ЛЕКЦИЯ 15
Интеллектуалды киберқорғаныс жүйелерінің даму бағыттары және кешенді қорғаныс

Лекция мақсаты

Курс бойындағы негізгі ұғымдарды біртұтас интеллектуалды киберқорғаныс архитектурасына біріктіру; гибридті анықтау, Threat Intelligence, MITRE ATT&CK, Zero Trust, түсіндірілетін ЖИ және адам қатысатын автоматтандырудың рөлін талдау.

Интеллектуалды киберқорғаныс ұғымы

Интеллектуалды киберқорғаныс — қауіпсіздік телеметриясын автоматты талдау, аномалия мен белгілі шабуыл белгілерін анықтау, контексті байланыстыру және әрекет ету шешімін қолдау үшін ережелерді, статистикалық әдістерді және машиналық оқытуды біріктіретін тәсіл.

Интеллектуалдылық толық автономдылықты білдірмейді. Жүйе жоғары көлемді деректі өңдеп, басымдық ұсына алады, бірақ маңызды бизнес-әсері бар шешімдерде саясат, түсіндірмелілік және адам бақылауы сақталады.

Гибридті анықтау

Гибридті жүйе сигнатуралық, ережелік, аномалиялық және машиналық оқыту әдістерін бірге қолданады. Белгілі шабуылдар үшін нақты ереже тиімді болуы мүмкін, ал бұрын белгісіз мінез-құлық ауытқуын аномалия моделі байқай алады.

Мысал. Белгілі зиянды доменге сұраныс Threat Intelligence арқылы бірден белгіленеді; ал бұрын кездеспеген доменге түнгі уақытта үлкен көлемді трафик мінез-құлықтық модель арқылы күмәнді деп бағалануы мүмкін.

Threat Intelligence және MITRE ATT&CK

Threat Intelligence — қауіп субъектілері, инфрақұрылым, индикаторлар, тактикалар мен техникалар туралы контекстік ақпарат. Ол ішкі телеметрияны сыртқы қауіп контекстімен байытуға көмектеседі.

MITRE ATT&CK тәрізді білім базалары қарсылас әрекеттерін тактика және техника деңгейінде жүйелеуге мүмкіндік береді. Қорғаныс командасы детекторлардың қандай әрекеттерді қамтитынын картаға түсіріп, бос аймақтарды анықтай алады.

Zero Trust қағидасы

Zero Trust — желінің ішкі бөлігін автоматты түрде сенімді деп қабылдамайтын қауіпсіздік қағидасы. Әр қолжетімділік субъект, құрылғы, ресурс және контекст бойынша тексеріледі; ең аз құқық, сегментация және үздіксіз бақылау қолданылады.

Мысал. Қызметкер корпоративтік желіде отырса да, маңызды деректер қорына қол жеткізу үшін оның идентификациясы, құрылғы күйі және берілген рөлі тексеріледі. Желі ішінде болу өздігінен толық сенім бермейді.

Түсіндірілетін жасанды интеллект

Explainable AI киберқауіпсіздік шешімінде модельдің неге белгілі оқиғаны күмәнді деп бағалағанын түсіндіруге бағытталған. Аналитикке тек «шабуыл» белгісі емес, шешімге ықпал еткен факторлар қажет.

Мысал. Модель пайдаланушы әрекетін аномалия деп белгіледі делік. Түсіндірме шешімге жаңа құрылғы, әдеттен тыс уақыт, сирек ресурс және қалыптан жоғары дерек көлемі әсер еткенін көрсетсе, аналитик тексеруді тезірек жүргізеді.

Адам және автоматтандыру

Human-in-the-loop тәсілінде автоматты жүйе деректі өңдеп, ұсыныс немесе бастапқы әрекет жасайды, ал жоғары тәуекелді шешімге адам қатысады. Бұл әсіресе false positive бизнес-процесті тоқтатуы мүмкін ортада маңызды.

Кері байланыс та қажет: аналитик растаған немесе жоққа шығарған alert-тер ережелерді, threshold мәндерін және модельдерді жетілдіруге пайдаланылады. Осылай қорғаныс жүйесі статикалық емес, үздіксіз жетілдірілетін циклге айналады.

