Ilmiy tadqiqotlar va ularning yechimlari jurnali
Aoka guvohnoma № 323759 ISSN: 3060-4818

WINDOWS REGISTRLARIDAGI ZARARLI O‘ZGARISHLARNI ANIQLASH VA BARTARAF ETISH USULLARI

Baxtiyorov Shaxzod Baxrom o‘g‘li
Muhammad al-Xorazmiy nomidagi Toshkent
axborot texnologiyalari universiteti
Kiberxavfsizlik yo‘nalishi talabasi,
Toshkent, O‘zbekiston
E-mail: shakhzod_bakhtiyorov.it@gmail.com
Olimov Iskandar Salimboyevich
Senior Lecturer, Department of Cryptology
Tashkent University of Information
Technologies named after Muhammad al-Khwarizmi
E-mail: olimoviskandar89@gmail.com
https://doi.org/10.5281/zenodo.24393469

Annotatsiya: Ushbu maqolada Windows registridagi zararli o‘zgarishlarni aniqlash, dalillarni saqlash va tizimning ishonchli holatini tiklash usullari tahlil qilinadi. Registr kalitlari, qiymat turlari, hive fayllari, foydalanuvchi konteksti va 32 hamda 64 bitli ko‘rinishlarning monitoringga ta’siri tushuntiriladi. Avtomatik ishga tushirish, xizmatlar, Winlogon, IFEO, COM va himoya siyosatlari bilan bog‘liq xavflar MITRE ATT&CK tasnifi asosida ko‘rib chiqiladi. Process Monitor, Autoruns, Sysmon, Windows Security jurnali va Microsoft Defender telemetriyasi vazifalari qiyoslanadi. Xavfsiz laboratoriya uchun PowerShell namunalari, hodisalarni bog‘lash tartibi va tiklash qarorlari ishlab chiqiladi. Muallif taklif qilgan balli mezon 16 ta sun’iy ssenariyda dasturiy hisoblash orqali tekshiriladi; 4 ballik chegarada precision va recall 0,75 ni tashkil etadi. Bu natijalar real zararli dasturlarni aniqlash samaradorligini emas, mezonlarning o‘zaro ta’sirini ko‘rsatadi. Asosiy xulosa shuki, registrdagi farqni jarayon, foydalanuvchi, fayl va tasdiqlangan o‘zgarish konteksti bilan birgalikda baholash zarur.
Kalit so‘zlar: Windows registri, zararli o‘zgarish, persistence, Sysmon, Process Monitor, Autoruns, Security 4657, baseline, hodisalarni korrelyatsiya qilish, xavfsiz tiklash.

Аннотация: В статье анализируются методы обнаружения вредоносных изменений реестра Windows, сохранения доказательств и восстановления доверенного состояния системы. Рассматриваются ключи и типы значений, файлы кустов реестра, пользовательский контекст, а также особенности 32- и 64-разрядных представлений. Риски, связанные с автозапуском, службами, Winlogon, IFEO, COM и политиками защиты, систематизированы с использованием MITRE ATT&CK. Сопоставляются возможности Process Monitor, Autoruns, Sysmon, журнала Security и телеметрии Microsoft Defender. Предлагаются безопасный лабораторный протокол, примеры PowerShell, порядок корреляции событий и выбора способа восстановления. Авторская балльная модель проверена программным расчётом на 16 синтетических сценариях; при пороге 4 балла точность положительных прогнозов и полнота равны 0,75. Эти показатели иллюстрируют поведение правил и не являются оценкой обнаружения реальных вредоносных программ.

Обоснована необходимость совместного анализа изменений реестра, процессов, пользователей, файлов и согласованных административных работ.

Ключевые слова: реестр Windows, вредоносные изменения, закрепление, Sysmon, Process Monitor, Autoruns, событие 4657, эталонное состояние, корреляция событий, восстановление.

Abstract: This article examines methods for detecting malicious Windows Registry changes, preserving evidence, and restoring a trusted system state. It explains registry keys, value types, hive files, user context, and the monitoring implications of 32-bit and 64-bit views. Risks involving startup entries, services, Winlogon, IFEO, COM, and security policies are organized using MITRE ATT&CK. The roles of Process Monitor, Autoruns, Sysmon, the Windows Security log, and Microsoft Defender telemetry are compared. A safe laboratory protocol, PowerShell examples, event correlation workflow, and recovery decision process are proposed. An author-defined scoring rule is evaluated computationally on 16 synthetic scenarios; at a threshold of four, both precision and recall are 0.75. These results illustrate rule behavior and do not estimate detection performance against real malware. The analysis shows why registry differences must be assessed together with process, user, file, and approved-change context, and why deleting a suspicious entry alone does not establish successful remediation.

Keywords: Windows Registry, malicious modification, persistence, Sysmon, Process Monitor, Autoruns, Security event 4657, baseline, event correlation, recovery.

KIRISH

Windows registri operatsion tizim va dasturlar foydalanadigan konfiguratsiya ma’lumotlarini saqlovchi iyerarxik bazadir. Dastur ishga tushishi, foydalanuvchi muhiti yoki xizmat sozlamasiga ta’sir qiladigan kichik o‘zgarish ham xavfsizlik hodisasining bir qismi bo‘lishi mumkin. Shuning uchun registrni tekshirishda faqat kalit nomini ko‘rish yetarli emas: o‘zgarishning manbasi, kutilgan vazifasi va oqibati aniqlanishi kerak [1, 14].

Mavzuning dolzarbligi. Zararli dastur o‘z faylini diskda saqlab qolgan taqdirda ham, keyingi kirishda uni ishga tushirish uchun konfiguratsiyaga tayanishi mumkin. Boshqa holatda hujumchi himoya sozlamasini o‘zgartirish yoki mavjud dastur bajarilishini boshqa komponentga yo‘naltirishga urinadi. Shu bilan birga yangilash xizmatlari, tizim administratori va dastur o‘rnatuvchilari ham registrga ko‘p yozadi. Monitoringning asosiy muammosi — zararli va qonuniy harakatlarning ayrim texnik belgilarida o‘xshashlik mavjudligidir [9–14].

Mavjud yondashuvlar tahlili. Microsoft hujjatlari registr tuzilishi, audit shartlari va diagnostika vositalarining texnik imkoniyatlarini belgilaydi. MITRE ATT&CK registrdan foydalanadigan hujum xatti-harakatlarini tasniflaydi. NIST SP 800-61 Rev. 3 esa aniqlash, javob berish va tiklashni tashkilotning umumiy xavflarni boshqarish faoliyati bilan bog‘laydi [1, 17, 20, 32]. Ushbu ishda bu manbalar yagona amaliy ketma-ketlikka birlashtiriladi: holatni bilish, o‘zgarishni qayd etish, sababni tekshirish, nazoratli tiklash va qayta tekshirish.

