DOI: https://www.doi.org/10.36719/2706-6185/09/17-20

Günel Zakir Rzayeva
Azərbaycan Texniki Universiteti
magistr
gunel.rza93@gmail.com

SİEM TEXNOLOGİYASININ TƏTBİQİNİN MÜƏSSİSƏLƏRDƏ ƏHƏMİYYƏTİ VƏ ÜSTÜNLÜKLƏRİ

Xülasə

Təhlükəsizlik Məlumatı və Hadisə İdarəetmə (SIEM) sistemləri kiberhücumların qarşısını almaq, aşkar etmək və onlara qarşı reaksiya vermək üçün güclü bir vasitə kimi geniş şəkildə tətbiq edilmişdir. SIEM həlləri yüksək riskli sahələri müəyyən etmək üçün geniş görünürlük təmin edən və hadisələrə cavab vermək üçün xərclərin və vaxtı azaltmağa yönəlmiş təsirlərin azaldılması strategiyalarına proaktiv şəkildə diqqət yetirən hərtərəfli sistemlərə çevrilmişdir. Hazırda SIEM sistemləri və əlaqəli həllər yavaş-yavaş böyük verilənlərin analitik alətləri ilə birləşir. Biz ən çox istifadə edilən SIEM-ləri kritik funksionallığı ilə bağlı araşdırırıq və orta və uzunmüddətli perspektivdə SIEM mənzərəsinə təsir edən xarici amillərin təhlilini təqdim edirik. SIEM-lərin növbəti nəsli üçün potensial təkmilləşdirmələrin siyahısı mövcud həllərin nəzərdən keçirilməsi, eləcə də kritik infrastrukturlarda onların faydaları və istifadəsi üzrə təhlilin bir hissəsi kimi təqdim olunur.

***Açar sözlər**: təhlükəsizlik, məlumat, konsolidasiya, korrelyasiya, süni intellekt.*

Gunel Zakir Rzayeva

IMPORTANCE AND ADVANTAGES OF SIEM TECHNOLOGY APPLICATION IN ENTERPRISES

Abstract

Security Information and Event Management (SIEM) systems have been widely deployed as a powerful tool to prevent, detect, and react against cyber-attacks. SIEM solutions have evolved to become comprehensive systems that provide a wide visibility to identify areas of high risks and proactively focus on mitigation strategies aiming at reducing costs and time for incident response. Currently, SIEM systems and related solutions are slowly converging with big data analytics tools. We survey the most widely used SIEMs regarding their critical functionality and provide an analysis of external factors affecting the SIEM landscape in mid and long-term. A list of potential enhancements for the next generation of SIEMs is provided as part of the review of existing solutions as well as an analysis on their benefits and usage in critical infrastructures.

***Keywords**: security, information, consolidation, correlation, artificial intelligence*

GİRİŞ

Təhlükəsizlik Məlumatı və Hadisələrin İdarə Edilməsi (SIEM) sistemləri administratorlara təhlükəsizlik siyasətlərini tərtib etməkdə və müxtəlif mənbələrdən hadisələri idarə etməkdə kömək etmək üçün hazırlanmışdır. Ümumiyyətlə, sadə SIEM bir-birindən müstəqil işləyə bilən, lakin hamısı birlikdə işləmədən ayrı bloklardan (məsələn, mənbə cihazı, jurnalların toplanması, təhlilin normallaşdırılması, qayda mühərriki, jurnalın saxlanması, hadisələrin monitorinqi) ibarətdir.

