UOK 004.048

İmamverdiyev Y.N.[1], Nəbiyev B.R.[2]
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]yadigar@lan.ab.az, [2]babek@iit.ab.az

PRESEDENTLƏR NƏZƏRİYYƏSİ ƏSASINDA ŞƏBƏKƏ TƏHLÜKƏSİZLİYİNİN MONİTORİNQİ ÜZRƏ QƏRARLARIN QƏBULU METODU

Kompüter şəbəkələrinin təhlükəsizliyi sistemlərində hadisələr haqqında sensorlardan daxil olan məlumatların emalından sonra insident kimi təsnif edilmiş hadisələrin sonrakı emalı haqqında qərarların avtomatik qəbul edilməsi mühüm praktiki əhəmiyyət daşıyır. Məqalədə şəbəkə təhlükəsizliyinin monitorinqi sistemlərində presedentlər nəzəriyyəsi əsasında qərarların qəbul edilməsi metodu təklif edilir. Təklif edilmiş yanaşmada insanın iştirakı minimaldır, presedentlərin müxtəlif yaxınlıq ölçülərinin qəbul edilmiş qərarlara təsiri də analiz edilir.

Açar sözləri: *şəbəkə monitorinqi, informasiya təhlükəsizliyi, sensorlar, şəbəkə trafiki analizi, presedentlər nəzəriyyəsi.*

Giriş

Kompüter şəbəkələri müasir cəmiyyətin informasiya infrastrukturunda kritik vacib sistemyaradıcı elementlərdən birinə çevrilmişdir. Kompüter şəbəkələrinin miqyasının böyüməsi, şəbəkədə emal olunan informasiyanın həcminin artması, şəbəkə xidmətlərinin spektrinin genişlənməsi şəbəkədə informasiya təhlükəsizliyi boşluqlarının artmasına səbəb olur. Eyni zamanda şəbəkənin təhlükəsizlik mühitində də dinamik dəyişikliklər baş verir. Belə vəziyyət şəbəkələrin təhlükəsizliyinin təmin edilməsini olduqca çətinləşdirir. Bu səbəbdən şəbəkə təhlükəsizliyinin monitorinqi (ŞTM) sistemi korporativ şəbəkələrin informasiya təhlükəsiliyi infrastrukturunda əvəzolunmaz komponentə çevrilir.

ŞTM kompüter sistemlərində və ya şəbəkədə baş vermiş və ya baş verəcək təhdidlərin aşkarlanmasına, şəbəkədə baş verən anomal hadisələri müəyyən etməyə kömək edən vasitədir. Müasir kompüter şəbəkələri təcrid olunmuş sistemlər deyil, şəbəkələr arasında mürəkkəb qarşılıqlı əlaqələr və qarşılıqlı asılılıqlar mövcuddur. Buna görə bir kompüter şəbəkəsində baş vermiş informasiya təhlükəsizliyi hadisəsinin təsiri kaskad effekti ilə sürətlə digər şəbəkələrə də keçə və bütün informasiya infrastrukturunun işini iflic edə bilər. Buna görə də baş vermiş hadisələrin nəticələrinin aradan qaldırılması üzrə mümkün qədər qısa müddətdə adekvat qərarlar qəbul edilməli və hadisələrə vaxtında reaksiya verilməlidir.

Çox zaman şəbəkə təhlükəsizliyi üzrə idarəetmə qərarları şəbəkə elementlərinin və informasiya təhlükəsizliyi vasitələrinin vəziyyəti haqqında tam məlumatın olmadığı və ya informasiya təhlükəsizliyi hadisələrinin analizi üçün vaxtın məhdudluğu şəraitində qəbul edilir. Hazırda mövcud olan şəbəkə təhlükəsizliyinin monitorinqi vasitələri və sistemlərində qərar qəbul edilməsi tamamilə insan faktorundan asılıdır və bu fəaliyyəti həyata keçirən insandan böyük əmək, təcrübə və bilik tələb edir [1].

İnformasiya təhlükəsizliyinin emalı üzrə qəbul edilmiş qərarlar bir çox halda əvvəllər qazanılmış təcrübəyə və qəbul edilmiş qərarlara əsaslanır, onları yeni situasiya üçün adaptasiya edir. Bunları nəzərə alaraq, insanın iştirakını minimal etmək məqsədi ilə uyğun süni intellekt yanaşmaları seçməklə monitorinq üzrə qərarların qəbul edilməsi prosesinin modelləşdirilməsi məsələsi aktualdır.