Ishning maqsadi — Windows registridagi xavfli o‘zgarishlarni aniqlash va bartaraf etishda qo‘llanadigan usullarni texnik jihatdan asoslash, ularning imkoniyatlari hamda cheklovlarini ko‘rsatish va takrorlanadigan xavfsiz tekshiruv tartibini taklif qilish.

Maqsadga erishish uchun quyidagi vazifalar belgilandi:

– registr tuzilishi, ruxsatlar va ko‘rinishlarning kuzatuvga ta’sirini tushuntirish;

– kuzatilishi lozim bo‘lgan asosiy konfiguratsiya nuqtalarini xavf mexanizmlari bilan bog‘lash;
– holat nusxasi va hodisa telemetriyasiga asoslangan aniqlashni qiyoslash;
– zararsiz sinov kalitida bajariladigan laboratoriya protokolini ishlab chiqish;
– balli baholashni sun’iy ssenariylarda hisoblash va xato qarorlarni tahlil qilish;
– dalil saqlash, aniq qiymatni tiklash va qayta zararlanishni tekshirish tartibini belgilash.

Tadqiqot usullari. Ish hujjatlar tahlili, tahdidlarni modellashtirish, usullarni qiyoslash va takrorlanuvchi hisoblash tajribasiga asoslanadi. Amaliy material ikki qismdan iborat: Windows muhitida bajarish uchun berilgan laboratoriya protokoli va ushbu ishni tayyorlashda Python orqali bajarilgan sun’iy ma’lumotlar tajribasi. Windows laboratoriyasining haqiqiy loglari yoki zararli dastur namunalari mazkur tadqiqotning empirik ma’lumotlari sifatida ishlatilmagan.

Ishning amaliy hissasi. Taklif etilgan yondashuv registr o‘zgarishini hodisa sababi bilan bog‘laydi, audit ishlamagan holatni xavfsiz holat bilan adashtirmaslikni talab qiladi va tiklashni alohida tekshiriladigan jarayon sifatida qaraydi. Balli model tayyor antivirus o‘rnini bosmaydi; u turli signallarning qarorga ta’sirini tushuntirish va qoidalarni muhitga moslashtirish uchun xizmat qiladi.

1. WINDOWS REGISTRINING TUZILISHI VA XAVFSIZLIK XUSUSIYATLARI

1.1. Kalit qiymat va ma’lumot tushunchalari

Registr daraxtidagi tugun **kalit** (key), uning ichidagi tugun **quyi kalit** (subkey), nomlangan yozuv esa **qiymat** (value) deb ataladi. Qiymatning nomi, turi va ma’lumoti bir-biridan farqlanadi. Masalan, sinov dasturining Mode nomli REG_SZ qiymati Baseline satrini saqlashi mumkin. Kalit mavjud bo‘lib, unda nomlangan qiymat bo‘lmasligi ham mumkin. Shu sababli «kalit yaratildi» va «qiymat o‘zgartirildi» turli amallardir [1].

Monitoring modeli kamida kalit yo‘li, qiymat nomi, turi va ma’lumotini alohida saqlashi lozim. Bir xil ko‘rinadigan «1» REG_SZ satri yoki REG_DWORD soni bo‘lishi mumkin. Faqat ekrandagi matnni solishtirish tur o‘zgarishini yo‘qotadi. Standart, ya’ni nomi bo‘sh qiymat ham alohida yozuv sifatida qayd etiladi; uni «qiymat mavjud emas» holati bilan birlashtirish noto‘g‘ri.

1.2. Asosiy registr bo‘limlari

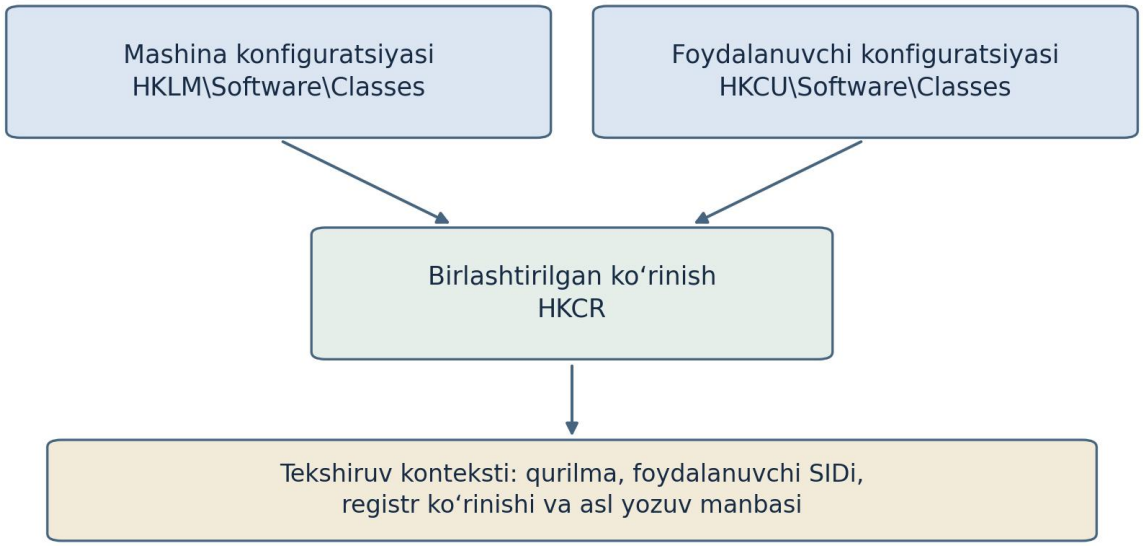
Registr muharriridagi asosiy bo‘limlar bir xil ma’nodagi mustaqil fayllar to‘plami emas. Ayrimlari tizim holatini, boshqalari joriy foydalanuvchini yoki birlashtirilgan ko‘rinishni ifodalaydi. HKCU tekshiruvchi jarayon ishlayotgan foydalanuvchi bilan bog‘liq; administrator hisobidan olingan HKCU nusxasi boshqa foydalanuvchining sozlamalarini avtomatik qamrab olmaydi [2].

