ЛЕКЦИЯ 13
Кибершабуылдарды мониторингтеу, талдау және интеллектуалды әрекет ету архитектуралары

Лекция мақсаты

Қауіпсіздік телеметриясын жинау, нормализациялау, корреляциялау, басымдыққа бөлу және автоматтандырылған әрекет ету архитектурасын түсіндіру; SIEM, SOAR және XDR рөлдерін өзара байланыста қарастыру.

Қауіпсіздік мониторингі

Қауіпсіздік мониторингі — желі, сервер, жұмыс станциясы, қолданба, бұлттық сервис және пайдаланушы әрекеттерінен келетін оқиғаларды үздіксіз бақылау процесі. Мақсат — үлкен оқиға ағынынан қауіпке қатысы бар өзгерістерді уақытында бөліп алу.

Мысал. Бір пайдаланушының сәтсіз кіруі қалыпты қате болуы мүмкін. Бірақ қысқа уақытта көптеген сәтсіз кіру, кейін сәтті кіру және одан соң маңызды файлдарға жаппай қолжетімділік байқалса, оқиғалар тізбегі басқа мағына береді.

Телеметрия және журналдар

Телеметрия — жүйенің күйі мен әрекеттерін сипаттайтын өлшемдер мен оқиғалар. Қауіпсіздік талдауында аутентификация журналы, endpoint оқиғалары, DNS, firewall, прокси, қолданба және бұлттық журналдар маңызды.

Журнал сапасы уақыттың синхрондалуына, субъект пен актив идентификаторларының бірізділігіне, қажетті өрістердің болуына және сақтау мерзіміне тәуелді. Контексті жоқ журнал корреляцияны қиындатады.

SIEM және нормализация

SIEM әртүрлі көздерден оқиғаларды жинап, ортақ форматқа келтіруге, іздеуге, корреляциялауға және ескерту қалыптастыруға арналған. Нормализация әр өнімдегі әртүрлі өрістерді ортақ мағынаға келтіреді.

Мысал. Бір жүйеде пайдаланушы өрісі user_name, екіншісінде account, үшіншісінде principal деп аталуы мүмкін. Нормализациядан кейін олар ортақ субъект ретінде салыстырылады.

Корреляция

Корреляция — жеке оқиғалар арасындағы уақыттық, субъектілік, активтік немесе мінез-құлықтық байланысты анықтау. Бір белгі әлсіз болуы мүмкін, ал бірнеше байланысты белгі қауіптің сенімділігін арттырады.

Корреляция ережелік және интеллектуалды болуы мүмкін. Ережелік тәсіл алдын ала белгілі шарттарды тексереді. Интеллектуалды тәсіл статистикалық ауытқуды немесе модель бағасын қосады. Екі тәсіл де актив маңыздылығы мен бизнес-контекстпен толықтырылуы тиіс.

Оқиғаны басымдыққа бөлу

Барлық alert бірдей маңызды емес. Басымдық анықтауда детектор сенімділігі, активтің құндылығы, ықтимал әсер, шабуыл кезеңі және қосымша растайтын белгілер ескеріледі.

Мысал. Бірдей күмәнді кіру тест серверінде және азаматтардың деректері сақталатын негізгі жүйеде анықталса, техникалық белгі ұқсас болғанымен әрекет ету басымдығы әртүрлі болады.

SOAR және автоматтандырылған әрекет ету

SOAR қауіпсіздік операцияларын оркестрациялауға және қайталанатын әрекеттерді автоматтандыруға көмектеседі. Playbook ескерту түскеннен кейін қандай дерек жиналатынын, қандай тексеру жүргізілетінін және қандай жағдайда автоматты шара қолданылатынын сипаттайды.

Автоматтандыруда қате оң нәтиженің салдары ескеріледі. Төмен тәуекелді әрекеттер автоматты орындалуы мүмкін, ал бизнеске қатты әсер ететін блоктау немесе есептік жазбаны тоқтату үшін қосымша растау қажет болуы ықтимал.

XDR және кешенді контекст

XDR endpoint, желі, идентификация, пошта және басқа телеметрияны байланыстырып, бір оқиғаны бірнеше бақылау қабатынан көруге мүмкіндік береді. Оның мәні тек деректі көбейту емес, бір шабуыл тізбегін ортақ контекстте көрсету.

Мысал. Фишинг хатынан кейін жаңа процесс іске қосылып, одан соң күмәнді DNS сұранысы мен ерекше сыртқы байланыс пайда болса, әр белгі жеке әлсіз болғанымен олардың байланысы маңызды инцидентті көрсетуі мүмкін.

Негізгі жіктеу және салыстыру

Компонент	Негізгі қызметі	Кіріс	Нәтиже
SIEM	Жинау, нормализация, корреляция	Журналдар мен оқиғалар	Alert, контекст
SOAR	Оркестрация және playbook	Alert, контекст	Автоматты/жартылай автоматты әрекет
XDR	Көп доменді байланыстыру	Endpoint, желі, identity және т.б.	Біріккен инцидент көрінісі
Аналитик	Контекстік бағалау	Alert және дәлелдер	Шешім, кері байланыс

Өзара байланыстар схемасы



Сурет 1. Қауіпсіздік мониторингінен әрекет етуге дейінгі цикл

Кешенді практикалық мысал

Ұйымда бір қызметкердің есептік жазбасына бірнеше сәтсіз кіру тіркелді делік. SIEM бұл оқиғаны қабылдайды, бірақ бірден жоғары қауіпті инцидент деп жариялamайды. Біраздан кейін сол есептік жазбамен жаңа құрылғыдан сәтті кіру, маңызды серверге қолжетімділік және әдеттен тыс дерек көлемін оқу байқалады.

Корреляция осы оқиғаларды бір субъект және уақыт аралығы бойынша байланыстырады. Активтің маңыздылығы қосылғаннан кейін басымдық жоғарылайды. SOAR playbook қосымша контекст жинап, сессияны тексеруге жібереді. Қауіп расталса, рұқсат етілген саясат шегінде сессияны тоқтату немесе есептік жазбаны уақытша шектеу сияқты әрекет орындалуы мүмкін.

Қорытынды

Интеллектуалды мониторинг архитектурасының тиімділігі жеке детектордан емес, сапалы телеметрия, нормализация, корреляция, актив контексті, басымдық және бақыланатын әрекет ету тізбегінен қалыптасады. Автоматтандыру шешім қабылдауды жеделдетеді, бірақ оның салдары мен қате оң нәтижелері міндетті түрде ескеріледі.

Бақылау сұрақтары

1. Қауіпсіздік мониторингінің мақсаты қандай?
2. Телеметрия мен журналдың рөлі қандай?
3. Нормализация не үшін қажет?
4. Корреляция қандай байланыстарды анықтайды?
5. SIEM қандай міндеттер атқарады?
6. Alert пен incident айырмашылығы неде?

7. SOAR playbook дегеніміз не?
8. Автоматтандыруда қандай тәуекел ескеріледі?
9. XDR қандай контекст береді?
10. Мониторингтен әрекет етуге дейінгі циклді түсіндіріңіз.

Әдебиеттер тізімі

1. Менщиков А.А., Заколдаев Д.А., Воробьева А.А. Введение в кибербезопасность и киберустойчивость. — СПб.: Университет ИТМО, 2024.
2. Лукьянец С.Е. Гибридные системы кибербезопасности: искусственный интеллект и анализ сетевого трафика. — 2025.