СӨЖ №1. Сигнатуралық және аномалиялық анықтау әдістерін салыстыру

Жұмыстың мақсаты

Кибершабуылдарды анықтауда қолданылатын сигнатуралық және аномалиялық әдістердің жұмыс қағидаларын зерттеу, олардың мүмкіндіктері мен шектеулерін бірдей критерийлер бойынша салыстыру және семестрлік жоба үшін анықтау тәсілін негіздеп таңдау.

Пәнмен және жеке семестрлік жобамен байланысы

СӨЖ №1 практикалық жұмыстардағы IDS/IPS, желілік трафик, машиналық оқыту және гибридті анықтау тақырыптарын байланыстырады. Нәтиже семестрлік жобада сигнатуралық, аномалиялық немесе гибридті анықтау тәсілін таңдауға негіз болады.

Қысқаша теориялық мәліметтер

Кибершабуылдарды анықтау жүйелерінің негізгі міндеті – желіде немесе ақпараттық жүйеде қауіпсіздікке әсер етуі мүмкін оқиғаларды уақтылы анықтау. Анықтау тәсілдері көбіне сигнатуралық және аномалиялық болып бөлінеді. Бұл екі тәсілдің кіріс деректері, шешім қабылдау логикасы және қателерінің сипаты әртүрлі болғандықтан, оларды бірдей өлшемдермен салыстыру маңызды.

Сигнатуралық анықтау белгілі шабуылдарға тән алдын ала сипатталған белгілерді іздеуге негізделеді. Ереже белгілі бір хаттама ерекшелігін, сұраныс құрылымын, оқиғалар тізбегін немесе басқа тұрақты белгіні сипаттай алады. Сәйкестік табылған кезде IDS/IPS alert қалыптастырады. Мұндай тәсілдің артықшылығы – белгілі қауіптерді түсіндірілетін логикамен анықтау және ереженің не себепті іске қосылғанын көрсету мүмкіндігі.

Сигнатуралық тәсілдің негізгі шектеуі – бұрын белгісіз немесе ережеде сипатталмаған шабуылдарды анықтау мүмкіндігінің төмендігі. Шабуылдың көрінісі өзгерсе, бұрынғы сигнатура сәйкес келмеуі мүмкін. Сондықтан ережелер базасын жаңарту, олардың сапасын бақылау және жалған іске қосылуларды талдау қажет.

Аномалиялық анықтау белгілі бір шабуылдың дайын сигнатурасын іздеудің орнына қалыпты мінез-құлықтан ауытқуды анықтайды. Қалыпты профиль статистикалық әдістермен немесе ML-модель арқылы қалыптастырылуы мүмкін. Желілік трафикте байланыс ұзақтығы, пакеттер саны, байттар көлемі, хаттама, порттар және уақыттық сипаттамалар сияқты белгілер пайдаланылуы ықтимал.

Аномалиялық әдіс бұрын белгісіз күмәнді белсенділікті анықтауға мүмкіндік береді, бірақ қалыпты әрекеттің өзгеруі False Positive санын арттыруы мүмкін. Модельдің нәтижесі оқыту деректерінің сапасына, класстар теңгеріміне, feature selection және threshold мәніне тәуелді. Сондықтан жоғары метрика автоматты түрде өндірістік тиімділікті білдірмейді.

Салыстыру кезінде Precision, Recall, F1-score, False Positive, False Negative және detection latency бірге қарастырылады. Бұған қоса түсіндірмелілік, есептеу ресурстары, жаңарту қажеттілігі және белгісіз шабуылдарға бейімделу қабілеті бағаланады. Бір ғана accuracy көрсеткіші қауіпсіздік міндетіндегі қателердің нақты сипатын ашпайды.

Практикада екі тәсіл бірін-бірі толықтыра алады. Сигнатуралық компонент белгілі шабуылдарға жоғары сенімді alert берсе, аномалиялық компонент қалыпты профильден ауытқитын жаңа оқиғаларды белгілей алады. Осындай біріктіру гибридті анықтау жүйесінің негізін құрайды және кейінгі практикалық жұмыстардағы Suricata+ML архитектурасымен тікелей байланысты.

Әдістемелік нұсқаулар

Алдымен зерттеу сұрағын нақты тұжырымдап, салыстырылатын екі тәсіл үшін бірдей бағалау критерийлерін белгілеңіз. Пайдаланылатын деректердің немесе жарияланған эксперимент нәтижелерінің шығу тегін, көлемін, класстарын және шектеулерін көрсетіңіз.

Сигнатуралық тәсіл үшін ереже немесе IDS/IPS нәтижелерін, ал аномалиялық тәсіл үшін ML немесе статистикалық модель нәтижелерін талдаңыз. Егер өз экспериментіңіз орындалса, бірдей тестілік деректерді пайдаланыңыз; кодта seed/random_state, split және негізгі параметрлерді тіркеңіз.

Кемінде екі конфигурацияны Precision, Recall, F1-score, FP, FN, latency және түсіндірмелілік бойынша салыстырыңыз. Нәтижені тек санмен бермей, айырмашылықтың себебін, қате көздерін және жалпылау шектеулерін түсіндіріңіз.

Қорытындыда семестрлік жоба үшін сигнатуралық, аномалиялық немесе гибридті тәсілді таңдауды негіздеңіз. Таңдау зерттеу сұрағына және қауіпсіздік талаптарына сүйенуі тиіс.