1-jadval. Asosiy registr bo‘limlari va tekshiruvdagi vazifasi

Qisqartma	Mazmuni	Monitoring uchun ahamiyati
HKLM	Kompyuter miqyosidagi konfiguratsiya	Tizim va dastur sozlamalarini tekshirish
HKCU	Joriy foydalanuvchi konfiguratsiyasi	Tekshirilayotgan hisob va SIDni qayd etish
HKU	Yuklangan foydalanuvchi bo‘limlari	Bir nechta hisobni farqlash

Qisqartma	Mazmuni	Monitoring uchun ahamiyati
HKCR	Sinflar va fayl bog‘lanishlarining birlashgan ko‘rinishi	O‘zgarishning HKLM yoki HKCU manbasini aniqlash
HKCC	Joriy apparat profili ko‘rinishi	Uni alohida to‘liq hive deb talqin qilmaslik

HKCR ma’lumotlari HKLM\Software\Classes va HKCU\Software\Classes bo‘limlaridan birlashtiriladi. Bu COM va fayl bog‘lanishlarini tekshirishda muhim: mashina bo‘yicha to‘g‘ri ko‘ringan yozuv ayrim foydalanuvchi kontekstida boshqa qiymat bilan ustun kelishi mumkin. Tahlilchi birlashgan natija bilan birga uning haqiqiy manbasini ham yozib borishi kerak [6].



1-rasm. Registrning mantiqiy ko‘rinishlari va kuzatuv konteksti

1.3. Qiymat turlari va taqqoslash aniqligi

Registr qiymatlari turli formatlarda saqlanadi. REG_EXPAND_SZ tarkibidagi muhit o‘zgaruvchisini darhol kengaytirib saqlash asl yozuvni o‘zgartirib ko‘rsatishi mumkin. Tahlilda xom qiymat va muayyan foydalanuvchi uchun hisoblangan yo‘l alohida maydon bo‘lgani ma’qul. REG_MULTI_SZ uchun satrlar ketma-ketligi, REG_BINARY uchun esa baytlar aynan saqlanishi kerak [4].

2-jadval. Ko‘p uchraydigan qiymat turlari

Tur	Ma’lumot	Taqqoslashdagi talab
REG_SZ	Matnli satr	Bo‘sh satrni mavjud emaslikdan ajratish
REG_EXPAND_SZ	Muhit o‘zgaruvchili satr	Xom satrni saqlash
REG_DWORD	32 bitli son	Sonni matn sifatida solishtirmaslik
REG_QWORD	64 bitli son	Katta son aniqligini saqlash

Tur	Ma’lumot	Taqqoslashdagi talab
REG_MULTI_SZ	Satrlar ketma-ketligi	Elementlar va tartibni saqlash
REG_BINARY	Ikkilik ma’lumot	Baytlar yoki ularning ishonchli kodlanishi

Yangi holatni eski holatga nisbatan baholashda uch turdagi farq ajratiladi: qo‘shish, o‘chirish va o‘zgartirish. Qiymat nomi o‘zgarganda esa oddiy ikki nusxali taqqoslash buni o‘chirish va qo‘shish juftligi sifatida ko‘rsatishi mumkin. Nom almashtirishni aniq hodisa sifatida ajratish uchun tegishli telemetriya kerak. Demak, holat farqi bilan bajarilgan amallar tarixi bir xil axborot emas.

1.4. Hive fayllari va vaqt belgilarini talqin qilish

Hive — kalitlar, quyi kalitlar va qiymatlarning fayllar bilan ta’minlanadigan mantiqiy guruhidir. Tizimning SYSTEM, SOFTWARE, SAM va SECURITY kabi hive fayllari odatda %SystemRoot%\System32\Config katalogida joylashadi. Foydalanuvchi sozlamalarining muhim qismi NTUSER.DAT bilan bog‘liq. Oflayn tahlilda asosiy hive bilan bog‘liq jurnal fayllari ham dalil qiymatiga ega bo‘lishi mumkin [3].

Registr hive nusxasi tizimning to‘liq disk tasviri o‘rnini bosmaydi. Unda ko‘rsatilgan faylning o‘zi, xotiradagi jarayon va tarmoq aloqasi alohida tekshiriladi. Ishlayotgan tizimdan dalil yig‘ishda foydalanilgan vosita, vaqt va usul qayd etilishi kerak; qo‘lda nusxalashning o‘zi izchil holat olinganini kafolatlamaydi. Bu ishda hive kriminalistikasining barcha ichki formatlari emas, o‘zgarishlarni aniqlash va tiklash uchun zarur axborot ko‘rib chiqiladi.

RegQueryInfoKey orqali olinadigan oxirgi yozish vaqti kalit darajasidagi ma’lumotdir [34]. Uni har bir qiymatning yaratilish vaqti yoki muayyan jarayonning yozish vaqti deb qabul qilib bo‘lmaydi. Hodisa vaqti, yig‘ish vaqti va kalit metama’lumoti alohida saqlansa, keyinchalik voqealar ketma-ketligini tiklashdagi chalkashlik kamayadi.

1.5. Ruxsatlar va registr ko‘rinishlari

Registr kalitining DACL ro‘yxati kimga qanday amal ruxsat etilishini, SACL esa qaysi mos murojaat audit qilinishini belgilaydi. KEY_SET_VALUE va KEY_CREATE_SUB_KEY huquqlari turli amallarni qamrab oladi. Qiymat matni o‘zgarmagan holda ruxsatlar haddan tashqari kengaytirilishi ham xavf tug‘dirishi mumkin. Shu sababli muhim kalitlar uchun qiymatlar bilan birga egasi va ruxsatlari ham tekshiriladi [7].

64 bitli Windows’da registrning ayrim qismlari 32 va 64 bitli dasturlar uchun alohida mantiqiy ko‘rinishga ega [5]. Barcha kalitlar ikki marta mavjud degan xulosa noto‘g‘ri. Inventarizatsiyada qaysi ko‘rinish o‘qilgani yoziladi; turli ko‘rinishlardan olingan natijalar bir-biriga aralashtirilmaydi. Shuningdek, bir kompyuterdagi bazaviy holat boshqa Windows versiyasi yoki boshqa rolga ega kompyuter uchun avtomatik etalon bo‘la olmaydi.

2. ZARARLI O‘ZGARISHLARNING ASOSIY MEXANIZMLARI

2.1. Avtomatik ishga tushirish yozuvlari

Run va RunOnce kalitlari foydalanuvchi tizimga kirganda dastur bajarilishini tashkil etadi. Run odatda takroriy, RunOnce esa bir martalik bajarilish uchun ishlatiladi. HKLM dagi yozuvning o‘zi

dasturni avtomatik ravishda SYSTEM huquqida bajaradi, degan xulosa kelib chiqmaydi. Mexanizmning hisob konteksti va ishga tushish shartlari alohida baholanadi [8, 9].

Shubha uyg‘otadigan holatlar qatoriga profilning yozish mumkin bo‘lgan katalogidagi noma’lum fayl, kutilmagan skript interpretatori, yashirilgan argumentlar va tasdiqlanmagan o‘rnatishdan keyin paydo bo‘lgan yozuv kiradi. Biroq AppData katalogidan ishga tushadigan barcha dasturlar zararli emas. Ishonchli xulosa uchun yozuvni yaratgan jarayon, faylning kelib chiqishi va foydalanuvchining kutilgan faoliyati birgalikda tekshiriladi.

