MECHANISM FOR EARLY DETECTION OF CYBERSECURITY INCIDENTS BASED ON CORRELATION RULES AND LOG ANALYSIS IN SIEM SYSTEMS

Ashurov Laziz Shoymardonovich

"IPS CLOUD" LLC

Abstract

This thesis investigates the improvement of mechanisms for the early detection of cybersecurity incidents in Security Information and Event Management (SIEM) systems based on correlation rules and log analysis. In modern information infrastructures, large volumes of security logs are generated by servers, network devices, web applications, databases, authentication systems, and other information resources, which limits the effectiveness of manually analyzing individual log entries. Therefore, a mechanism is proposed for the centralized collection, normalization, temporal and contextual correlation, and comprehensive analysis of security events obtained from various sources based on correlation rules. Particular attention is paid to identifying logical relationships among events such as anomalies in user authentication, repeated failed login attempts, privilege changes, unusual network activity, and access to critical resources. The proposed mechanism is based on the following stages: log collection → normalization → event correlation → risk assessment → alert generation → incident investigation and escalation. Formulating correlation rules according to event criticality, frequency of occurrence, time intervals, source and target objects, and security context makes it possible to reduce false-positive alerts and prioritize the detection of high-risk events. As a result, the use of SIEM and log analysis tools is shown to enable cybersecurity incidents to be identified not merely as individual signals, but as sequences of interconnected events, thereby improving the speed of incident response.

Keywords

SIEM, log analysis, correlation rules, cybersecurity incident, early incident detection, security monitoring, log data, anomaly, risk assessment, alert, incident detection, information security.

SIEM TIZIMLARIDA KORRELYATSIYA QOIDALARI VA LOG-TAHLIL ASOSIDA KIBERXAVFSIZLIK HODISALARINI ERTA ANIQLASH MEXANIZMI

Ashurov Laziz Shoymardonovich
"IPS CLOUD" MChJ

ANNOTATSIYA

Mazkur tezisda Security Information and Event Management (SIEM) tizimlarida korrelyatsiya qoidalari va log-tahlil asosida kiberxavfsizlik hodisalarini erta aniqlash mexanizmini takomillashtirish masalalari tadqiq etiladi. Zamonaviy axborot infratuzilmalarida serverlar, tarmoq qurilmalari, web-ilovalar, ma’lumotlar bazalari, autentifikatsiya tizimlari va boshqa axborot resurslaridan katta hajmdagi xavfsizlik jurnallari shakllanishi alohida log yozuvlarini qo‘lda tahlil qilish samaradorligini cheklaydi. Shu sababli turli manbalardan olingan xavfsizlik hodisalarini markazlashtirilgan holda yig‘ish, normallashtirish, vaqt va kontekst bo‘yicha bog‘lash hamda korrelyatsiya qoidalari asosida kompleks tahlil qilishga yo‘naltirilgan mexanizm taklif etiladi. Bunda foydalanuvchi autentifikatsiyasidagi anomaliyalar, takroriy muvaffaqiyatsiz kirish urinishlari, imtiyozlarning o‘zgarishi, noodatiy tarmoq faolligi va kritik resurslarga murojaatlar kabi hodisalar o‘rtasidagi mantiqiy bog‘liqliklarni aniqlashga alohida e’tibor qaratiladi. Taklif etilayotgan mexanizm loglarni yig‘ish → normallashtirish → hodisalarni korrelyatsiya qilish → risk darajasini baholash → ogohlantirishni shakllantirish → hodisani tekshirish va eskalatsiya qilish bosqichlariga asoslanadi. Korrelyatsiya qoidalarini hodisaning kritikligi, takrorlanish chastotasi, vaqt oralig‘i, manba va maqsad obyektlari hamda xavfsizlik kontekstiga mos shakllantirish

ortiqcha ogohlantirishlarni kamaytirish va yuqori xavfli hodisalarni ustuvor aniqlash imkonini beradi. Natijada SIEM va log-tahlil vositalaridan foydalanish kiberxavfsizlik hodisalarini alohida signallar darajasida emas, balki o‘zaro bog‘langan hodisalar ketma-ketligi sifatida aniqlash hamda ularga javob berish tezkorligini oshirishga xizmat qilishi asoslanadi.

Kalit so‘zlar: SIEM, log-tahlil, korrelyatsiya qoidalari, kiberxavfsizlik hodisasi, hodisalarni erta aniqlash, xavfsizlik monitoringi, log ma’lumotlari, anomaliya, risk baholash, alert, incident detection, axborot xavfsizligi.

