security for Exchange**: Protecție dedicată pentru serverele de email Exchange, inclusiv detecția spam-ului și a atacurilor de tip phishing.
* **Sandbox Analyzer**: Analiza comportamentului fișierelor suspecte într-un mediu izolat pentru a determina dacă acestea sunt dăunătoare.
* **eXtended Detection and Response**: Capacități avansate de detectare și răspuns extins, integrând date din mai multe surse pentru o viziune unificată asupra amenințărilor.
* **Endpoint Detection and Response**: Soluție pentru monitorizarea și răspunsul la incidentele de securitate la nivel de endpoint.
* **Security for Storage**: Protecție pentru soluțiile de stocare, asigurându-se că datele sunt în siguranță.
* **GravityZone Security for Containers**: Securitate pentru aplicațiile și mediile bazate pe containere.
* **Email Security**: Protecție împotriva amenințărilor cibernetice care vin prin intermediul email-ului, inclusiv malware și phishing.

1. **GravityZone Business Security Enterprise**

GravityZone Business Security Enterprise oferă soluții avansate pentru protejarea endpoint-urilor, fiind un instrument esențial în arsenalul de securitate al organizațiilor. Printre opțiunile propuse de acest produs se numără:

* **Endpoint Detection and Response (EDR)**: Monitorizarea continuă a activităților pe endpoint-uri pentru a detecta comportamentele anormale și a răspunde rapid.
* **HyperDetect**: Tehnologie avansată de detecție a amenințărilor care ajută la identificarea rapidă a atacurilor complexe.
* **Fileless Attack Protection**: Protecție împotriva atacurilor fără fișiere, care utilizează aplicații legitime pentru a compromite sistemele.
* **Incidents**: Gestionarea și investigarea incidentelor de securitate pentru a reduce impactul acestora.
* **Endpoint tags**: Utilizarea etichetelor pentru a organiza și clasifica endpoint-urile, facilitând gestionarea acestora.
* **Live Search**: Funcționalitate care permite căutarea în timp real a endpoint-urilor pentru a identifica amenințări sau activități suspecte.
* **Cross-endpoint correlation**: Corelarea datelor și alertelor între endpoint-uri pentru a oferi o imagine de ansamblu mai completă asupra incidentelor de securitate.
* **Autonomous response recommendations**: Recomandări automate pentru acțiuni de răspuns, ajutând organizațiile să reacționeze rapid și eficient la amenințări.
* **Custom Rules for EDR**: Posibilitatea de a crea reguli personalizate pentru a se adapta nevoilor specifice de securitate ale organizației.

**Concluzie**: În urma sarcinilor realizate privind studiul și testarea soluției Bitdefender GravityZone, s-a evidențiat importanța acestui instrument în managementul securității cibernetice. GravityZone oferă o gamă variată de soluții eficiente, precum antimalware, control avansat al amenințărilor, protecție împotriva atacurilor fileless și managementul patch-urilor, toate fiind esențiale pentru o protecție completă a infrastructurii IT.

De asemenea, activarea versiunii trial pentru GravityZone Business Security Enterprise a fost un proces ușor și intuitiv, facilitând accesul la funcționalitățile avansate ale platformei. Această experiență permite evaluarea practică a capabilităților oferite de produs, cum ar fi detecția și răspunsul la incidente, corelarea între endpoint-uri și protecția autonomă, aspecte cruciale pentru întărirea securității organizației.