2.2. Xizmatlar konfiguratsiyasi

Windows xizmatining bajariluvchi fayli va boshqa konfiguratsiyasi registr bilan bog‘liq. Yangi xizmat yaratish yoki mavjud xizmat sozlamasini almashtirish doimiy ishlashni ta’minlash uchun suiiste’mol qilinishi mumkin [10]. Tahlilda HKLM\SYSTEM\CurrentControlSet\Services ostidagi o‘zgarishlar xizmatning nomi, hisob konteksti va bajariluvchi fayli bilan bog‘lanadi.

Xizmat nomining Microsoft mahsulotiga o‘xshashi qonuniylik dalili emas. Aksincha, uchinchi tomon mahsulotining yangi xizmati ham tasdiqlangan yangilanishning bir qismi bo‘lishi mumkin. Tekshirishda xizmat haqidagi boshqaruv ma’lumotlari va registr holati qiyoslanadi. Faqat registr yozuvini o‘chirish amalda ishlayotgan xizmatni to‘xtatmaydi; noto‘g‘ri o‘chirish esa mahsulot yoki operatsion tizim faoliyatini buzishi mumkin.

2.3. Winlogon IFEO va COM yozuvlari

Winlogon bilan bog‘liq Shell va Userinit kabi sozlamalar kirish jarayoniga ta’sir qiladi. Ularning kutilmagan o‘zgarishi qo‘shimcha dastur bajarilishiga olib kelishi mumkin [13]. «Barcha kompyuterlar uchun yagona to‘g‘ri qiymat» yondashuvi kiosk, maxsus qobiq yoki boshqariladigan ish joylarida xato bo‘ladi. Tiklash uchun aynan shu qurilma roliga mos tasdiqlangan konfiguratsiya olinadi.

Image File Execution Options (IFEO) dasturlarni diagnostika qilish imkoniyatlari bilan bog‘liq. Uning Debugger kabi qiymatlari dasturning odatiy bajarilish yo‘lini o‘zgartirish yoki himoya dasturini ishlatmaslik uchun suiiste’mol qilinishi mumkin [11]. Tekshiruv debugging vositasining mavjudligini, o‘zgarish sababini va qaysi dasturga ta’sir qilganini aniqlaydi. Barcha IFEO kalitlarini yalpi o‘chirish to‘g‘ri bartaraf etish usuli emas.

COM obyektlariga murojaatlarni boshqa komponentga yo‘naltirish ham registr orqali sodir bo‘lishi mumkin. CLSID ostidagi InprocServer32 yoki LocalServer32 bilan bog‘liq yo‘llarni tekshirishda foydalanuvchi va mashina konfiguratsiyasi ajratiladi [12]. Noma’lum DLL haqidagi yozuvning o‘zi uning yuklanganini isbotlamaydi: yuklanish yoki jarayon hodisasi bilan tasdiqlash zarur.

2.4. Himoya siyosatlari va ruxsatlarni zaiflashtirish

Hujumchi himoya komponentlari sozlamalariga yoki xavfsizlikka ta’sir qiluvchi siyosatlarga o‘zgartirish kiritishga urinishi mumkin. Registr modifikatsiyasi MITRE ATT&CK’da T1112 sifatida umumlashtiriladi, ammo maqsad va natijaga qarab boshqa texnikalar bilan ham bog‘lanadi [14]. Shu sababli tahlil yozuv nomini texnika identifikatoriga almashtirish bilan tugamaydi; real ta’sir alohida tekshiriladi.

Microsoft Defender’dagi tamper protection himoyalangan sozlamalarning ruxsatsiz o‘zgartirilishini cheklaydi. Ayrim urinishlar boshqaruv vositasida muvaffaqiyatli ko‘rinsa ham, haqiqiy himoyalangan

holat o‘zgarmasligi mumkin [29]. Istisnolarni himoyalash esa boshqaruv usuli va mahsulot shartlariga bog‘liq [30]. Demak, registrda ko‘ringan qiymatni mahsulotning amaldagi holati bilan tekshirmasdan «antivirus o‘chirildi» deb xulosa qilish mumkin emas.

2.5. Kuzatuv nuqtalarini ustuvorlashtirish

Quyidagi yo‘llar tekshiruv uchun boshlang‘ich nuqtalardir. Ro‘yxat registrga bog‘liq barcha hujumlarni qamrab olmaydi. Jadvaldagi «dalil» ustuni har bir yozuvning xavfliligini tasdiqlash uchun qanday qo‘shimcha ma’lumot kerakligini ko‘rsatadi. Yo‘llardagi <dastur>, <xizmat> va <CLSID> belgilarini haqiqiy yozuv nomi almashtiradi.

3-jadval. Muhim kuzatuv nuqtalari va tekshiriladigan dalillar

Nuqta	Kuzatiladigan yozuv	Qo‘shimcha dalil
Run va RunOnce	HKCU yoki HKLM\Software\Microsoft\Windows\CurrentVersion osti	Yozuvchi jarayon, fayl yo‘li, kirishdan keyingi bajarilish
Xizmat	HKLM\SYSTEM\CurrentControlSet\Services\<xizmat>	Xizmat holati, ImagePath, hisob va fayl imzosi
Winlogon	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	Shell yoki Userinit o‘zgarishining tasdiqlangan sababi
IFEO	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<dastur>	Debugger va mo‘ljaldagi dastur faoliyati
COM	HKCU yoki HKLM\Software\Classes\CLSID\<CLSID>	Haqiqiy yozuv manbasi, DLL yoki EXE yuklanishi
Himoya siyosati	Mahsulotning tegishli Policies va sozlama bo‘limlari	Amaldagi himoya holati va boshqaruv siyosati
Ruxsatlar	Yuqoridagi kritik kalitlarning egasi va DACL holati	Oldingi ruxsat, o‘zgarish subyekti va ehtiyoj

Kuzatuv qoidasining doirasi uning maqsadi bilan belgilanadi. Masalan, Run yozuvlariga qaratilgan qoida COM o‘zgarishini ushlamasa, bu qoidaning aynan belgilangan doirasi bilan izohlanishi mumkin. Tizim qamrovi esa barcha qoidalar, ko‘rinishlar va foydalanuvchilar bo‘yicha alohida tekshiriladi. «Hodisa yo‘q» degan holatni «zararli o‘zgarish yo‘q» degan kafolatga aylantirishdan oldin ma’lumot manbalari sog‘lomligi tasdiqlanadi.