KIRISH

Raqamli infratuzilmaning murakkablashuvi va axborot tizimlari o‘rtasidagi integratsiyaning kuchayishi kiberxavfsizlik hodisalarini o‘z vaqtida aniqlash masalasini yanada dolzarb qilmoqda. Zamonaviy tashkilotlarda serverlar, tarmoq qurilmalari, operatsion tizimlar, ma’lumotlar bazalari, web-ilovalar, autentifikatsiya xizmatlari va axborot xavfsizligi vositalari doimiy ravishda katta hajmdagi log ma’lumotlarini shakllantiradi. Ushbu ma’lumotlarda kiberhujum yoki xavfsizlik hodisasining dastlabki belgilari mavjud bo‘lishi mumkin, biroq ularni alohida-alohida tahlil qilish tahdidning umumiy manzarasini aniqlash uchun yetarli emas.

Mazkur muammoni hal etishda Security Information and Event Management (SIEM) tizimlari muhim o‘rin tutadi. SIEM turli manbalardan xavfsizlikka oid ma’lumotlarni markazlashtirilgan holda yig‘ish, normallashtirish, saqlash, qidirish va tahlil qilish imkonini beradi. Uning muhim funksiyalaridan biri turli vaqtda va turli axborot resurslarida sodir bo‘lgan hodisalar o‘rtasidagi mantiqiy bog‘liqlikni aniqlash orqali potensial kiberxavfsizlik hodisasini shakllantirishdir.

Amaliyotda alohida log yozuvi har doim ham kiberhujumni anglatmaydi. Masalan, foydalanuvchining autentifikatsiyadan bir marta muvaffaqiyatsiz o‘tishi oddiy xatolik bo‘lishi mumkin. Biroq qisqa vaqt oralig‘ida bir IP-manzildan ko‘plab muvaffaqiyatsiz

autentifikatsiya urinishlari qayd etilishi, undan keyin muvaffaqiyatli kirish va kritik resursga murojaat kuzatilishi xavfsizlik nuqtai nazaridan ancha yuqori ahamiyatga ega hodisalar ketma-ketligini shakllantiradi. Shu sababli xavfsizlik monitoringida individual log yozuvlarini emas, balki ularning vaqt, manba, foydalanuvchi, aktiv va hodisa turi bo‘yicha o‘zaro bog‘liqligini tahlil qilish zarur.

SIEM tizimlarida bunday bog‘liqliklarni aniqlashning asosiy vositalaridan biri korrelyatsiya qoidalari hisoblanadi. Korrelyatsiya qoidalari bir yoki bir nechta axborot manbalaridan kelib tushgan hodisalarni belgilangan mantiqiy shartlar, vaqt intervallari, takrorlanish chastotasi va xavfsizlik konteksti bo‘yicha birlashtirish imkonini beradi. Natijada alohida holatda past xavfli ko‘ringan signallar o‘zaro bog‘langanda yuqori riskli xavfsizlik hodisasi sifatida aniqlanishi mumkin.

Biroq korrelyatsiya qoidalarining haddan tashqari umumiy shakllantirilishi ko‘p sonli false positive ogohlantirishlarni yuzaga keltiradi. Aksincha, juda qat’iy shartlar bilan tuzilgan qoidalar ayrim real hujumlarni aniqlamay qolishi, ya’ni false negative holatlariga sabab bo‘lishi mumkin. Ko‘p sonli asossiz ogohlantirishlar esa xavfsizlik operatsiyalari markazi (Security Operations Center — SOC) mutaxassislarining ish yukini oshirib, kritik hodisalarga javob berish tezligiga salbiy ta’sir ko‘rsatadi.

Shu jihatdan korrelyatsiya qoidalarini log-tahlil natijalari, hodisalarning kritikligi, vaqt oralig‘i, takrorlanish chastotasi, foydalanuvchi xatti-harakati va himoyalanayotgan aktivning qiymatini hisobga olgan holda shakllantirish muhim ahamiyatga ega. Bunda SIEM tizimi oddiy loglarni saqlash va ogohlantirish generatsiya qilish vositasidan hodisalarni kontekstual tahlil qiluvchi va ustuvorlashtiruvchi xavfsizlik monitoringi mexanizmiga aylanishi mumkin.