Орындау тәртібі

1. Сигнатуралық және аномалиялық анықтаудың жұмыс қағидаларын салыстыру.
2. Кемінде 7 салыстыру критерийін негіздеу.
3. Бірдей деректер немесе бірдей эксперименттік шарттар негізінде екі тәсілдің нәтижелерін талдау.
4. False Positive және False Negative жағдайларының операциялық салдарын түсіндіру.
5. Precision, Recall, F1-score және detection latency көрсеткіштерін салыстыру.
6. Белгілі және бұрын белгісіз қауіптерді анықтау мүмкіндігін бағалау.
7. Гибридті қолданудың қажеттілігін негіздеу және қарапайым архитектуралық сызба ұсыну.
8. Семестрлік жоба үшін қолданылатын тәсіл туралы дәлелді қорытынды жасау.

Тапсырмалар

1. Сигнатуралық және аномалиялық анықтаудың жұмыс қағидаларын салыстыру.
2. Кемінде 7 салыстыру критерийін негіздеу.
3. Бірдей деректер немесе бірдей эксперименттік шарттар негізінде екі тәсілдің нәтижелерін талдау.
4. False Positive және False Negative жағдайларының операциялық салдарын түсіндіру.
5. Precision, Recall, F1-score және detection latency көрсеткіштерін салыстыру.
6. Белгілі және бұрын белгісіз қауіптерді анықтау мүмкіндігін бағалау.
7. Гибридті қолданудың қажеттілігін негіздеу және қарапайым архитектуралық сызба ұсыну.
8. Семестрлік жоба үшін қолданылатын тәсіл туралы дәлелді қорытынды жасау.

Орындау мысалы

Мысалы, бір зертханалық PCAP/ағындық деректер жиыны үшін Suricata alert нәтижелері мен ML-модельдің классификация нәтижелері салыстырылады. Бірдей тестілік оқиғаларда TP, FP және FN есептеліп, қай тәсіл белгілі шабуылдарды жақсы анықтайтыны, ал қайсысы жаңа аномалияларға сезімтал екені түсіндіріледі.

Жеке тапсырма

Әр магистрант семестрлік жобасындағы бір қауіп немесе аномалия класын таңдап, сол міндет үшін сигнатуралық және аномалиялық анықтаудың қолданылуын салыстырады. Деректер жиынтығы, қауіп класы немесе салыстырылатын конфигурация басқа магистранттардан ерекшеленуі тиіс.

Нәтижелерді ұсыну формасы

– 5–7 бет аналитикалық есеп
– салыстыру кестесі
– деректер/артефактілер сипаттамасы
– кемінде бір нәтижелер кестесі немесе график

– гибридті архитектура сызбасы
– семестрлік жоба үшін шешімнің негіздемесі

Есепке қойылатын талаптар

Есепте жұмыстың мақсаты, зерттеу сұрағы, пайдаланылған деректердің немесе қауіпсіздік артефактілерінің шығу тегі, талдау әдісі, салыстыру критерийлері, нәтижелер және олардың интерпретациясы берілуі тиіс. Қорытынды әрбір сандық немесе сапалық нәтижемен байланыстырылып, жұмыстың шектеулері көрсетіледі.

Код қолданылған жағдайда random_state немесе seed, split, preprocessing кезеңдері, негізгі параметрлер және бағдарламалық орта тіркеледі. Нәтижені тек кесте немесе метрика түрінде беру жеткіліксіз: магистрант алынған айырмашылықтардың себебін және нәтижені қандай жағдайда жалпылауға болмайтынын түсіндіреді.

Бағалау критерийлері

Критерий	**Үлес салмағы**
Теориялық негіз және терминдерді дұрыс қолдану	15%
Әдіс пен критерийлерді негіздеу	15%
Деректер/артефактілермен жұмыс	20%
Салыстыру және нәтижелерді талдау	20%
Жеке тапсырма және семестрлік жобамен байланыс	20%
Есепті рәсімдеу және дереккөздер	10%

Бақылау сұрақтары

1. Сигнатуралық анықтау қандай қағидаға негізделеді?
2. Аномалиялық анықтаудың негізгі айырмашылығы қандай?
3. Неліктен сигнатуралық әдіс белгісіз шабуылды өткізіп алуы мүмкін?
4. Қалыпты профиль аномалиялық анықтауда қандай рөл атқарады?
5. False Positive және False Negative нені білдіреді?
6. Неліктен accuracy жеткіліксіз?
7. Precision және Recall қандай ақпарат береді?
8. Detection latency не үшін бағаланады?
9. Гибридті анықтаудың мақсаты қандай?
10. Семестрлік жоба үшін тәсілді қандай критерийлермен таңдау керек?

Әдебиеттер тізімі

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

2. Бегаев А.Н., Бегаев С.Н., Федотов В.А. Тестирование на проникновение: учебно-методическое пособие. Санкт-Петербург: Университет ИТМО, 2018. 45 с.

3. Вострецова Е.В. Основы информационной безопасности: учебное пособие для студентов вузов. Екатеринбург: Издательство Уральского университета, 2019. 204 с.

4. Шаньгин В.Ф. Информационная безопасность: учебное пособие. Москва: ДМК Пресс, 2014. 702 с.

5. Назарян А.К., Карцан И.Н. Современные кибератаки: классификация и способы защиты // Информатика. Экономика. Управление. 2025. Т. 4, № 1. С. 1001–1007.

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

7. Сигалов Д.А. Методы выявления поверхности атаки веб-приложений при помощи анализа клиентского JavaScript-кода: диссертация. Москва: МГУ имени М.В. Ломоносова, 2024.