3. O‘ZGARISHLARNI ANIQLASH VA DALILLARNI YIG‘ISH USULLARI

3.1. Bazaviy holat bilan taqqoslash

Bazaviy holat (baseline) — ma’lum vaqtda ishonchli deb tasdiqlangan konfiguratsiya nusxasi. Unda qurilma identifikatori, Windows yig‘masi, foydalanuvchi SIDi, registr ko‘rinishi, kalit va qiymatlar, olish vaqti hamda muhim ruxsatlar saqlanadi. Nusxa yaratilganidan keyin tasdiqlangan yangilanishlar ham

hisobga olinadi. Eskirgan etalon ko‘p noto‘g‘ri ogohlantirish, zararlangan tizimdan olingan etalon esa yashirin xavf tug‘diradi.

Ikki nusxani taqqoslash joriy holatda nima farq qilishini ko‘rsatadi, lekin farqni kim yaratganini isbotlamaydi. O‘zgarish kuzatuv oralig‘ida paydo bo‘lib, keyin o‘chirilsa, davriy suratga olish uni o‘tkazib yuborishi mumkin. Shu bois bazaviy holat doimiy hodisa kuzatuvini to‘ldiradi. Taqqoslashdagi «o‘qish imkoni yo‘q» holati alohida xato bo‘lib saqlanadi; u bo‘sh kalit yoki o‘chirilgan qiymatga tenglashtirilmaydi.

3.2. Process Monitor orqali aniq amalni kuzatish

Process Monitor registr, fayl tizimi va jarayon faoliyatini real vaqtda qayd etadi. Operatsiya, yo‘l, natija va jarayon xususiyatlari bo‘yicha filtrlash muayyan dastur qaysi qiymatga yozganini tekshirishga yordam beradi [15]. Registr tahlilida RegSetValue, RegCreateKey, RegDeleteValue va RegDeleteKey kabi operatsiyalar alohida ko‘riladi. SUCCESS bajarilgan amalni, ACCESS DENIED esa rad etilgan urinishni bildirishi mumkin; ikkalasi bir xil oqibat emas.

Usul ayniqsa qisqa laboratoriya yoki takrorlanuvchi muammoni o‘rganishda qulay. Kuzatuv boshlanishidan oldingi tarix avtomatik tiklanmaydi. Ko‘p hodisani nazoratsiz yig‘ish katta fayl va tahlil shovqiniga olib keladi. Mahalliy tajriba uchun tor yo‘l filtri, belgilangan vaqt oralig‘i va saqlangan PML fayli tavsiya etiladi. Hisobotda skrinshotdan tashqari xom dalilning joylashuvi ham ko‘rsatiladi.

3.3. Autoruns orqali ishga tushish nuqtalarini tekshirish

Autoruns avtomatik ishga tushish joylarini, jumladan logon yozuvlari, xizmatlar, Winlogon va boshqa kengaytmalarni bir ko‘rinishda tekshirish imkonini beradi [16]. Tahlilchi yozuvdan registrdagi joyga yoki bog‘liq faylga o‘tib, konfiguratsiyani tekshirishi mumkin. Bu vosita ishga tushish nuqtalarini qamrab olish uchun foydali, ammo barcha registr o‘zgarishlarining vaqt bo‘yicha to‘liq jurnalini bermaydi.

Tasdiqlangan Microsoft yozuvlarini yashirish ko‘rishni yengillashtirishi mumkin, biroq bu xavfsizlik bo‘yicha yakuniy qaror emas. Imzolanmagan ichki dastur qonuniy bo‘lishi, ishonchli bajariluvchi fayl esa zararli argumentlar bilan chaqirilishi mumkin. Dastlab holat saqlanadi, keyin aynan qaysi yozuvni vaqtincha o‘chirish kerakligi aniqlanadi. Xususiy fayllarni tashqi tekshiruv xizmatiga yuborish mahalliy tashkilot siyosati bilan kelishilgan bo‘lishi kerak.

3.4. Sysmon hodisalari va ularning chegaralari

Sysmon registr hodisalarini jarayon identifikatorlari bilan bog‘lashga xizmat qiladi. 12-raqamli hodisa yaratish yoki o‘chirish, 13-raqamli hodisa qiymat yozish, 14-raqamli hodisa nom almashtirish bilan bog‘liq [17, 18]. ProcessGuid jarayonlarni bog‘lashda PIDning qayta ishlatilishidan keladigan chalkashlikni kamaytiradi. Jurnal odatda Microsoft-Windows-Sysmon/Operational kanalidan o‘qiladi [36].

Sysmon’ni to‘liq registr zaxirasi deb bo‘lmaydi. Hodisa tarkibi amal, qiymat turi, versiya va konfiguratsiyaga bog‘liq; ayniqsa eski qiymatni hamisha olish kafolatlanmaydi. Rasmiy tavsif Event 13 uchun DWORD va QWORD yozilgan qiymatlarini qayd etishni alohida ko‘rsatadi [17]. Shu sababli tiklash ma’lumoti faqat Details maydoniga bog‘lanmaydi. Kritik yozuvlar uchun oldingi tasdiqlangan holat alohida saqlanadi.

4-jadval. Registr tekshiruvida ishlatiladigan asosiy hodisalar

Manba va ID	Mazmuni	Muhim cheklov
Sysmon 12	Registr obyektini yaratish yoki o‘chirish	Konfiguratsiya qamroviga bog‘liq
Sysmon 13	Qiymatga yozish	To‘liq oldingi holat zaxirasi emas
Sysmon 14	Kalit yoki qiymat nomini almashtirish	Boshqa hodisalar bilan bog‘lash kerak
Sysmon 1	Jarayon yaratilishi	Alohida yig‘ish qoidasini tekshirish kerak
Security 4657	Registr qiymatini yaratish, o‘zgartirish yoki o‘chirish	Audit Registry va mos SACL talab etiladi
Security 4688	Yangi jarayon yaratilishi	Buyruq satri uchun qo‘shimcha siyosat kerak

Konfiguratsiyani sozlashda ortiqcha istisnolar kritik hodisalarni yashirib qo‘ymasligi tekshiriladi. Har bir yangi qoida uchun «qaysi nazorat o‘zgarishi qayd etilishi kerak» degan sinov belgilanadi. Sysmon xizmatining holati, konfiguratsiya o‘zgarishi va log yetkazib berish uzilishlari ham kuzatiladi. Faqat hodisalar sonining kamayishi yaxshi tuning bo‘lganini isbotlamaydi; kamayishning sababi aniqlanishi kerak [36].