Taklif etilayotgan yondashuvda jarayon quyidagi mantiqiy sikl asosida tashkil etiladi:

LOG MA’LUMOTLARINI YIG‘ISH → NORMALLASHTIRISH → HODISALARNI BOG‘LASH → KORRELYATSIYA QOIDALARINI

QO‘LLASH → RISKNI BAHOLASH → ALERT SHAKLLANTIRISH → HODISANI TEKSHIRISH → JAVOB CHORASINI BELGILASH.

Mazkur mexanizmning asosiy vazifasi barcha log yozuvlarini bir xil darajada qayta ishlash emas, balki o‘zaro bog‘liq xavfsizlik signallaridan real kiberxavfsizlik hodisasini imkon qadar erta ajratib olishdan iborat.

Tadqiqotning maqsadi — SIEM tizimlarida korrelyatsiya qoidalari va log-tahlil asosida kiberxavfsizlik hodisalarini erta aniqlash mexanizmini shakllantirish, hodisalarni risk darajasiga ko‘ra ustuvorlashtirish hamda false positive ogohlantirishlarni kamaytirishga qaratilgan yondashuvlarni asoslashdan iborat.

TADQIQOT METODLARI

Mazkur tadqiqotda SIEM tizimlarida turli axborot manbalaridan shakllanadigan log ma’lumotlarini korrelyatsion tahlil qilish orqali kiberxavfsizlik hodisalarini erta aniqlash mexanizmi ishlab chiqildi. Tadqiqotning metodologik asosini tizimli tahlil, log ma’lumotlarini normallashtirish, hodisalarni vaqt va kontekst bo‘yicha korrelyatsiya qilish, riskga asoslangan baholash hamda xavfsizlik ogohlantirishlarini ustuvorlashtirish usullari tashkil etdi.

Tahlil qilinadigan ma’lumotlar manbalari sifatida server va operatsion tizim loglari, tarmoq qurilmalari, firewall va IDS/IPS vositalari, web-serverlar, ma’lumotlar bazalari, autentifikatsiya xizmatlari hamda endpoint xavfsizlik tizimlaridan olinadigan hodisalar nazarda tutildi. Turli manbalarda loglarning formatlari bir-biridan farq qilishi sababli ularni yagona tahlil muhitiga keltirish uchun normallashtirish bosqichi modelning asosiy komponentlaridan biri sifatida belgilandi.

Taklif etilayotgan mexanizm quyidagi bosqichlar asosida ishlaydi:

LOG MANBALARI → MA’LUMOTLARNI YIG‘ISH → PARSING VA NORMALLASHTIRISH → HODISALARNI KORRELYATSIYA QILISH →

RISKNI BAHOLASH → ALERTNI USTUVORLASHTIRISH → INCIDENTNI TEKSHIRISH.

Loglarni normallashtirish jarayonida har bir hodisa uchun vaqt belgisi, manba va maqsad IP-manzili, foydalanuvchi identifikatori, hodisa turi, port, protokol, amal natijasi va kritikligi kabi atributlarning yagona strukturada shakllantirilishi nazarda tutiladi. Bu turli xavfsizlik vositalaridan kelgan hodisalarni o‘zaro solishtirish imkonini beradi.

Korrelyatsiya mexanizmini shakllantirishda hodisalar o‘rtasidagi bog‘liqlik to‘rtta asosiy mezon asosida tahlil qilinadi: vaqt, subyekt, obyekt va hodisalar ketma-ketligi. Masalan, bir foydalanuvchi hisobiga qisqa vaqt davomida ko‘plab muvaffaqiyatsiz kirish urinishlari, keyinchalik muvaffaqiyatli autentifikatsiya va undan so‘ng yuqori imtiyozli resursga murojaat qayd etilishi o‘zaro bog‘liq hodisalar sifatida baholanadi.

Korrelyatsiya qoidasining umumiy mantiqiy ko‘rinishi quyidagicha ifodalanishi mumkin:

$$\mathbf{CR = (E_1 \wedge E_2 \wedge ... \wedge E_n) \mid \Delta t \leq T}$$

bunda CR — korrelyatsiya qoidasi; $E_1...E_n$ — o‘zaro bog‘lanadigan xavfsizlik hodisalari; Δt — hodisalar orasidagi vaqt oralig‘i; T — qoida uchun belgilangan maksimal vaqt chegarasidir.

