ЛЕКЦИЯ 3
Кибершабуылдарды анықтау және алдын алу жүйелері: IDS/IPS, сигнатуралық және аномалиялық тәсілдер

Лекция мақсаты: кибершабуылдарды анықтау және алдын алу жүйелері: ids/ips, сигнатуралық және аномалиялық тәсілдер бойынша негізгі ұғымдарды, теориялық қағидаларды, салыстырмалы ерекшеліктерді және киберқорғаныста қолданылуын түсіндіру.

Негізгі ұғымдар

IDS — Желі немесе хост оқиғаларын бақылап, күмәнді белсенділікті анықтайтын жүйе.

IPS — Күмәнді белсенділікті анықтап, алдын ала берілген саясат бойынша бұғаттайтын жүйе.

Сигнатуралық әдіс — Белгілі шабуылға тән ереже немесе үлгіні іздеу тәсілі.

Аномалиялық әдіс — Қалыпты мінез-құлықтан ауытқуды анықтау тәсілі.

Салыстырмалы сипаттама

Түрі/тәсілі	Анықтамасы	Ерекшелігі	Артықшылығы	Кемшілігі
IDS	Желі немесе хост оқиғаларын бақылап, күмәнді белсенділікті анықтайтын жүйе.	Шабуылды анықтайды және ескерту береді.	Трафикке тікелей әсер етпей мониторинг жүргізеді.	Өздігінен шабуылды тоқтатпайды.
IPS	Күмәнді белсенділікті анықтап, алдын ала берілген саясат бойынша бұғаттайтын жүйе.	Анықтаумен бірге белсенді қарсы әрекет етеді.	Шабуылды ерте кезеңде шектеуге мүмкіндік береді.	Қате ереже заңды трафикті бұғаттауы мүмкін.
Сигнатуралық әдіс	Белгілі шабуылға тән ереже немесе үлгіні іздеу тәсілі.	Белгілі қауіптерге бағытталған.	Жылдам және нәтижесі түсінікті.	Жаңа шабуылдарды өткізіп алуы мүмкін.
Аномалиялық әдіс	Қалыпты мінез-құлықтан ауытқуды анықтау тәсілі.	Белгісіз ауытқуларды іздейді.	Жаңа шабуылдарды анықтау мүмкіндігі бар.	False Positive саны жоғары болуы мүмкін.

Жұмыс істеу схемасы

Желілік/хосттық деректер → IDS/IPS → сигнатуралық талдау + аномалиялық талдау → ескерту → тексеру → қарсы әрекет

Теориялық түсіндірме

IDS

Шабуылды анықтайды және ескерту береді. Трафикке тікелей әсер етпей мониторинг жүргізеді. Сонымен бірге өздігінен шабуылды тоқтатпайды. Сондықтан бұл тәсілді нақты ақпараттық жүйенің архитектурасы, қауіп моделі, деректер сапасы және қолданыстағы қорғаныс механизмдерімен бірге қарастыру қажет.

IPS

Анықтаумен бірге белсенді қарсы әрекет етеді. Шабуылды ерте кезеңде шектеуге мүмкіндік береді. Сонымен бірге қате ереже заңды трафикті бұғаттауы мүмкін. Сондықтан бұл тәсілді нақты ақпараттық жүйенің архитектурасы, қауіп моделі, деректер сапасы және қолданыстағы қорғаныс механизмдерімен бірге қарастыру қажет.

Сигнатуралық әдіс

Белгілі қауіптерге бағытталған. Жылдам және нәтижесі түсінікті. Сонымен бірге жаңа шабуылдарды өткізіп алуы мүмкін. Сондықтан бұл тәсілді нақты ақпараттық жүйенің архитектурасы, қауіп моделі, деректер сапасы және қолданыстағы қорғаныс механизмдерімен бірге қарастыру қажет.

Аномалиялық әдіс

Белгісіз ауытқуларды іздейді. Жаңа шабуылдарды анықтау мүмкіндігі бар. Сонымен бірге false positive саны жоғары болуы мүмкін. 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

Кибершабуылдарды анықтау және алдын алу жүйелері: IDS/IPS, сигнатуралық және аномалиялық тәсілдер 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.