3.5. Security 4657 va audit shartlari

Security 4657 registr **qiymati** o‘zgarishini kuzatadi; u kalitga tegishli barcha amallar uchun umumiy hodisa emas [20]. Uni olish uchun Audit Registry siyosati va mo‘ljaldagi kalitda tegishli hisobga mos Set Value audit yozuvi kerak. Faqat siyosatni yoqish yoki faqat SACL qo‘shish yetarli emas. Muvaffaqiyatli va rad etilgan murojaatlar auditi ham alohida sozlanadi [19].

Hodisada foydalanuvchi, jarayon, obyekt yo‘li, qiymat nomi va mavjud o‘zgarish maydonlari tekshiriladi. Security jurnalidagi HKCU yo‘li \REGISTRY\USER\<SID> ko‘rinishida kelishi mumkin [20]. Normalizatsiya foydalanuvchi SIDini yo‘qotmasligi kerak. 4688 bilan bog‘lashda esa Audit Process Creation hamda buyruq satrini kiritish siyosati tekshiriladi; buyruq argumentlarida maxfiy ma’lumot bo‘lishi mumkin [21].

Audit sozlashda butun registr daraxtiga barcha o‘qish amallarini yig‘ish odatda amaliy emas. Kritik kalitlar, kerakli amallar va foydalanuvchilar tanlanadi. Sinov qiymati o‘zgartirilib, kutilgan hodisa borligi tekshiriladi. Hodisa chiqmasa, qoida doirasi, foydalanuvchi konteksti, SACL meroslanishi va jurnal mavjudligi tekshiriladi. Bu tekshiruvdan keyingina monitoring ishlayapti deb hisoblash mumkin.

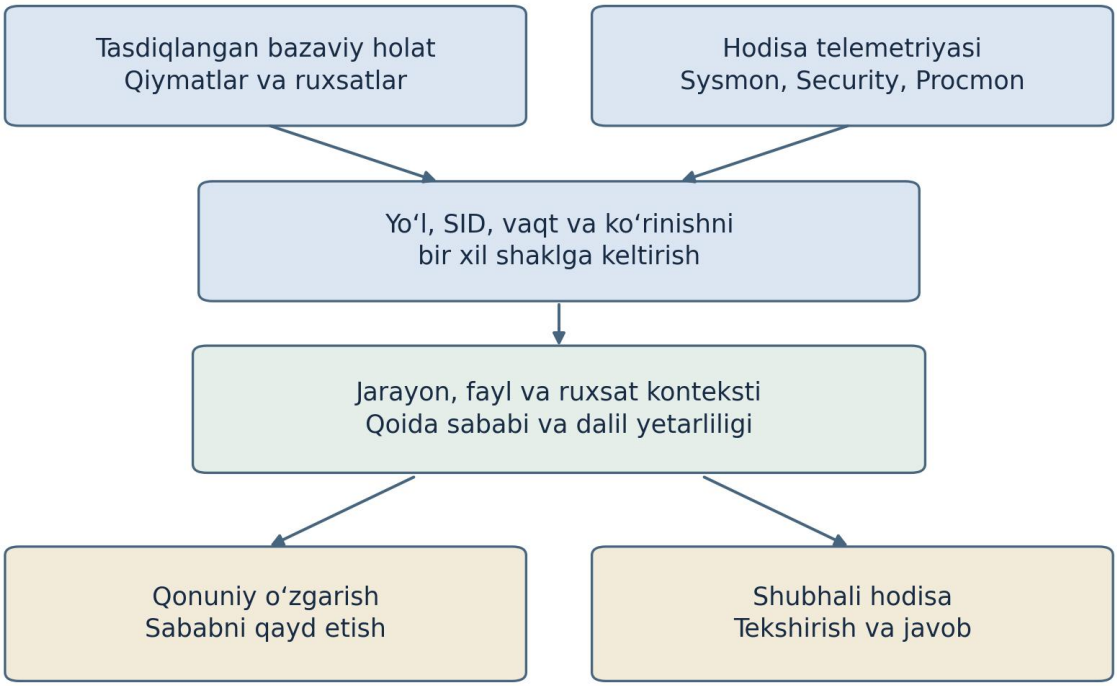
3.6. Telemetriyani birlashtirish va hodisa kartasi

Bir qurilmada turli manbalar kalit yo‘lini turlicha ifodalashi mumkin. Tahlil uchun xom yo‘l saqlanib, yonida normallashtirilgan yo‘l yuritiladi. SID, kompyuter va registr ko‘rinishi alohida maydonlar sifatida qoladi. Vaqt UTC ko‘rinishida saqlansa, bir nechta qurilma ma’lumotini bog‘lash osonlashadi. Mahalliy vaqtni ko‘rsatishda uning vaqt mintaqasi ham yoziladi.

Taklif etilayotgan hodisa kartasi quyidagilarni birlashtiradi: kalit va qiymat, amal, eski va yangi ma’lumot mavjudligi, foydalanuvchi, yozuvchi jarayon, uning ota jarayoni, bog‘liq fayl yo‘li, hash, imzo

holati hamda o‘zgarish uchun berilgan ruxsat. Jarayon zanjiri va vaqt bo‘yicha yaqin hodisalarni birga tekshirish MITRE’ning xatti-harakatga asoslangan aniqlash strategiyasiga mos keladi [37].

Microsoft Defender for Endpoint o‘rnatilgan muhitda DeviceRegistryEvents jadvali registr va tashabbuskor jarayon ma’lumotlarini tahlil qilishga imkon beradi. Mahsulot ulanmagan qurilmada bu jadvaldan natija kutish to‘g‘ri emas [22]. Imzo tekshiruvida Get-AuthenticodeSignature qo‘llanishi mumkin, lekin Valid holat faqat imzo tekshiruvi natijasidir; faylning barcha kontekstlarda zararsizligi haqidagi kafolat emas [23].



2-rasm. Holat va hodisa ma’lumotlarini birlashtiruvchi aniqlash modeli

3.7. Izohlanadigan balli saralash modeli

Hodisalarni tekshirish navbatiga qo‘yish uchun muallif quyidagi oddiy mezonni taklif qiladi. U statistik o‘rgatilgan model yoki sanoat standarti emas; vaznlar tushuntirish maqsadida tanlangan. Har bir belgi 0 yoki 1 qiymat oladi. Baholashdan oldin ma’lumotning noma’lumligi bilan belgining yo‘qligi ajratiladi.

$$R = \max(0, 2K + 2W + 2L + U + C - 2A)$$

5-jadval. Taklif etilgan baholash modelining belgilari

Belgi	1 qiymat berish sharti	Ball
K	Kritik konfiguratsiya nuqtasi o‘zgargan	+2
W	Bog‘liq bajariluvchi yo‘l foydalanuvchi yozishi mumkin bo‘lgan joyda	+2
L	Shu vazifa uchun noodatiy interpretator yoki ishga tushirish usuli bor	+2
U	Yozuvchi jarayon kutilgan faoliyatga mos kelmaydi	+1

Belgi	1 qiymat berish sharti	Ball
C	Bog‘liq jarayon yoki fayl hodisasi shubhani kuchaytiradi	+1
A	Aynan shu o‘zgarish uchun tekshirilgan ruxsat mavjud	−2

W belgisi faqat katalog nomiga qarab emas, amaldagi yozish huquqi va yo‘lni to‘g‘ri ajratish orqali baholanadi. U belgisi ham shunchaki «imzo yo‘q» degani emas. A belgisi faqat fayl nomining ruxsat ro‘yxatida borligidan chiqarilmaydi: ish topshirig‘i, vaqt, qurilma va o‘zgarish doirasi mos bo‘lishi kerak. Shunda istisnolar haddan tashqari kengayib ketmaydi.