Korrelyatsiya natijasida aniqlangan hodisalarni ustuvorlashtirish uchun risk ko‘rsatkichidan foydalanish taklif etiladi. Uning soddalashtirilgan modeli quyidagicha ifodalanadi:

$$\mathbf{R = w_1S + w_2F + w_3A + w_4C}$$

bunda R — hodisaning integral risk ko‘rsatkichi; S — hodisaning xavflilik darajasi (severity); F — hodisaning takrorlanish chastotasi (frequency); A — ta’sir ko‘rsatilayotgan axborot aktivining kritikligi (asset criticality); C — hodisaning

kontekstual xavflilik darajasi (context); w_1–w_4 esa tegishli ko‘rsatkichlarning vazn koeffitsiyentlaridir.

1-jadval. SIEM korrelyatsiya mexanizmida foydalaniladigan asosiy mezonlar

Mezon	**Tahlil qilinadigan ko‘rsatkich**	**Korrelyatsiyadagi vazifasi**
Vaqt	Hodisalar oralig‘i, takrorlanish chastotasi	Bog‘liq hodisalarni vaqt oynasida aniqlash
Subyekt	User ID, IP-manzil, qurilma	Bir manbaga tegishli faollikni bog‘lash
Obyekt	Server, endpoint, ma’lumotlar bazasi	Hujum yo‘naltirilgan aktivni aniqlash
Hodisa turi	Login failure, privilege change, network event	Hujum ketma-ketligini shakllantirish
Kritik daraja	Severity va aktiv qiymati	Alert ustuvorligini belgilash
Kontekst	Oldingi hodisalar va foydalanuvchi xatti-harakati	Hodisaning real xavfliligini aniqlashtirish

Taklif etilayotgan mexanizmda risk darajasiga qarab alertlar past, o‘rta, yuqori va kritik toifalarga ajratiladi. Past darajadagi hodisalar loglash va monitoring rejimida saqlanishi, o‘rta darajadagi hodisalar qo‘shimcha tekshiruvga yuborilishi, yuqori va kritik darajadagi hodisalar esa SOC mutaxassisiga ustuvor alert sifatida yetkazilishi ko‘zda tutiladi.

Mexanizm samaradorligini baholashda Detection Rate, False Positive Rate, False Negative Rate, Mean Time to Detect (MTTD) va alertlarning umumiy soniga nisbatan haqiqiy xavfsizlik hodisalari ulushi kabi ko‘rsatkichlardan foydalanish maqsadga muvofiq. Bunda maqsad alertlar sonini shunchaki ko‘paytirish emas, balki xavfsizlik

mutaxassisiga yetkazilayotgan signallarning aniqligi va amaliy qiymatini oshirishdan iborat.

Shu tariqa, taklif etilayotgan metodika alohida log yozuvlarini tahlil qilishdan “log → bog‘langan hodisalar → korrelyatsiya → risk → ustuvor alert → incident” tamoyiliga o‘tishni nazarda tutadi. Bu SIEM tizimida katta hajmdagi log ma’lumotlari orasidan xavfli hodisalar ketma-ketligini erta ajratish va kiberxavfsizlik hodisalariga javob berish vaqtini qisqartirish uchun metodik asos yaratadi.

NATIJALAR VA MUHOKAMA

Tadqiqot doirasida taklif etilgan mexanizm SIEM tizimida shakllanadigan katta hajmdagi log ma’lumotlarini alohida hodisalar sifatida emas, balki vaqt, foydalanuvchi, tarmoq manzili, axborot aktivi va hodisalar ketma-ketligi bo‘yicha o‘zaro bog‘langan xavfsizlik signallari sifatida tahlil qilishga asoslanadi. Bunday yondashuv bir qarashda past xavfli bo‘lgan bir nechta hodisaning yagona kiberxavfsizlik incidentiga tegishli ekanligini aniqlash imkonini beradi.

Korrelyatsiya mexanizmining muhim jihati turli axborot manbalaridan kelgan log yozuvlarini yagona xavfsizlik kontekstida birlashtirishdir. Masalan, autentifikatsiya tizimida qisqa vaqt davomida ketma-ket muvaffaqiyatsiz kirish urinishlari, keyinchalik muvaffaqiyatli autentifikatsiya, yangi yoki noodatiy IP-manzildan ulanish hamda undan so‘ng foydalanuvchi imtiyozlarining o‘zgartirilishi alohida kuzatilganda turli darajadagi hodisalar sifatida baholanishi mumkin. Ularning vaqt va subyekt bo‘yicha korrelyatsiyasi esa potensial hisob yozuvining kompрometatsiyasini ko‘rsatuvchi yuqori ustuvorlikdagi alertni shakllantirish uchun asos bo‘ladi.