Даму бағыттары

Интеллектуалды киберқорғаныстың дамуында көпмодальды телеметрияны біріктіру, нақты уақыттағы талдау, федеративті және құпиялылықты сақтайтын оқыту, модель дрейфін бақылау, түсіндірілетін шешімдер және қауіпсіз автоматтандыру маңызды бағыттар болып табылады.

Жаңа технологияны енгізгенде тек дәлдікке емес, дерек сапасына, құпиялылыққа, ресурстық шығынға, модельді жаңарту мүмкіндігіне және шабуылшының модельдің өзіне әсер ету тәуекеліне назар аудару қажет.

Негізгі жіктеу және салыстыру

Бағыт	Мақсаты	Негізгі талап
Гибридті анықтау	Әртүрлі детекторларды біріктіру	Корреляция және контекст
Threat Intelligence	Сыртқы қауіп контекстін қосу	Өзектілік және сенімділік
MITRE ATT&CK	Қамтуды жүйелеу	Тактика/техникамен сәйкестендіру
Zero Trust	Автоматты сенімді азайту	Үздіксіз тексеру, ең аз құқық
Explainable AI	Модель шешімін түсіндіру	Аналитикке негіздеме
Human-in-the-loop	Қауіпті автоматтандыруды бақылау	Адам растауы және кері байланыс

Өзара байланыстар схемасы



Сурет 1. Кешенді интеллектуалды киберқорғаныс архитектурасы

Кешенді практикалық мысал

Ұйымның кешенді қорғаныс жүйесінде endpoint, желі, аутентификация, веб-қосымша және бұлт журналдары жиналады. Белгілі индикаторлар ережелермен, мінез-құлық ауытқулары машиналық оқыту модельдерімен анықталады. Threat Intelligence сыртқы контекст қосады, ал ATT&CK оқиғаның ықтимал тактикасы мен техникасын сипаттауға көмектеседі.

Жүйе әр alert-ті автоматты түрде блоктамайды. Активтің маңыздылығы, модель сенімділігі және ықтимал салдар есепке алынып, әрекет ету деңгейі таңдалады. Төмен тәуекелді тексерулер автоматтандырылады, ал маңызды есептік жазбаны тоқтату сияқты әрекеттерге аналитик растауы қажет болуы мүмкін. Аналитиктің шешімі кейін детекторларды жетілдіруге кері байланыс береді.

Кешенді қорғаныстың негізгі қағидасы

Кешенді киберқорғаныс бір технологияға немесе бір интеллектуалды модельге тәуелді болмауы тиіс. Қорғаныс активтерді түгендеуден басталып, шабуыл бетін азайту, қолжетімділікті басқару, телеметрия жинау, анықтау, корреляция, әрекет ету және қалпына келтіру кезеңдерін біріктіреді. Интеллектуалды құралдар осы циклдің бірнеше кезеңінде шешім қабылдауды қолдайды, бірақ базалық кибергигиена мен архитектуралық бақылаулардың орнына жүрмейді.

Мысал. Ұйым өте дәл аномалия детекторын енгізгенімен, жұмыстан кеткен қызметкерлердің есептік жазбаларын жоймаса және сыртқы сервистерін жаңартпаса, жалпы тәуекел жоғары болып қалады. Сондықтан интеллектуалды анықтау алдын алу шараларымен бірге қолданылуы тиіс.

Defense in Depth және интеллектуалды құралдар

Defense in Depth — бір қорғаныс қабаты бұзылған жағдайда келесі қабаттар шабуылдың таралуын шектейтін көпқабатты тәсіл. Периметрлік сүзу, endpoint қорғау, аутентификация, сегментация, қолданба қауіпсіздігі, резервтік көшіру, журналдау және мониторинг бір-бірін толықтырады. Интеллектуалды талдау осы қабаттардан келетін деректерді байланыстырып, жеке әлсіз белгілерден ортақ қауіп контекстін қалыптастырады.

Мысал. Фишинг хат қорғаныс сүзгісінен өтіп кетуі мүмкін. Бірақ пайдаланушы күмәнді файлды ашқаннан кейін endpoint жүйесі жаңа процесті, DNS мониторингі сирек доменді, ал identity жүйесі ерекше кіруді тіркесе, корреляцияланған контекст шабуылды ертерек анықтауға көмектеседі.