Presedentlər nəzəriyyəsi (ing. Case-Based Reasoning, CBR) əvvəllər baş vermiş presedentlər haqqında toplanmış biliklər əsasında qərar qəbul edilməsi metodologiyasıdır [2] və onun şəbəkə təhlükəsizliyi üzrə qərarların qəbul edilməsi prosesinə tətbiqinin məqsədəuyğun olmasını fərz etmək olar. Bu məqalədə presedentlər nəzəriyyəsinin baxılan məsələyə tətbiqinin mümkünlüyü araşdırılır.

Şəbəkə təhlükəsizliyi monitorinqinin funksiyaları

Şəbəkə təhlükəsizliyinin monitorinqi sistemi istifadəçilərin davranışı da daxil olmaqla şəbəkədə baş verən bir sıra prosesləri əvvəlcədən müəyyən edilmiş rejimdə müşahidə etməli, təhlükəsizliyə yaranmış və ya yarana biləcək pozuntuları və təhdidləri fasiləsiz izləməlidir. Bu vəzifələri yerinə yetirmək üçün monitorinq sisteminə aşağıdakı komponentlər daxil olmalıdır [3–10]:

- Proseslər – şəbəkədə baş verən bütün hadisələr nəzərdə tutulur. Bu hadisələrə şəbəkə servisləri, istifadəçi trafikləri, şəbəkə avadanlıqlarının vəziyyəti və s. aiddir.
- Sensorlar – şəbəkədə baş verən bütün hadisələr sensorlar vasitəsilə qeydə alınır (SNMP, SPAN Port, NetFlow və s.) və sonra bu məlumatlar verilənlər bazasına ötürülür.
- Verilənlərin toplanması və analizi – informasiya təhlükəsizliyi hadisələri haqqında sensorlardan alınmış verilənlər vahid bazada toplanır və analiz edilir (verilənlərin konsolidasiyası, normallaşdırılması və süzülməsi, hadisələrin aqreqasiyası, korrelyasiyası və s.).
- Hadisələrin klassifikasiyası – məlumatlar toplandıqdan sonra şübhəli hadisələr müəyyən siniflərə klassifikasiya edilir (təsnifatlandırılır).
- Təhlükələrin qiymətləndirilməsi – təhlükə mənbəyinin aşkarlanması və identifikasiyası yerinə yetirilir. Bundan sonra təhlükənin nə dərəcədə risqli olması qimətləndirilir və ona uyğun emal prioriteti müəyyən edilir. Təhlükənin risq dərəcəsi bu təhlükənin şəbəkəyə və ya ayrı-ayrı istifadəçilərə vura biləcəyi ziyanın miqyasından asılıdır.
- Qərarlara dəstək sistemi – şübhəli hadisələrə reaksiya üsulları haqqında qərar qəbul edilməsi üçün nəzərdə tutulub. Təhlükənin risq dərəcəsinə və miqyasına uyğun olaraq qərar sistem tərəfindən avtomatik və ya əvvəlcədən müəyyən olunmuş ekspertlər tərəfindən qəbul edilir.
- İnformasiyanın ötürülməsi – təhlükənin növü, mənbəyi, risq dərəcəsi və ona uyğun olaraq verilmiş qərar haqqında hesabat tərtib olunur, aidiyyəti şəxslərə və ya proseslərə ötürülür.

Beləliklə, sensorlardan məlumatlar toplandıqdan sonra analiz edilir və aşkarlanmış hadisələr klassifikasiya edilir. Klassifikasiya prosesi aparıldıqdan sonra, şəbəkə təhlükəsizliyinə zərərli təsir edə biləcək hadisələr seçilir və onların təhlükə mənbəyi identifikasiya edilir. Təhlükə identifikasiya olunduqdan və onun mənbəyi aşkarlandıqdan sonra, təhlükənin nə dərəcədə risqli olması qiymətləndirilir. Təhlükə qiymətləndirildikdən sonra qərarlara dəstək sistemi vasitəsi ilə təhlükə və hazır həllər bazası arasında əks-əlaqə yaradılır.