Taklif etilgan mexanizmda korrelyatsiya qoidalari faqat hodisaning mavjudligini emas, balki uning takrorlanish chastotasi, vaqt oralig‘i, manba va maqsad obyektlari, aktivning kritikligi hamda oldingi hodisalar bilan aloqasini ham hisobga oladi. Shu sababli SIEM

tizimida hosil bo‘ladigan barcha alertlarni bir xil darajada ko‘rib chiqish o‘rniga, ularni risk ko‘rsatkichlari asosida ustuvorlashtirish imkoniyati yaratiladi.

2-jadval. Korrelyatsiya qoidalarining namunaviy qo‘llanish mexanizmi

Hodisalar kombinatsiyasi	**Korrelyatsiya sharti**	**Potensial tahdid**	**Ustuvorlik**
Ko‘p marotaba login xatosi	Bir foydalanuvchi yoki IP bo‘yicha qisqa vaqt ichida takrorlanish	Brute-force ehtimoli	O‘rta
Login xatosi → muvaffaqiyatli login	Ketma-ket xatolardan so‘ng muvaffaqiyatli kirish	Hisob yozuvi kompрometatsiyasi ehtimoli	Yuqori
Muvaffaqiyatli login → privilege change	Bir sessiya yoki foydalanuvchi doirasida	Imtiyozlarni oshirish ehtimoli	Yuqori
Noodatiy IP → login → kritik resursga kirish	Vaqt va foydalanuvchi bo‘yicha bog‘liqlik	Ruxsatsiz kirish ehtimoli	Yuqori
Login → privilege change → kritik obyektga murojaat	Belgilangan vaqt oynasidagi hodisalar zanjiri	Kompleks hujum ssenariysi	Kritik

Jadvaldagi korrelyatsiya ssenariylari qat’iy universal qoidalar sifatida emas, balki himoyalanayotgan axborot tizimining xususiyatlariga muvofiq sozlanadigan namunaviy mexanizmlar sifatida qaralishi lozim. Masalan, autentifikatsiyadagi muvaffaqiyatsiz urinishlarning chegaraviy qiymati foydalanuvchilar soni, tizim turi, normal trafik xususiyati va tashkilotning xavfsizlik siyosatiga qarab farqlanishi mumkin.

Taklif etilgan yondashuvning muhim natijalaridan biri alertlarni risk darajasiga ko‘ra differensial boshqarish imkoniyatidir. Bunda har bir korrelyatsiya natijasi uchun integral risk ko‘rsatkichi hisoblanadi va unga muvofiq tegishli javob chorasi belgilanadi.

3-jadval. SIEM alertlarini risk darajasi bo‘yicha boshqarish modeli

Risk darajasi	**SIEMdagi holat**	**Tavsiya etiladigan harakat**
Past	Alohida yoki kam ahamiyatli hodisa	Loglash va monitoring
O‘rta	Shubhali hodisalar kombinatsiyasi	Qo‘shimcha avtomatik tahlil
Yuqori	Hujum ehtimoli yuqori bo‘lgan korrelyatsiya	SOC mutaxassisiga alert yuborish va tekshirish
Kritik	Kritik aktivga ta’sir qiluvchi kompleks hodisa	Incident sifatida eskalatsiya qilish va tezkor javob choralarini boshlash

Mazkur tasnif xavfsizlik operatsiyalari markazida alertlar oqimini ustuvorlashtirishga xizmat qiladi. Chunki SIEM samaradorligini faqat generatsiya qilingan alertlar soni bilan baholash metodologik jihatdan yetarli emas. Haddan tashqari ko‘p past ahamiyatli ogohlantirishlar alert fatigue, ya’ni xavfsizlik mutaxassislarining ogohlantirishlar oqimidan ortiqcha yuklanishi holatini yuzaga keltirishi mumkin. Bunday vaziyatda yuqori xavfli hodisaning katta miqdordagi ikkilamchi alertlar orasida e’tibordan chetda qolish ehtimoli ortadi.