Əsasən, bütün SIEM-lər idarə olunan infrastruktur tərəfindən yaradılan hadisələri toplamaq, saxlamaq və əlaqələndirmək qabiliyyətinə malikdir. Bu əsas imkanlardan başqa, adətən SIEM-lərin bazardakı müxtəlif mövqelərini əks etdirən mövcud sistemlər arasında çoxlu fərqlər var. Bu bölmə SIEM həllərinin təhlili zamanı nəzərə alınmalı olan xüsusiyyətlərin siyahısını təqdim edir. Müxtəlif kommersiya SIEM-ləri ilə təcrübəmizə əsaslanaraq və ədəbiyyatdan kommersiya və açıq mənbəli SIEM-lərin istifadəsi ilə bağlı müəyyən edilmiş məlumatları əks etdirərək, hər bir SIEM xüsusiyyətini

aşağı/əsas, orta və ya yüksək/qabaqcıl kimi qiymətləndirir. Bu qiymətləndirməyə yalnız seçilmiş SIEM həllərinin əsas konfiqurasiyası daxildir, təhlildə heç bir əlavə xüsusiyyət nəzərə alınmır.

Korrelyasiya qaydaları: SIEM tərəfindən hadisənin aşkarlanmasının müvəffəqiyyəti korrelyasiya qaydalarının gücündən asılıdır. Əksər SIEM-lərin əsas korrelyasiya qaydalarına malik olmasına baxmayaraq, onlardan bir neçəsi güclü axtarış imkanlarına malikdir və SIEM məlumatlarında istifadə oluna bilən mürəkkəb axtarışları yazmaq üçün axtarış emal dillərini dəstəkləyir.

Məlumat mənbələri: SIEM sisteminin əsas xüsusiyyətlərindən biri idarə olunan infrastrukturda çoxsaylı və müxtəlif məlumat mənbələrindən hadisələri toplamaq qabiliyyətidir. Əksər SIEM-lər həm dəstəklənən sensorlar, həm də dəstəklənən məlumat növləri (məsələn, təhlükə kəşfiyyatı) daxil olmaqla bir neçə növ məlumat mənbəyini yerli olaraq dəstəkləyir. Digər həllər üçün (məsələn, QRadar, USM) belə bir xüsusiyyət SIEM-ə inteqrasiya olunmuş əlavə komponentlər tərəfindən dəstəklənə bilər. Bu xüsusiyyət yerli olaraq dəstəklənən məlumat mənbələrini və SIEM-in onları avtomatik olaraq fərdiləşdirmək imkanlarını qiymətləndirir.

Real vaxtda emal: Bu xüsusiyyət SIEM-in daimi dəyişiklik altında real vaxt məlumatlarını idarə etmək qabiliyyətini nəzərə alır. O, kibertəhlükəsizlik insidentlərinin qarşısını almaq və ya onlara reaksiya vermək üçün alət tərəfindən tətbiq edilən real vaxt rejimində nəzarət, monitorinq və boru kəməri imkanlarını, həmçinin SIEM-lərin real vaxtda milyonlarla hadisəni təhlil etməli olduğu performans hesablama imkanlarını qiymətləndirir. Bütün tədqiq edilmiş SIEM-lər təkmil real vaxt emal imkanlarına malikdir.

Məlumat həcmi: Müxtəlif mənbələrdən gələn böyük həcmli məlumatların təhlili toplanmış hadisələrdən daha çox məlumat əldə etmək və daha yaxşı monitorinq üçün vacibdir. Bununla belə, böyük həcmdə toplanmış məlumatı canlı SIEM sistemində saxlamaq çox vaxt baha başa gəlir və praktiki deyil. Bu xüsusiyyət cari sistemlərin korrelyasiya, indeksləşdirmə və saxlama əməliyyatları üçün böyük həcmdə verilənləri dəstəkləmək imkanlarını qiymətləndirir.

SIEM sistemləri son istifadəçi cihazlarından, serverlərdən və şəbəkə avadanlığından, həmçinin təhlükəsizlik divarları, antivirus və ya müdaxilənin qarşısının alınması sistemləri (IPS) kimi xüsusi təhlükəsizlik avadanlığından təhlükəsizliklə bağlı hadisələri toplamaq üçün iyerarxik şəkildə çoxsaylı kolleksiya agentlərini yerləşdirməklə işləyir. Kollektorlar hadisələri mərkəzləşdirilmiş idarəetmə konsoluna yönləndirirlər, burada təhlükəsizlik analitikləri səs-küyü süzür, nöqtələri birləşdirir və təhlükəsizlik insidentlərini prioritetləşdirir.