Presedentlər nəzəriyyəsinin əsas müddəaları

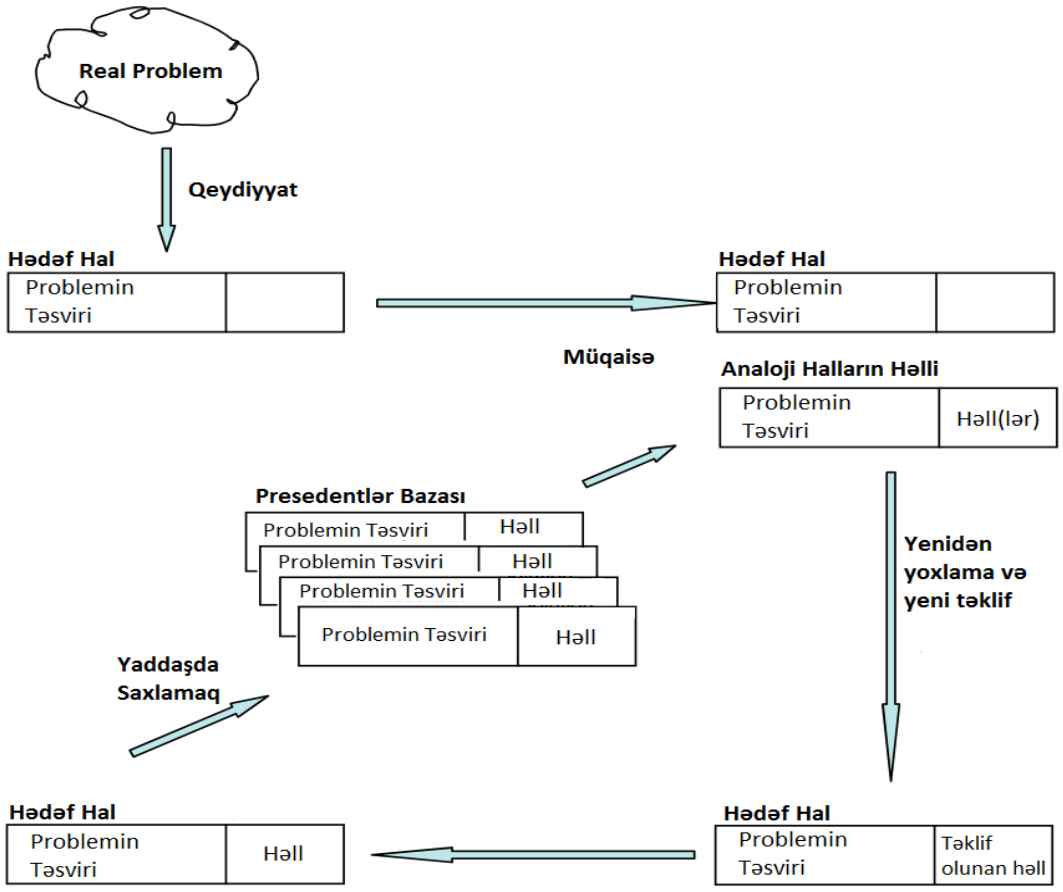
CBR metodologiyasının mahiyyəti aşağıdakından ibarətdir. Faktiki olaraq, presedent <problem, həll metodu> cütüdür. Zaman keçdikcə meydana çıxan situasiyalar və onların həlli yolları xüsusi bazada – presedentlər bazasında saxlanılır. Yeni situasiya yarandıqda presedentlər bazasında oxşar situasiya axtarılıb tapılır və onun həll metodu baxılan situasiyaya adaptasiya olunur. CBR metodologiyası diaqnostika, proqnozlaşdırma, müxtəlif predmet sahələrində planlaşdırma və lahiyələndirmə işlərində və bir çox klassifikasiya məsələlərinin həllində istifadə olunur [2, 11–13]. CBR informasiya təhlükəsziliyinin müxtəlif aspektlərinə – risqlərin qiymətləndirilməsinə [14], müdaxilələrin aşkarlanmasına [15], şəbəkə təhlükəsizliyi vəziyyətinin analizinə də tətbiq edilmişdir [16].