Shu sababli korrelyatsiya qoidalarini optimallashtirishda false positive va false negative ko‘rsatkichlari o‘rtasidagi muvozanat alohida ahamiyat kasb etadi. Korrelyatsiya chegaralarining haddan tashqari yumshoq belgilanishi noto‘g‘ri ogohlantirishlarni

ko‘paytirishi, juda qat’iy chegaralar esa real tahdidlarning aniqlanmay qolishiga olib kelishi mumkin. Optimal konfiguratsiya normal faoliyat profili va aniqlangan incidentlar natijalari asosida qoidalarni davriy qayta ko‘rib chiqishni talab etadi.

Mexanizmning ishlash jarayonini quyidagi adaptiv sikl orqali ifodalash mumkin:

LOG → NORMALLASHTIRISH → KORRELYATSIYA → RISKNI BAHOLASH → ALERT → TAHLIL → INCIDENT → QAYTA ALOQA → KORRELYATSIYA QOIDASINI TAKOMILLASHTIRISH.

Qayta aloqa bosqichi mexanizmning muhim elementi hisoblanadi. SOC mutaxassisi tomonidan alert haqiqiy incident yoki false positive sifatida tasniflangandan keyin ushbu natija tegishli korrelyatsiya qoidasini takomillashtirish uchun foydalanilishi mumkin. Natijada SIEM konfiguratsiyasi tashkilotning real xavfsizlik muhiti va normal faoliyat profiliga bosqichma-bosqich moslashtiriladi.

Taklif etilgan mexanizmning samaradorligini amaliy baholashda Detection Rate, False Positive Rate, False Negative Rate va Mean Time to Detect (MTTD) ko‘rsatkichlarini qiyosiy tahlil qilish maqsadga muvofiq. Bunda korrelyatsiya mexanizmi joriy etilishidan oldingi va keyingi holatlarni taqqoslash orqali hodisalarni aniqlash aniqligi hamda tezkorligidagi o‘zgarishlarni baholash mumkin.

Shunday qilib, nazariy tahlil SIEM tizimlarida korrelyatsiya qoidalari va kontekstual log-tahlildan birgalikda foydalanish alohida xavfsizlik signallaridan o‘zaro bog‘langan hodisalar zanjiriga o‘tish imkonini berishini ko‘rsatadi. Biroq mexanizmning real samaradorligi haqida miqdoriy xulosa chiqarish uchun uni nazorat qilinadigan yoki real axborot infratuzilmasida eksperimental sinovdan o‘tkazish, real loglar asosida aniqlash ko‘rsatkichlarini hisoblash va bazaviy SIEM konfiguratsiyasi bilan qiyoslash talab etiladi.

XULOSA

SIEM tizimlarida korrelyatsiya qoidalari va log-tahlil mexanizmlaridan kompleks foydalanish kiberxavfsizlik hodisalarini erta aniqlash samaradorligini oshirishning muhim yo‘nalishlaridan biri hisoblanadi. Axborot infratuzilmasida shakllanadigan katta hajmdagi log ma’lumotlarini alohida qaydlar sifatida tahlil qilish murakkab hujum ssenariylarini o‘z vaqtida aniqlash uchun yetarli emas. Shu sababli turli manbalardan olingan xavfsizlik hodisalarini yagona kontekstda birlashtirish va ular o‘rtasidagi mantiqiy bog‘liqliklarni aniqlash zarur.

Tadqiqot doirasida taklif etilgan mexanizm loglarni yig‘ish, parsing va normallashtirish, hodisalarni korrelyatsiya qilish, risk darajasini baholash, alertlarni ustuvorlashtirish, incidentni tekshirish va qayta aloqa asosida korrelyatsiya qoidalarini takomillashtirish bosqichlaridan tashkil topadi. Mazkur ketma-ketlik SIEM tizimini faqat xavfsizlik hodisalarini qayd etuvchi vosita sifatida emas, balki kiberxavfsizlik incidentlarini aniqlash va ustuvorlashtirishga xizmat qiluvchi analitik mexanizm sifatida qo‘llash imkonini beradi.

Korrelyatsiya qoidalarini shakllantirishda vaqt oralig‘i, foydalanuvchi yoki tarmoq subyekti, himoyalanayotgan obyekt, hodisa turi, takrorlanish chastotasi, aktivning kritikligi va xavfsizlik kontekstini birgalikda hisobga olish muhim ahamiyatga ega. Bunda alohida holatda past xavfli bo‘lgan bir nechta log yozuvlari o‘zaro bog‘langanda yuqori yoki kritik darajadagi kiberxavfsizlik hodisasini ko‘rsatishi mumkin.

