ЛЕКЦИЯ 4
Желілік трафикті мониторингтеу және кибершабуыл белгілерін анықтау

Лекция мақсаты: желілік трафикті мониторингтеу және кибершабуыл белгілерін анықтау бойынша негізгі ұғымдарды, теориялық қағидаларды, салыстырмалы ерекшеліктерді және киберқорғаныста қолданылуын түсіндіру.

Негізгі ұғымдар

PCAP — Желілік пакеттердің толық жазбасы.

NetFlow — Желілік ағын туралы жинақталған метадеректер.

Zeek журналдары — Желілік белсенділікті құрылымдалған оқиғаларға түрлендіретін деректер.

Жүйелік журналдар — Хост пен сервистегі оқиғалар жазбасы.

Салыстырмалы сипаттама

Түрі/тәсілі	Анықтамасы	Ерекшелігі	Артықшылығы	Кемшілігі
PCAP	Желілік пакеттердің толық жазбасы.	Пакет деңгейіндегі егжей-тегжейлі талдау.	Терең талдауға мүмкіндік береді.	Көлемі үлкен, сақтау ресурсын қажет етеді.
NetFlow	Желілік ағын туралы жинақталған метадеректер.	IP, порт, протокол, уақыт, байттар саны.	Ұзақ мерзімді мониторингке ыңғайлы.	Пакет мазмұнын көрсетпейді.
Zeek журналдары	Желілік белсенділікті құрылымдалған оқиғаларға түрлендіретін деректер.	Қосылыстар мен протокол оқиғаларын тіркейді.	Корреляция мен ML үшін ыңғайлы.	Дұрыс баптау және интерпретация қажет.
Жүйелік журналдар	Хост пен сервистегі оқиғалар жазбасы.	Аутентификация, процесс, қате және өзгерістерді көрсетеді.	Желілік контексті хост оқиғаларымен толықтырады.	Көп көлемдегі журналды орталықтандыру қажет.

Жұмыс істеу схемасы

Трафикті жинау → алдын ала өңдеу → белгілерді бөлу → қалыпты профильмен салыстыру → аномалия → ескерту

Теориялық түсіндірме

PCAP

Пакет деңгейіндегі егжей-тегжейлі талдау. Терең талдауға мүмкіндік береді. Сонымен бірге көлемі үлкен, сақтау ресурсын қажет етеді. Сондықтан бұл тәсілді нақты ақпараттық жүйенің архитектурасы, қауіп моделі, деректер сапасы және қолданыстағы қорғаныс механизмдерімен бірге қарастыру қажет.

NetFlow

IP, порт, протокол, уақыт, байттар саны. Ұзақ мерзімді мониторингке ыңғайлы. Сонымен бірге пакет мазмұнын көрсетпейді. Сондықтан бұл тәсілді нақты ақпараттық жүйенің архитектурасы, қауіп моделі, деректер сапасы және қолданыстағы қорғаныс механизмдерімен бірге қарастыру қажет.

Zeek журналдары

Қосылыстар мен протокол оқиғаларын тіркейді. Корреляция мен ML үшін ыңғайлы. Сонымен бірге дұрыс баптау және интерпретация қажет. Сондықтан бұл тәсілді нақты ақпараттық жүйенің архитектурасы, қауіп моделі, деректер сапасы және қолданыстағы қорғаныс механизмдерімен бірге қарастыру қажет.

Жүйелік журналдар

Аутентификация, процесс, қате және өзгерістерді көрсетеді. Желілік контекстті хост оқиғаларымен толықтырады. Сонымен бірге көп көлемдегі журналды орталықтандыру қажет. Сондықтан бұл тәсілді нақты ақпараттық жүйенің архитектурасы, қауіп моделі, деректер сапасы және қолданыстағы қорғаныс механизмдерімен бірге қарастыру қажет.

Қорғаныстық қолдану

Қарастырылған әдістер жеке-жеке емес, көпдеңгейлі киберқорғаныс құрамында тиімді. Деректерді жинау, қалыпқа келтіру, талдау, қауіп деңгейін бағалау және әрекет ету біртұтас процесс ретінде ұйымдастырылады. Интеллектуалды компоненттер үлкен көлемдегі оқиғаларды өңдеуге көмектеседі, ал соңғы шешім тәуекел мен контекстті ескере отырып қабылданады.

Қорытынды

Желілік трафикті мониторингтеу және кибершабуыл белгілерін анықтау кибершабуылдарды анықтау және оларға қарсы әрекет ету жүйесінің маңызды бөлігі болып табылады. Тиімділік бір ғана құралға емес, әдістерді дұрыс біріктіруге, деректер сапасына, тұрақты мониторингке және нәтижелерді тексеруге тәуелді.

Бақылау сұрақтары

1. Негізгі ұғымдарға анықтама беріңіз.
2. Кестеде берілген тәсілдердің негізгі айырмашылықтары қандай?
3. Әр тәсілдің артықшылығы неде?
4. Негізгі кемшіліктері қандай?
5. Қандай деректер талданады?
6. Қандай жағдайда гибридті тәсіл тиімді?
7. Жалған оң және жалған теріс нәтиженің әсері қандай?
8. Интеллектуалды әдістердің рөлі қандай?
9. Қарастырылған схема кезеңдерін түсіндіріңіз.
10. Бұл тәсіл кешенді киберқорғаныспен қалай байланысады?

Список источников

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. Вострецова Е.В. Основы информационной безопасности: учебное пособие. — Екатеринбург: Издательство Уральского университета, 2019. — 204 с. — ISBN 978-5-7996-2677-8.

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