CBR-in metodologiyası 4 prosesdən ibarət tsiklik prosedur şəklində həyata keçirilir [2]:

1. Konkret situasiya üçün oxşar presedentin axtarılması (Retrieve);
2. Presedentin həll metodunun konkret situasiyaya tətbiqi (Reuse);
3. Alınmış həllin yoxlanılması və zəruri olduqda həllin korreksiya (adaptasiya) olunması (Revise);
4. Alınmış həllin sonradan istifadə üçün presedentlər bazasında saxlanılması (Retain).

Çox zaman bu prosesləri 4Re-prosesləri adlandırırlar. Şək. 1-də CBR tsiklinin sxemi göstərilib.

Hazırda presedentlərin seçilməsi üçün çox sayda metodlar işlənmişdir. Oxşarlıq metrikası əsasında seçim daha çox istifadə edilir [11, 12]. Əlamətlər fəzasında cari situasiyaya uyğun olan nöqtə müəyyən edilir və oxşarlıq metrikasından istifadə etməklə ona ən yaxın nöqtə – presedent tapılır. Bir çox sistemdə presedent «xassə-qiymət» cütü şəklində təsvir edilir. Daha mürəkkəb strukturlu presedentlərə də baxılır, belə sistemlərdə struktur oxşarlıq metrikaları istifadə edilir [11].



Şəkil 1. CBR metodologiyasının blok-sxemi

Şəkil 1-də hazır həllər yaddaşı kimi mərkəzdə presedentlər bazası yerləşdirilib. Yeni bir problem baş verdikdə o, əlamətlərin vektor funksiyası ilə bazada qeydiyyatdan keçirilir, bu presedentlər bazasından problemlərin axtarılmasını təmin edir. Aydındır ki, funkiyaların oxşarlıq səviyyəsi nə qədər çoxdursa, presedentlərin axtarış effektivliyi də bir o qədər yüksək olar.

CBR bir çox halda digər suni intellekt sistemlərindən əsaslı fərqlənir. Birinci fərq predmet sahəsi üzrə ümumi biliklər bazasına əsaslanmasıdır; CBR sistemindən istifadə edərək konkret həllər bazasına müraciət etmək daha məqsədəuyğundur. İkinci əsas fərq isə daim artan və dayanıqlı biliklər bazasının olmasıdır, hər bir problem həll edilən kimi təcrübə yaddaşa ötürülür və bu həll yaranacaq növbəti problem üçün dərhal əlyetərli olur.

CBR əsasında monitorinq qərarlarının qəbulu metodu

Qərar dəstək sistemində CBR aparatının istifadəsinin əsas məqsədi, keçmişdə meydana çıxan presedentlərin əsasında mövcud vəziyyətə uyğun hazır həllin verilməsini təmin etməkdir. CBR metodologiyasını şəbəkə təhlükəsizliyinin monitorinqi üzrə qərarların qəbul edilməsinə tətbiq etmək üçün əvvəlcə informasiya təhlükəsizliyi hadisələrini əlamətlər vektoru kimi formal təsvir etmək zəruridir.

İnformasiya təhlükəsizliyi hadisələrinin təsviri üçün bir sıra yanaşmalar təklif edilib [17, 18], hadisələr haqqında müxtəlif mənbələrin generasiya etdikləri verilənlərin vahid formatının müəyyən edilməsi üzrə də cəhdlər mövcuddur [19]. Qeyd edək ki, konkret hadisənin təsviri tətbiq sahəsi ilə müəyyən edilir və bura tətbiq sahəsi üçün maraqlı olan bütün informasiya daxil edilə bilər. Bu işdə *e* informasiya təhlükəsizliyi hadisəsi formal olaraq aşağıdakı kimi təsvir edilir:

$$e = (Etype, DT, ID, rb, sev, v_1, ..., v_n),$$

burada *Etype* – hadisənin tipini təsvir edir, *DT* – hadisənin baş vermə vaxtını və zamanını bildirir, *ID* – hadisənin aşkarlandığı mənbənin identifikatorlarıdır, *rb* – mənbənin etibarlıq dərəcəsidir, *sev* – hadisənin risq dərəcəsidir, v_1, ..., v_n – hadisəni təsvir etmək üçün tətbiq sahəsindən asılı olaraq tələb edilən digər atributlardır (məsələn, IP-ünvan, protokol, port nömrəsi və s.). v_i atributları tək qiymətlər və ya elementlər toplusu kimi qiymətlər ala bilər. Eyni tipli hadisələr eyni atributlar çoxluğuna malik olur.