Bəzi sistemlərdə əvvəlcədən emal kənar kollektorlarda baş verə bilər, yalnız müəyyən hadisələr mərkəzləşdirilmiş idarəetmə qovşağına ötürülür. Bu yolla ötürülən və saxlanılan məlumatların həcmi azaldıla bilər. Maşın öyrənməsindəki irəliləyişlər sistemlərə anomaliyaları daha dəqiq qeyd etməyə kömək etsə də, analitiklər hələ də sistemə ətraf mühit haqqında məlumat verərək rəy bildirməlidirlər.

SIEM alətləri şirkətin infrastrukturu boyunca host sistemləri, tətbiqləri və təhlükəsizlik cihazları, məsələn, antivirus filtrləri və təhlükəsizlik duvarları tərəfindən yaradılmış hadisə və jurnal məlumatlarını toplamaq və bu məlumatları mərkəzləşdirilmiş platformada bir araya gətirməklə işləyir. SIEM alətləri məlumatları uğurlu və uğursuz girişlər, zərərli proqram fəaliyyəti və digər ehtimal olunan zərərli fəaliyyət kimi kateqoriyalara ayırır və çeşidləyir.

SIEM proqramı potensial təhlükəsizlik problemlərini müəyyən etdikdə təhlükəsizlik xəbərdarlıqları yaradır. Əvvəlcədən müəyyən edilmiş qaydalar toplusundan istifadə edərək, təşkilatlar bu xəbərdarlıqları aşağı və ya yüksək prioritet kimi təyin edə bilərlər.

Məsələn, 25 dəqiqə ərzində 25 uğursuz giriş cəhdi yaradan istifadəçi hesabı şübhəli kimi qeyd oluna bilər, lakin yenə də aşağı prioritet olaraq təyin edilə bilər, çünki giriş cəhdləri, ehtimal ki, giriş məlumatını unutmuş istifadəçi tərəfindən edilib.

Bununla belə, beş dəqiqə ərzində 130 uğursuz giriş cəhdi yaradan istifadəçi hesabı yüksək prioritet hadisə kimi qeyd olunacaq, çünki bu, çox güman ki, davam edən kobud güc hücumudur.

SIEM vacibdir, çünki o, böyük miqdarda təhlükəsizlik məlumatlarını süzgəcdən keçirərək və proqram təminatının yaratdığı təhlükəsizlik xəbərdarlıqlarına üstünlük verməklə müəssisələrin təhlükəsizliyi idarə etməsini asanlaşdırır.

SIEM proqramı təşkilatlara başqa cür aşkarlana bilməyən hadisələri aşkar etməyə imkan verir. Proqram təminatı zərərli fəaliyyət əlamətlərini müəyyən etmək üçün jurnal qeydlərini təhlil edir. Bundan əlavə, sistem şəbəkə üzrə müxtəlif mənbələrdən hadisələri topladığı üçün hücumun vaxt cədvəlini yenidən yarada bilər, bu da şirkətə hücumun xarakterini və onun biznesə təsirini müəyyən etməyə imkan verir.

SIEM sistemi həm də bu mənbələr arasında daxil edilmiş bütün təhlükəsizlik hadisələrini özündə əks etdirən hesabatları avtomatik yaratmaqla təşkilata uyğunluq tələblərinə cavab verməyə kömək edə bilər. SIEM proqramı olmadan şirkət jurnal məlumatlarını toplamalı və hesabatları əl ilə tərtib etməli olacaqdı.

Bir təşkilatın sistemləri izləmək və şübhəli fəaliyyətləri bildirmək üçün SIEM həllinə ehtiyac duymasının səbəbi, orta təşkilatın hal-hazırda yaratdığı məlumatların miqdarının əl ilə idarə etmək üçün çox olmasıdır.

