ЛЕКЦИЯ 7
Гибридті интеллектуалды киберқауіпсіздік жүйелері

Лекция мақсаты: Гибридті интеллектуалды киберқауіпсіздік жүйелері тақырыбының негізгі ұғымдарын, процестерін және қолданылатын тәсілдерін кеңінен түсіндіру; олардың ерекшеліктері, артықшылықтары мен шектеулерін салыстыру және практикалық жағдайларда қолданылуын көрсету.

Негізгі ұғым және оның маңызы

Гибридті киберқауіпсіздік жүйесі сигнатуралық, мінез-құлықтық және интеллектуалды талдау әдістерін бір архитектурада біріктіреді. Мұндай тәсілдің мақсаты белгілі шабуылдарды жылдам танумен қатар бұрын нақты сигнатурасы болмаған ауытқуларды да анықтау.

Бұл элементті жеке қарастыру жеткіліксіз. Киберқауіпсіздік жүйесінде оның нәтижесі қорғалатын активтің маңыздылығы, уақыттық контекст, басқа журналдар мен бақылау құралдарының нәтижелері және ұйымның қауіпсіздік саясаты арқылы нақтыланады. Осылайша автоматты белгі соңғы шешім емес, негізделген талдаудың бір бөлігі болып табылады.

Жүйенің немесе процестің құрылымы

Желілік деректерді жинау қабаты трафикті, ағындарды және қауіпсіздік оқиғаларын тіркейді. Жүктелген материалда Wireshark, Tcpdump және Zeek деректер жинау құралдарының мысалы ретінде, Elasticsearch сақтау ортасы ретінде қарастырылады. Деректердің уақыт белгілерінің дұрыстығы кейінгі корреляция үшін маңызды.

Бұл элементті жеке қарастыру жеткіліксіз. Киберқауіпсіздік жүйесінде оның нәтижесі қорғалатын активтің маңыздылығы, уақыттық контекст, басқа журналдар мен бақылау құралдарының нәтижелері және ұйымның қауіпсіздік саясаты арқылы нақтыланады. Осылайша автоматты белгі соңғы шешім емес, негізделген талдаудың бір бөлігі болып табылады.

Негізгі әдістер

Сигнатуралық талдау алдын ала белгілі ережелермен сәйкестікті іздейді. Suricata сияқты IDS/IPS жүйесі белгілі шабуыл үлгілерін анықтауда тиімді. Оның артықшылығы — түсінікті және жылдам шешім; негізгі шектеуі — жаңа немесе өзгертілген шабуыл үшін дайын ереже болмауы.

Бұл элементті жеке қарастыру жеткіліксіз. Киберқауіпсіздік жүйесінде оның нәтижесі қорғалатын активтің маңыздылығы, уақыттық контекст, басқа журналдар мен бақылау құралдарының нәтижелері және ұйымның қауіпсіздік саясаты арқылы нақтыланады. Осылайша автоматты белгі соңғы шешім емес, негізделген талдаудың бір бөлігі болып табылады.

Жұмыс істеу қағидасы

Интеллектуалды талдау машиналық оқыту арқылы қалыпты трафик профилінен ауытқуды іздейді. Жүктелген материалда LSTM уақыттық трафикті талдау компоненті ретінде көрсетілген. AI сигнатуралық детекторды алмастырмайды, оны толықтырады.

Бұл элементті жеке қарастыру жеткіліксіз. Киберқауіпсіздік жүйесінде оның нәтижесі қорғалатын активтің маңыздылығы, уақыттық контекст, басқа журналдар мен бақылау құралдарының нәтижелері және ұйымның қауіпсіздік саясаты арқылы нақтыланады. Осылайша автоматты белгі соңғы шешім емес, негізделген талдаудың бір бөлігі болып табылады.

Талдау және шешім қабылдау

Корреляция кезеңінде сигнатуралық және AI нәтижелері бір актив, уақыт және байланыс контекстінде біріктіріледі. Екі тәуелсіз детектор бір оқиғаға белгі берсе, сенімділік артады. Тек AI белгі берген жағдайда оқиға қосымша тексеріледі.

Бұл элементті жеке қарастыру жеткіліксіз. Киберқауіпсіздік жүйесінде оның нәтижесі қорғалатын активтің маңыздылығы, уақыттық контекст, басқа журналдар мен бақылау құралдарының нәтижелері және ұйымның қауіпсіздік саясаты арқылы нақтыланады. Осылайша автоматты белгі соңғы шешім емес, негізделген талдаудың бір бөлігі болып табылады.

Қарсы әрекет ету

Автоматты әрекет ету белгілі саясат бойынша орындалады. Жүктелген архитектурада firewall API арқылы трафикті шектеу және SIEM арқылы хабарлау идеясы көрсетілген. Жоғары әсерлі әрекеттерде жалған оң нәтиже қаупіне байланысты адам растауы қажет болуы мүмкін.

Бұл элементті жеке қарастыру жеткіліксіз. Киберқауіпсіздік жүйесінде оның нәтижесі қорғалатын активтің маңыздылығы, уақыттық контекст, басқа журналдар мен бақылау құралдарының нәтижелері және ұйымның қауіпсіздік саясаты арқылы нақтыланады. Осылайша автоматты белгі соңғы шешім емес, негізделген талдаудың бір бөлігі болып табылады.