R qiymati chegaradan yuqori bo‘lsa, hodisa tekshiruvga ajratiladi. Ma’lumot yetishmasligi alohida «qo‘shimcha dalil kerak» holatini beradi. Amaliy muhitda himoyani tasdiqlanmagan o‘chirish kabi kritik holatlar oddiy yig‘indi balldan mustaqil majburiy tekshiruv qoidasiga ega bo‘lishi lozim. 4-bo‘limdagi hisoblash tajribasi faqat formulani baholaydi; bunday qo‘shimcha qoidalar uning natijalariga aralashtirilmagan.

4. XAVFSIZ LABORATORIYA VA HISOBLASH TAJRIBASI

4.1. Laboratoriya doirasi va tayyorlash

Quyidagi protokol Windows 11 virtual mashinasida takrorlash uchun beriladi. U o‘quv tajribasi bo‘lib, haqiqiy zararli fayl, avtomatik ishga tushirish yozuvi yoki antivirusni o‘chirishni talab qilmaydi. Barcha yozish amallari joriy foydalanuvchining HKCU\Software\RegistryResearchLab kaliti bilan cheklanadi. Monitoring o‘rnatishdan oldin virtual mashina holati saqlanadi; mavjud korporativ kuzatuv konfiguratsiyasi bu misol bilan almashtirilmaydi.

Sinov qiymatini yaratish odatda oddiy foydalanuvchi huquqida bajariladi. Sysmon o‘rnatish, Security jurnalini o‘qish yoki SACL sozlash kabi bosqichlar esa tegishli yuqori huquqlarni talab qilishi mumkin. Barcha listinglar bir PowerShell seansida ketma-ket bajariladigan qilib yozilgan. Windows laboratoriyasida olinadigan natijalar quyida **kutiladigan natijalar** sifatida keltiriladi; ular ushbu maqolada olingan haqiqiy Windows loglari deb taqdim etilmaydi.

4.2. Boshlang‘ich holatni yaratish va saqlash

Birinchi listing avval shu nomli sinov kaliti bor-yo‘qligini tekshiradi. Mavjud kalit topilsa, uning ma’lumotini o‘zgartirmasdan to‘xtaydi. Dalillar uchun tasodifiy identifikatorli alohida katalog yaratiladi. REG_SZ va REG_DWORD qiymatlarining birga ishlatilishi matn hamda son turlarini taqqoslashni ko‘rsatadi.

```
$ErrorActionPreference = 'Stop'
$labKey = 'HKCU:\Software\RegistryResearchLab'
$nativeKey = 'HKCU\Software\RegistryResearchLab'
if (Test-Path -LiteralPath $labKey) {
throw 'Sinov kaliti mavjud. Avval uning egasini tekshiring.'
}
$tag = [guid]::NewGuid().ToString('N')
$work = Join-Path $env:TEMP ('RegistryLab_' + $tag)
New-Item -ItemType Directory -Path $work | Out-Null
```

```
New-Item -Path $labKey | Out-Null
New-ItemProperty -Path $labKey -Name Mode `
-PropertyType String -Value 'Baseline' | Out-Null
New-ItemProperty -Path $labKey -Name Counter `
-PropertyType DWord -Value 0 | Out-Null
$backup = Join-Path $work 'baseline.reg'
reg.exe export $nativeKey $backup
if ($LASTEXITCODE -ne 0) { throw 'Eksport bajarilmadi.' }
Get-Acl -LiteralPath $labKey |
Select-Object Owner, Sddl |
ConvertTo-Json | Set-Content (Join-Path $work 'acl.json')
Write-Output $work
```

1-listing. Alohida laboratoriya kaliti va boshlang‘ich nusxani yaratish

reg export kalit va qiymatlarni .reg fayliga chiqaradi [25]. Bu nusxa ruxsatlar, barcha metama’lumotlar yoki to‘liq operatsion tizim holatining ekvivalenti emas. Shu sababli listing egasi va DACLga oid SDDL ko‘rinishini Get-Acl orqali alohida yozadi [35]. SACLni ham saqlash zarur bo‘lsa, tegishli audit huquqlari bilan alohida yig‘ish talab etiladi. Asl dalil fayllari o‘zgartirilmaydigan joyga ko‘chirilishi mumkin.

4.3. Qiymatlarning turini saqlagan holda taqqoslash

Quyidagi funksiya faqat berilgan kalitdagi qiymatlarni oladi; quyi kalitlarni rekursiv qamrab olmaydi. Xom ma’lumot JSON ko‘rinishiga keltirilib, turi alohida saqlanadi. Shu yo‘l bilan son, satr va ko‘p satrli qiymatlarni bir xil oddiy matnga aylantirishdan keladigan xato kamayadi. Asl yozuvdagi muhit o‘zgaruvchilari avtomatik kengaytirilmaydi.

```
function Get-LabSnapshot([string]$Path) {
$key = Get-Item -LiteralPath $Path
$optionType = [Microsoft.Win32.RegistryValueOptions]
$option = $optionType::DoNotExpandEnvironmentNames
foreach ($name in ($key.GetValueNames() | Sort-Object)) {
$raw = $key.GetValue($name, $null, $option)
[pscustomobject]@{
Name = $name
Type = $key.GetValueKind($name).ToString()
Data = ConvertTo-Json -InputObject $raw -Compress
}
}
}
$before = @(Get-LabSnapshot $labKey)
$before | ConvertTo-Json -Depth 5 |
Set-Content (Join-Path $work 'before.json')
Set-ItemProperty -LiteralPath $labKey -Name Mode -Value 'Changed'
Set-ItemProperty -LiteralPath $labKey -Name Counter -Value 7
```

```
New-ItemProperty -Path $labKey -Name Marker `
-PropertyType String -Value 'DemoOnly' | Out-Null
$after = @(Get-LabSnapshot $labKey)
Compare-Object $before $after -Property Name, Type, Data
```

2-listing. Zararsiz o‘zgarishlar va boshlang‘ich holat bilan taqqoslash

Compare-Object natijasida <= belgisi boshlang‘ich, => belgisi keyingi nusxadagi yozuvni anglatadi. Mode va Counter o‘zgargani uchun eski hamda yangi yozuvlar juft holda ko‘rinadi; Marker esa yangi yozuv sifatida chiqadi. Bu yerda aniqlangan farqlar zararli niyatga ega emas. Laboratoriyaning vazifasi o‘zgarishlarni ko‘rish va to‘g‘ri talqin qilishdir, «har bir farq zararli» qoidasini tasdiqlash emas.