Baxılan presedentə presedentlər bazasından ən uyğun presedentin seçilməsi problemi CBR-ə əsaslanan sistemlərin ən mühüm hissəsidir. "Yaxın qonşu" üsulu ən geniş yayılmış və tez-tez istifadə olunan yanaşmadır [12]. İstifadəçi məqsədə nail olmaq üçün "yaxın qonşu" üsulu ilə presedentlərin yaxınlıq dərəcəsini ölçür və cari hadisəyə yaxınlıq dərəcəsini müəyyənləşdirir. Hər əlamətin cəki əmsalı təyin olunur ki, bu da onun nisbi əhəmiyyətini müəyyən edir. Bütün parametrlər üzrə presendentə yaxınlıq dərəcəsini hesablamaq üçün aşağıdakı düstürdan istifadə etmək olar:

$$sim(i,k) = \frac{\sum_{j=1}^{n} w_j \cdot sim(e_{ij}, e_{kj})}{\sum_{j=1}^{n} w_j},$$

w_j – *j* əlamətinin çəkisi; *sim* – oxşarlıq metrikası; e_{ij} və e_{kj} – uyğun olaraq cari *i* hadisəsi və *k* presedenti üçün e_j əlamətinin qiymətləridir.

Oxşarlıq metrikasının seçilməsi olduqca vacib məsələdir, çünki oxşar presedentlərin axtarışı bu seçimdən çox asılıdır. Presedentlərin yaxınlıq və ya oxşarlıq metrikası kimi Evklid məsafəsi, Maholonobis məsafəsi, Hemminq məsafəsi, Manhetten məsafəsi və s. istifadə edilir. Hər bir konkret halda metrikanın seçilməsi istifadə edilən informasiyanın fiziki və ya stastistik təbiəti də nəzərə alınmaqla aparılır.

Presedentlər bazasında uyğun presedent tapılmadığı halda qərar əvvəlcədən müəyyən olunmuş ekspertlər tərəfindən qəbul olunur. Qərarlara dəstək sistemi hər iki halda – uyğun presedent tapıldığı və tapılmadığı halda qəbul olunmuş qərarı təhlükəni zərərsizləşdirmək üçün proseslərə və eyni zamanda hesabat formasında aydiyyəti şəxslərə ötürür. Yeni insidentlər və onların həlləri dəqiqləşdirildikdən sonra bu həllər yekun qərar vermək hüququ olan aidiyyəti şəxslər tərəfindən hazır həllər bazasına ötürülür.

Nəticə

Bu məqalədə presedentlər nəzəriyyəsinin kompüter şəbəkələrinin informasiya təhlükəsizliyinin monitorinqi sistemlərində qərarların qəbulu üçün tətbiqinin mümkünlüyü analiz edilmişdir. Modifikasiya edilmiş CBR-tsiklin şəbəkə təhlükəsizliyinin monitorinqi üzrə qərarların qəbulu üçün əsas mərhələləri nəzərdən keçirilmişdir. İnformasiya təhlükəsizliyi hadisələrinin təsviri üçün format və presedentlərin seçilməsi üçün ümumi yanaşma təklif edilmişdir. Gələcək tədqiqatlarda presedentlər bazası ilə işləmək üçün alqoritmlərin və prosedurların işlənməsi, presedentlərin adaptasiyası və verilmiş oxşarlıq metrikası üzrə presedentlərin seçilməsi metodunun işlənməsi nəzərdə tutulur.