Тәуекелдер мен шектеулер

Ережелер мен модельдер тұрақты жаңартылуы тиіс. Жаңа қауіп туралы деректер сигнатураларды толықтыруға, ал тексерілген жаңа трафик модельді қайта оқытуға пайдаланылады. Жаңа модель міндетті түрде бұрынғы нұсқамен салыстырылып бағаланады.

Бұл элементті жеке қарастыру жеткіліксіз. Киберқауіпсіздік жүйесінде оның нәтижесі қорғалатын активтің маңыздылығы, уақыттық контекст, басқа журналдар мен бақылау құралдарының нәтижелері және ұйымның қауіпсіздік саясаты арқылы нақтыланады. Осылайша автоматты белгі соңғы шешім емес, негізделген талдаудың бір бөлігі болып табылады.

Жіктелуі және салыстырмалы сипаттамасы

Компонент	**Міндеті**	**Артықшылығы**	**Шектеуі**
Сигнатуралық IDS/IPS	Белгілі қауіп	Жылдам, түсінікті	Жаңа қауіпке ереже жоқ
AI/ML	Аномалия	Белгісіз ауытқу	FP/FN
SIEM	Корреляция	Контекст	Баптау қажет
Автоматты әрекет	Шектеу	Жылдам реакция	Қате блоктау

Процестің жалпы схемасы

Трафик → жинау → сигнатуралық талдау + AI талдауы → корреляция → қауіп деңгейі → ескерту/әрекет → кері байланыс

Схеманың түсіндірмесі

Схемада әр кезең алдыңғы кезеңнен алынған ақпаратқа сүйенеді. Бастапқы дерек толық немесе сапалы болмаса, кейінгі талдаудың сенімділігі төмендейді. Сондықтан деректерді жинаудан бастап әрекет етуге дейінгі барлық кезеңде бақылау, валидация және кері байланыс қажет. Кері байланыс жаңа ережелерді енгізуге, модельді қайта бағалауға және қорғаныс архитектурасын жетілдіруге мүмкіндік береді.

Практикалық мысалдар

Мысал 1

Suricata белгілі ережеге сәйкес күмәнді трафикті анықтады, ал ML сол хосттағы байланыс жиілігінің қалыпты профильден ауытқуын көрсетті. Екі белгі бір уақыт пен активте сәйкес келгендіктен, оқиға басымдығы көтеріледі.

Бұл мысалда шешім бір ғана индикаторға сүйенбей қабылданады. Актив, уақыт, пайдаланушы, желілік байланыс және қосымша журналдар салыстырылған кезде жалған қорытынды ықтималдығы төмендейді және әрекет ету басымдығы дұрысырақ анықталады.

Мысал 2

Сигнатура іске қосылмады, бірақ AI сервердің бұрын байланыспаған көптеген мекенжаймен қысқа сессиялар орнатқанын анықтады. Жүйе аналитикке қосымша контекст береді.

Бұл мысалда шешім бір ғана индикаторға сүйенбей қабылданады. Актив, уақыт, пайдаланушы, желілік байланыс және қосымша журналдар салыстырылған кезде жалған қорытынды ықтималдығы төмендейді және әрекет ету басымдығы дұрысырақ анықталады.

Артықшылықтары мен кемшіліктері

Қарастырылған тәсілдердің артықшылығы — қауіпсіздік оқиғаларын жүйелі талдау, үлкен көлемдегі деректерден маңызды белгілерді бөлу, белгілі және белгісіз қауіптерді салыстыру және әрекет ету уақытын қысқарту. Кемшіліктеріне деректердің толық болмауы, жалған оң және жалған теріс нәтижелер, қате конфигурация, ескірген ережелер немесе модельдер, интеграцияның күрделілігі және автоматты әрекеттің заңды бизнес-процеске әсер ету ықтималдығы жатады.

Қорытынды

Гибридті интеллектуалды киберқауіпсіздік жүйелері кибершабуылдарды анықтау және оларға қарсы әрекет етудің кешенді жүйесіндегі маңызды бағыт болып табылады. Нәтиженің сапасы жеке құралмен ғана емес, деректердің сапасымен, бірнеше қорғаныс механизмінің өзара байланысымен, тұрақты мониторингпен және алынған белгілерді контекстпен тексерумен анықталады.

Бақылау сұрақтары

1. Негізгі ұғымға анықтама беріңіз.
2. Қарастырылған процестің негізгі кезеңдерін түсіндіріңіз.
3. Кестеде берілген тәсілдердің айырмашылығы қандай?
4. Негізгі артықшылықтарды атаңыз.
5. Негізгі кемшіліктер мен шектеулер қандай?
6. Қандай деректер талдау үшін маңызды?
7. Интеллектуалды әдістердің рөлі қандай?
8. Автоматтандыру кезінде адам бақылауы не үшін қажет?
9. Практикалық мысалдағы шешім қабылдау логикасын түсіндіріңіз.
10. Бұл тақырып кешенді киберқорғаныспен қалай байланысады?

Әдебиеттер тізімі:

1. Лукьянец С.Е. Гибридные системы кибербезопасности: искусственный интеллект и анализ сетевого трафика для противодействия современным угрозам. — 2025.

2. Менщиков А.А., Заколдаев Д.А., Воробьева А.А. Введение в кибербезопасность и киберустойчивость : учебно-методическое пособие. — Санкт-Петербург: Университет ИТМО, 2024. — 72 с.