Модельдің өзіне бағытталған қауіптер

Жасанды интеллект киберқорғанысқа жаңа мүмкіндік берумен қатар жаңа шабуыл бетін де қалыптастырады. Қарсылас оқыту деректеріне әсер етуге, модельді шатастыратын кіріс қалыптастыруға, модель туралы ақпарат алуға немесе автоматтандырылған шешімді манипуляциялауға тырысуы мүмкін. Сондықтан ML pipeline, деректердің шығу тегі, модель нұсқалары және жаңарту процесі де қорғалатын актив ретінде қарастырылады.

Мысал. Егер аномалия моделі ұзақ уақыт бойы автоматты түрде жиналған, тексерілмеген деректермен қайта оқытылса, шабуылшы белгілі мінез-құлықты біртіндеп «қалыпты» ретінде енгізуге тырысуы ықтимал. Бұған қарсы деректер сапасын бақылау, нұсқалау және қайта оқытуды валидациялау қажет.

Модель дрейфін үздіксіз бақылау

Өндірістік ортада модельді бір рет енгізіп қою жеткіліксіз. Жаңа сервистер, жаңа пайдаланушы топтары, инфрақұрылым өзгерістері және қарсылас тактикасының өзгеруі бастапқы деректер үлестірімін өзгертеді. Модельдің precision, recall, alert көлемі және қате оң нәтижелер динамикасы уақыт бойынша бақылануы тиіс. Белгілі шектен ауытқу қайта калибрлеу немесе қайта оқыту қажеттігін көрсетуі мүмкін.

Автоматтандырылған әрекет етудің деңгейлері

Барлық жауап шарасын бірдей автоматтандыру дұрыс емес. Әрекеттерді тәуекеліне қарай бөлуге болады: ақпарат жинау және контекст байыту толық автоматтандырылуы мүмкін; төмен тәуекелді уақытша шектеу саясат бойынша автоматты орындалуы мүмкін; ал маңызды серверді оқшаулау, қызметкер есептік жазбасын ұзақ мерзімге бұғаттау немесе бизнес-сервисті тоқтату сияқты әрекеттер адам растауын талап етуі мүмкін.

Автоматтандыру деңгейі	**Мысал әрекет**	**Негізгі шарт**
Төмен тәуекел	Қосымша журналдарды жинау, Threat Intelligence тексеру	Бизнес-процеске әсер етпейді
Орташа тәуекел	Сессияны уақытша шектеу, қосымша аутентификация сұрау	Саясат және сенімді контекст қажет
Жоғары тәуекел	Серверді оқшаулау, маңызды аккаунтты бұғаттау	Адам растауы немесе өте жоғары сенімділік
Қалпына келтіру	Қызметті қайта қосу, ережені қайтару	Инцидент күйі мен бақылау нәтижесі тексеріледі

Threat Intelligence сапасын бағалау

Threat Intelligence дерегінің құндылығы оның көлемімен емес, өзектілігімен, сенімділігімен және ұйым контекстіне сәйкестігімен анықталады. Ескі индикаторлар немесе тексерілмеген дерек артық alert туғызуы мүмкін. Сондықтан индикатордың алынған уақыты, дереккөз сенімділігі және ішкі телеметриямен сәйкестігі бағаланады.

MITRE ATT&CK арқылы қорғаныс қамтуын талдау

ATT&CK тактика мен техникаларды ортақ тілде сипаттауға мүмкіндік береді. Ұйым өз детекторларын белгілі техникалармен сәйкестендіріп, қай кезеңдер жақсы бақыланатынын және қай жерде телеметрия немесе детектор жетіспейтінін анықтай алады. Бұл «бізде SIEM бар» деген жалпы тұжырымнан нақтырақ: қандай қарсылас әрекеті қай дереккөз және қай ереже арқылы көрінетіні көрсетіледі.