Ədəbiyyat

1. Nəbiyev B. Şəbəkə təhlükəsizliyi monitorinqinin sistem və vasitələrinin analizi / II respublika elmi konfransı "Riyaziyyatın tətbiqi məsələləri və yeni informasiya texnologiyaları", Sumqayıt, 27-28 noyabr 2012, s.188–189
2. Aamodt A., Plaza E. Case-Based Reasoning: Foundational Issues, Methodological Variations, and System Approaches // AI Communications, 1994, Vol. 7, No. 1, pp. 39–59.
3. Мельников М.И. Автоматизированная система мониторинга по сетям TCP/IP // Доклад Томский государственный университет систем управления и радиоэлектороники, 2008, № 2(18), с.98–100.
4. Андрианов Г.А., Самуйлов К.Е., Гайдамака Ю.В. Анализ модели трафика ОКС-7 по результатам обработки статистики измерений // Вестник связи, 2007, №11, с. 17–23.
5. Булахов Н.Г. Методы обнаружения компьютерных вирусов и сетевых червей / Научная сессия ТУСУР, Томск : В-Спектр, 2008, с. 39–41.
6. Миков А., Замятина Е., Панов М. Мультиагентная система защиты распределенной имитационной модели с удаленным доступом / Proc. of the 7th International Conference on Information Research and Applications –i.Tech, 2009, pp. 199–204.
7. Артамонов В.А., Лепешкин О.М. Подход к реализации сетевой системы обнаружения аномалий на основе реконструкции модели сетевого трафика // Инфокоммуникационные технологии, 2007, № 3, с. 145–147.
8. Васенин В.А., Афонин С.А., Слепухин А.Ф. К созданию системы сетевого мониторинга / Всероссийская научно-методическая конференция "Телематика'99", СПб.: СПбГУ ИТМО, 1999, с.54–56.
9. LaMacchia B. A., Sebastian L., Matthew L., Rudi M., Price K.T. .NET framework security, Boston : Addison-Wesley, 2002, 816 p.
10. Чугунов А.В. Системы индикаторов и мониторинг развития информационного общества и экономики знаний // Вестник международных организаций: образование, наука, новая экономика, 2006, №7, с.13–30.
11. Mántaras L.R., Bridge D., McSherry D. Case-Based Reasoning: An Overview // AI Communications, 1997, Vol. 10, No. 1, pp. 21–29.
12. Родин Е.А. Схема адаптивной системы фильтрации сообщений на основе метода вывода по прецедентам // Доклады ТУСУРа, 2010, № 2 (22), с.299–303.
13. Sebestyénová J. CBR in agent-based decision support system // International Journal of Computer Science Issues, 2007, pp. 127–138.
14. Kim J., Hwang I. CBR evaluation modeling for security risk analysis in information security system // International Conference Security Technology, 2008, pp. 66–70.
15. Balachandran B., Safavi-Naini R., Pieprzyk J. Case-based reasoning for intrusion detection / Computer Security Applications Conference, 1996, pp. 214–223.
16. Zhu A., Zhang J. A case-based reasoning method for network security situation analysis // Control, Automation and Systems Engineering, 2011, pp. 1–4.
17. AlienValult: AlienVault Unified SIEM, 2010. http://www.alienvault.com/.
18. Debar H., Curry D., Feinstein B. The Intrusion Detection Message Exchange Format (IDMEF). RFC 4765 (Experimental), 2007.
19. ArcSight Inc.: Common event format: Event interoperability standard, 2006. http://www.arcsight.com/collateral/CEFstandards.pdf.

УДК 004.048

Имамвердиев Ядигар Н.[1], Набиев Бабек Р.[2]
Институт Информационных Технологий НАНА, Баку, Азербайджан
[1]yadigar@lan.ab.az, [2]babek@iit.ab.az

Метод принятия решений на основе теории прецедентов для мониторинга сетевой безопасности

Автоматическое принятие решений по обработке событий информационной безопасности в системах безопасности компьютерных сетей имеет важное практическое значение. В статье предложен метод принятия решений на основе теории прецедентов для мониторинга сетевой безопасности. Предлагаемый подход требует минимизирует участие человека, также анализируется влияние различных метрик близости прецедентов на принятые решения.

Ключевые слова: *информационная безопасность, мониторинг безопасности сети, сенсоры, анализ сетевого трафика, теория прецедентов.*

Yadigar N. İmamverdiyev [1], Babek R. Nabiyev [2]
Institute of Information Technology of ANAS, Baku, Azerbaijan
[1]yadigar@lan.ab.az, [2]babek@iit.ab.az

A decision-making method for computer network security monitoring based on case-based reasoning

Automatic decisions on handling of information security events in security systems of computer networks have great practical importance. The paper proposes a decision making method based on case-based reasoning for the computer network security monitoring. The proposed approach requires minimal human intervention, also analyzes the impact on the decisions of different similarity metrics for precedents.

Key words: *information security, network security monitoring, sensor, network traffic analysis, case-based reasoning.*