Login idarə edilməsi SIEM funksiyalarının əsasını təşkil edir; SIEM sistemini qidalandıran daha çox fərqli mənbələrdən logların növləri nə qədər çox olarsa, o, bir o qədər çox təsirli hesabatlar yaradır. Bu imkan SIEM-ə korrelyasiya qaydalarına qarşı müxtəlif mənbələrdən olan logları çarpaz istinad etməklə müvafiq hadisələri əlaqələndirməyə imkan verir.

Aşağıdakılar təşkilatların SIEM həllinə ehtiyac duymasının əsas üç səbəbidir:

1. Hadisələrin aşkarlanması

SIEM həlli, əks halda diqqətdən kənarda qala biləcək hadisələri aşkar edir. Bu texnologiya zərərli fəaliyyət göstəricilərini aşkar etmək üçün jurnal qeydlərini təhlil edir. Üstəlik, şəbəkə üzrə bütün mənbələrdən hadisələri topladığı üçün sistem onun xarakterini və təsirini müəyyən etmək üçün hücum qrafikini yenidən qura bilər. Platforma təhlükəsizlik nəzarətlərinə tövsiyələr göndərir - məsələn, zərərli məzmunu bloklamaq üçün bir firewall yönləndirmək.

2. Qaydalara uyğunluq

Şirkətlər bu mənbələr arasında daxil edilmiş bütün təhlükəsizlik hadisələrini əks etdirən hesabatlar yaratmaqla uyğunluq tələblərinə cavab vermək üçün SIEM-dən istifadə edirlər. SIEM olmadan təşkilat jurnal məlumatlarını əl ilə əldə etməli və hesabatları tərtib etməlidir.

3. Hadisələrin İdarə Edilməsi

SIEM təhlükəsizlik qrupuna şəbəkə üzrə hücum marşrutunu müəyyən etməyə, təhlükəyə məruz qalmış mənbələri müəyyən etməyə və davam edən hücumları dayandırmaq üçün avtomatlaşdırılmış mexanizmləri təmin etməyə imkan verməklə insidentlərin idarə edilməsini təkmilləşdirir.

SIEM sistemi həmçinin şirkətin təhlükəsizlik komandasına hücumun şəbəkə üzrə keçdiyi marşrutu aşkar etməyə, təhlükəyə məruz qalmış mənbələri müəyyən etməyə və davam edən hücumların qarşısını almaq üçün avtomatlaşdırılmış alətlər təqdim etməyə imkan verməklə insidentlərin idarə edilməsini təkmilləşdirir.

SIEM-in gələcək tendensiyalarına aşağıdakılar daxildir:

Təkmilləşdirilmiş orkestr. Hazırda SIEM şirkətləri yalnız əsas iş axını avtomatlaşdırması ilə təmin edir. Bununla belə, təşkilatlar böyüməyə davam etdikcə, SIEM əlavə imkanlar təklif etməlidir. Məsələn, süni intellekt və maşın öyrənməsinin kommersiyalaşdırılmasının artması səbəbindən SIEM alətləri şirkət daxilindəki müxtəlif departamentləri eyni səviyyədə qoruma təmin etmək üçün daha sürətli orkestrasiya təklif etməli olacaq. Bundan əlavə, təhlükəsizlik protokolları və həmin protokolların icrası daha sürətli, eyni zamanda daha effektiv və daha səmərəli olacaqdır.

İdarə olunan aşkarlama və cavab (MDR) alətləri ilə daha yaxşı əməkdaşlıq. Hack və icazəsiz giriş təhdidləri artmaqda davam etdikcə, təşkilatların təhlükəsizlik təhdidlərini aşkar etmək və təhlil etmək üçün iki səviyyəli yanaşma tətbiq etməsi vacibdir. Şirkətin İT komandası SIEM-i daxili tətbiq edə bilər, idarə olunan xidmət təminatçısı (MSP) isə MDR alətini tətbiq edə bilər.

Təkmilləşdirilmiş bulud idarəetməsi və monitorinqi. SIEM təchizatçıları buluddan istifadə edən təşkilatların təhlükəsizlik ehtiyaclarını daha yaxşı qarşılamaq üçün öz alətlərinin bulud idarəetməsini və monitorinq imkanlarını təkmilləşdirəcək.