Zero Trust және үздіксіз контекст

Zero Trust жағдайында қолжетімділік туралы шешім тек логин сәтінде қабылданбайды. Құрылғы күйі, пайдаланушы рөлі, ресурс сезімталдығы, орналасу және мінез-құлық өзгерісі үздіксіз ескерілуі мүмкін. Интеллектуалды модельдер контекстік тәуекел score-ын қалыптастыруға көмектеседі, бірақ соңғы саясат түсінікті және тексерілетін болуы тиіс.

Құпиялылықты сақтайтын интеллектуалды талдау

Киберқауіпсіздік модельдері пайдаланушы әрекеті, желілік байланыс және жүйелік журналдар сияқты сезімтал телеметриямен жұмыс істейді. Сондықтан қажетті деректерді ғана жинау, қолжетімділікті шектеу, сақтау мерзімін белгілеу және мүмкін болғанда деректерді псевдонимдеу маңызды. Федеративті оқыту сияқты тәсілдер кей сценарийде бастапқы деректерді орталыққа толық жинамай модельді жетілдіруге мүмкіндік береді, бірақ олар да қауіпсіздік пен сапа мәселелерін толық жоймайды.

Кибертұрақтылықпен байланысы

Интеллектуалды киберқорғаныстың түпкі мақсаты тек шабуылды табу емес, ұйымның маңызды функцияларын сақтау. Кибертұрақтылық алдын алу, анықтау, әсерді шектеу, қалпына келтіру және алынған сабақ бойынша жүйені жетілдіруді қамтиды. Сондықтан резервтік көшіру, қалпына келтіру жоспары және бизнес үздіксіздігі интеллектуалды детекторлармен бір деңгейде маңызды.

Мысал. Тұрғындарға қызмет көрсететін порталға шабуыл жасалғанда жүйе күмәнді белсенділікті анықтап, зақымдалған компонентті оқшаулауы мүмкін. Бірақ азаматтарға негізгі қызмет көрсету балама арна немесе резервтік инфрақұрылым арқылы жалғасса ғана ұйым кибертұрақты деп бағаланады.

Интеллектуалды киберқорғанысты енгізу кезеңдері

Практикалық енгізу активтер мен тәуекелдерді анықтаудан басталады. Кейін қажетті телеметрия таңдалады, базалық ережелер мен детекторлар құрылады, ML қажет болатын міндеттер бөлінеді, метрикалар мен әрекет ету саясаты анықталады. Пилоттық кезеңде false positive, latency және аналитик жүктемесі өлшенеді. Өндірістік енгізуден кейін модельдер мен playbook-тар тұрақты мониторинг және кері байланыс арқылы жаңартылады.

Қорытынды архитектуралық қағида

Кешенді жүйені келесі байланыс арқылы түсіндіруге болады: Активтер мен тәуекелдер → алдын алу және Zero Trust → телеметрия → ережелік және ML детекторлар → SIEM/XDR корреляциясы → Threat Intelligence және ATT&CK контексті → тәуекелді бағалау → SOAR және аналитик → оқшаулау/қалпына келтіру → кері байланыс. Бұл циклде әр компоненттің нәтижесі келесі компонентке контекст береді, ал кері байланыс бүкіл жүйені жетілдіреді.

Қорытынды

Кешенді интеллектуалды киберқорғаныс бір ғана жасанды интеллект моделінен тұрмайды. Ол активтерді түсіну, сапалы телеметрия, ережелік және ML детекторлар, Threat Intelligence, ATT&CK контексті, Zero Trust қағидалары, бақыланатын автоматтандыру және адам сараптамасын бір циклге біріктіреді. Болашақ жүйелер үшін дәлдікпен қатар түсіндірілетіндік, тұрақтылық, құпиялылық және қауіпсіз автоматтандыру маңызды.

Бақылау сұрақтары

1. Интеллектуалды киберқорғаныс дегеніміз не?
2. Гибридті анықтаудың артықшылығы қандай?
3. Threat Intelligence қандай контекст береді?
4. MITRE ATT&CK не үшін қолданылады?
5. Zero Trust қағидасының мәні неде?
6. Explainable AI аналитикке не береді?
7. Human-in-the-loop қашан қажет?
8. Кері байланыс детекторды қалай жақсартады?
9. Интеллектуалды жүйені енгізуде қандай тәуекелдер ескеріледі?
10. Кешенді киберқорғаныс архитектурасын 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.