Taklif etilgan riskga asoslangan ustuvorlashtirish mexanizmi barcha alertlarni bir xil darajada qayta ishlash o‘rniga ularni past, o‘rta, yuqori va kritik toifalarga ajratishga imkon beradi. Bu SOC mutaxassislarining e’tiborini yuqori xavfli hodisalarga yo‘naltirish, ortiqcha alertlar oqimini boshqarish va potensial incidentlarni imkon qadar erta tekshirish uchun metodik asos yaratadi.

Shuningdek, korrelyatsiya qoidalarini bir marta shakllantiriladigan statik konfiguratsiya sifatida ko‘rib chiqish maqsadga muvofiq emas. Aniqlangan haqiqiy incidentlar, false

positive holatlar va normal foydalanuvchi faolligi haqidagi ma’lumotlar asosida qoidalarni muntazam qayta sozlash talab etiladi. Shu asosda:

LOG → KORRELYATSIYA → RISK → ALERT → TAHLIL → INCIDENT → QAYTA ALOQA → QOIDALARNI OPTIMALLASHTIRISH

ko‘rinishidagi uzluksiz sikl shakllanadi.

Xulosa qilib aytganda, SIEM tizimlarida korrelyatsiya qoidalarini kontekstual log-tahlil va riskga asoslangan ustuvorlashtirish bilan integratsiya qilish kiberxavfsizlik hodisalarini erta aniqlash mexanizmini takomillashtirish uchun istiqbolli yondashuv hisoblanadi. Mexanizmning amaliy samaradorligini asoslash uchun keyingi tadqiqotlarda uni real yoki nazorat qilinadigan log ma’lumotlari asosida eksperimental sinovdan o‘tkazish hamda Detection Rate, False Positive Rate, False Negative Rate va Mean Time to Detect (MTTD) ko‘rsatkichlari bo‘yicha bazaviy SIEM konfiguratsiyasi bilan qiyosiy baholash maqsadga muvofiq.

FOYDALANILGAN ADABIYOTLAR

1. Scarfone K., Mell P. **Guide to Intrusion Detection and Prevention Systems (IDPS).** NIST Special Publication 800-94. — Gaithersburg: National Institute of Standards and Technology, 2007. DOI: 10.6028/NIST.SP.800-94.

2. Kent K., Souppaya M. **Guide to Computer Security Log Management.** NIST Special Publication 800-92. — Gaithersburg: National Institute of Standards and Technology, 2006. DOI: 10.6028/NIST.SP.800-92.

3. National Institute of Standards and Technology. **Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.** NIST Special Publication 800-61 Rev. 3. — Gaithersburg: NIST, 2025.

4. National Institute of Standards and Technology. **Cybersecurity Framework (CSF) 2.0.** — Gaithersburg: NIST, 2024. DOI: 10.6028/NIST.CSWP.29.

5. MITRE. **MITRE ATT&CK®: Enterprise Matrix.** — MITRE Corporation. Kiberhujumchilarning taktika va texnikalarini tasniflash hamda SIEM korrelyatsiya qoidalarini hujum ssenariylari bilan bog‘lash uchun metodologik manba.

6. Cichonski P., Millar T., Grance T., Scarfone K. **Computer Security Incident Handling Guide.** NIST Special Publication 800-61 Rev. 2. — Gaithersburg: NIST, 2012. DOI: 10.6028/NIST.SP.800-61r2.

7. Chuvakin A., Schmidt K., Phillips C. **Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management.** — Waltham: Syngress, 2013.

8. Kent K., Chevalier S., Grance T., Dang H. **Guide to Integrating Forensic Techniques into Incident Response.** NIST Special Publication 800-86. — Gaithersburg: NIST, 2006. DOI: 10.6028/NIST.SP.800-86.

9. National Institute of Standards and Technology. **Security and Privacy Controls for Information Systems and Organizations.** NIST Special Publication 800-53 Rev. 5. — Gaithersburg: NIST, 2020. DOI: 10.6028/NIST.SP.800-53r5.

10. OASIS. **STIX™ Version 2.1.** OASIS Standard. — 2021. Tahdidlar haqidagi ma’lumotlarni standartlashtirilgan shaklda ifodalash va xavfsizlik hodisalari o‘rtasidagi bog‘liqliklarni tavsiflash uchun qo‘llaniladigan standart.