SIEM və SOAR tək alətə çevriləcək. SOAR-ın üstünlüklərini əldə etmək üçün ənənəvi SIEM məhsulları axtarın; lakin, SOAR satıcıları, ehtimal ki, məhsullarının imkanlarını genişləndirməklə cavab verəcəklər.

ƏDƏBİYYAT

1. Bryant, B.D.; Saiedian, H. Yeni öldürmə zəncirinə əsaslanan təsnifat modeli ilə SIEM xəbərdarlığı metadata aqreqasiyasının təkmilləşdirilməsi. Hesablama. Təhlükəsiz. 2020, 94.
2. CyberX. IoT və ICS Təhlükəsizliyi üçün NIST Tövsiyələri. İcra Xülasəsi. Ağ kağız.
3. Water ISAC. 15 Su və Tullantı Su Kommunal Xidmətləri üçün Kibertəhlükəsizliyin Əsasları. İstifadə edilə bilən zəifliklər və hücumları azaltmaq üçün ən yaxşı təcrübələr.
4. Miller, D.; Harris, S.; Harper, A.; Van Dayk, S.; Blask, C. Təhlükəsizlik Məlumatı və Hadisələrin İdarə Edilməsi (SIEM) Tətbiqi; Mc Graw Hill: Nyu York, NY, ABŞ, 2010.
5. Granadillo, G.G.; El-Barbori, M.; Debar, H. Təhlükəsizlik Məlumatı və Hadisə İdarəetmə Sistemləri üçün Alert Korrelyasiyasının yeni növləri. Yeni Texnologiyalar, Mobillik və Təhlükəsizlik üzrə 8-ci Beynəlxalq Konfransın materiallarında, NTMS, Larnaka, Kipr, 21-23 noyabr 2016-cı il.
6. Nicolett, M.; Kavanagh, K.M. Təhlükəsizlik Məlumatı və Tədbirlərin İdarə Edilməsi üçün Magic Quadrant, Gartner Texniki Hesabatı.
7. Kavanagh, K.M.; Rochford, O. Sehrli Kvadrant Təhlükəsizlik Məlumatı və Hadisələrin İdarə Edilməsi, Gartner Texniki Hesabatı.
8. Rochford, O.; Kavanagh, K.M.; Bussa, T. Təhlükəsizlik Məlumatı və Hadisələrin İdarə Edilməsi üçün Kritik İmkanlar; Texniki Hesabat; Gartner: Stamford, CT, ABŞ, 2016.
9. DiSIEM; Qalan-Korroto, İ.; Robla, E.; Prieto-Peres, S.; Qonzales-Zarzosa, A.; Bessani, A.; Respicio, J.; Alves, L.; Ferreira, A.; Serckumecka, P.; və b. Turkay: SIEM-lərin Genişləndirilməsinin Dərin Təhlili; DiSIEM Texniki Hesabatı D2.1; DiSIEM Layihəsi: Lissabon, Portuqaliya, 2017.
10. Gartner. 2020-ci illəri formalaşdıracaq 7 makro faktor, RəsmiVebsayt.
11. TechTarget; Axtarış Təhlükəsizliyi. SIEM Strategiyasını, İdarə etməsini və Müəssisədə Müvəffəqiyyəti Necə Müəyyən etməli; Elektron Bələdçi; TechTarget: Newton, MA, ABŞ, 2014.
12. Godfrey, M. net Forensics—Təhlükəsizlik İnformasiya İdarə etmə Həlli, Ağ Kağız.
13. Moore, J. EiQ Networks Bulud Kanalı Tərəfdaşları üçün İdarə olunan SIEM təklifedir.
14. PRWIRE. Tripwire, Tripwire Giriş Mərkəzi ilə Yeni Nəsil Təhlükəsizlik Məlumatı və Hadisələrin İdarə Edilməsi (SIEM) Həllini Təqdim edir.

Rəyçi: dos. Fərid Babayev

Göndərilib: 05.02.2022 Qəbul edilib: 10.03.2022