4.4. Process Monitor va Sysmon bilan kuzatuv

Process Monitor’da dastlab Path ustuniga RegistryResearchLab yo‘lini qamrab oluvchi filtr qo‘yiladi. Yozish amallari bo‘yicha toraytirishdan oldin sinov hodisasi ko‘rinayotgani tekshiriladi. Kuzatuv 2-listingdagi o‘zgarishlardan oldin boshlanadi va undan keyin to‘xtatiladi. Natijada PowerShell jarayoni, yo‘l va bajarilgan operatsiya tekshiriladi. Filtrga faqat powershell.exe ni kiritish PowerShell 7 ishlatilganda pwsh.exe hodisalarini yashirishi mumkin.

Sysmon uchun quyidagi kichik konfiguratsiya alohida laboratoriyaga mo‘ljallangan. U registr bo‘yicha sinov kalitini, jarayonlar bo‘yicha esa yaratish hodisalarini qayd etadi. XML sintaksisi joriy o‘rnatilgan versiyaning sxemasi bilan tekshiriladi; sxema versiyasi dastur versiyasi bilan bir xil tushuncha emas [17].

```
<Sysmon schemaversion="4.82">
<HashAlgorithms>sha256</HashAlgorithms>
<EventFiltering>
<ProcessCreate onmatch="exclude" />
<RegistryEvent onmatch="include">
<TargetObject condition="contains"
>\Software\RegistryResearchLab</TargetObject>
</RegistryEvent>
</EventFiltering>
</Sysmon>
```

3-listing. Laboratoriya uchun cheklangan Sysmon konfiguratsiyasi

Konfiguratsiya registry-lab.xml nomi bilan saqlanadi. Yangi laboratoriya mashinasida sxemani ko‘rish uchun Sysmon64.exe -s, o‘rnatish uchun Sysmon64.exe -i registry-lab.xml qo‘llanadi. Oldin o‘rnatilgan agent mavjud bo‘lsa, avval uning boshqaruv usuli va amaldagi konfiguratsiyasi aniqlanadi. O‘rnatish muvaffaqiyati sinov hodisasi jurnalga tushgani bilan tasdiqlanadi.

Get-WinEvent jurnallarni vaqt va identifikator bo‘yicha filtrlash imkonini beradi [24]. Listingdagi XML maydonlari nom bilan olinadi; ekrandagi tarjima qilingan Message matnini satr bo‘yicha ajratishga tayanilmaydi. Ayrim hodisalarda Details yoki User bo‘lmasa, tegishli ustun bo‘sh qoladi. Tahlilchi yo‘q ma’lumotni xayolan to‘ldirmasligi kerak.

```
$filter = @{
LogName = 'Microsoft-Windows-Sysmon/Operational'
Id = 12, 13, 14
```

```
StartTime = (Get-Date).AddHours(-1)
}
Get-WinEvent -FilterHashtable $filter | ForEach-Object {
$ev = $_
$xml = [xml]$ev.ToXml()
$fields = @{}
foreach ($item in $xml.Event.EventData.Data) {
$fields[[string]$item.Name] = [string]$item.'#text'
}
if ($fields.TargetObject -like '*\RegistryResearchLab*') {
[pscustomobject]@{
Utc = $ev.TimeCreated.ToUniversalTime().ToString('o')
EventId = $ev.Id
ProcessGuid = $fields.ProcessGuid
Image = $fields.Image
TargetObject = $fields.TargetObject
Details = $fields.Details
}
}
} | Export-Csv (Join-Path $work 'events.csv') `
-NoTypeInformation -Encoding UTF8
```

4-listing. Laboratoriya hodisalarini nomlangan maydonlar orqali chiqarish

Xom jurnal ham alohida saqlanadi. Masalan, wevtutil epl buyrug‘i bilan tegishli kanal .evtx fayliga eksport qilinadi [33]. CSV tahlil uchun qulay, lekin xom jurnalning o‘rnini to‘liq bosa olmaydi. Yig‘ish vaqti va eksport faylining SHA-256 qiymati dalillar ro‘yxatiga kiritiladi. Hash nusxa o‘zgarmaganini tekshirishga yordam beradi, lekin hodisaning o‘zi to‘g‘ri ekanini mustaqil isbotlamaydi.

4.5. Security auditi va tiklashni tekshirish

Security 4657 tajribasi uchun Advanced Audit Policy Configuration ichidagi Object Access → Audit Registry’da muvaffaqiyat auditi yoqiladi. Registry Editor’da aynan laboratoriya kalitining Permissions → Advanced → Auditing bo‘limida sinov foydalanuvchisi uchun muvaffaqiyatli Set Value auditi belgilanadi. Menyu nomlari Windows tiliga qarab farq qilishi mumkin. Ushbu sozlamalardan **keyin** qiymat o‘zgartirilib, Security jurnalidan 4657 qidiriladi [19, 20].

Keyingi listing .reg importining muhim chegarasini namoyish etadi. Eksport nusxasidagi Mode va Counter qiymatlari qayta yoziladi, lekin nusxada bo‘lmagan Marker avtomatik o‘chirilmaydi. Import eski nusxaga mos barcha keyingi qo‘shimchalarni bekor qiladigan umumiy rollback emas [26].

```
reg.exe import $backup
if ($LASTEXITCODE -ne 0) { throw 'Import bajarilmadi.' }
$merged = @(Get-LabSnapshot $labKey)
Compare-Object $before $merged -Property Name, Type, Data
# Faqat shu tajribada yaratilgan qo‘shimcha qiymat o‘chiriladi.
Remove-ItemProperty -LiteralPath $labKey -Name Marker
```

```
$restored = @(Get-LabSnapshot $labKey)
$difference = Compare-Object $before $restored `
-Property Name, Type, Data
if ($null -eq $difference) {
'Tekshirilgan qiymatlar boshlang‘ich holatga mos.'
} else {
$difference
}
```

5-listing. Importdan keyingi qoldiq qiymatni topish va aniq tiklash

Oxirgi xabar faqat tekshirilgan qiymatlarning mosligini bildiradi. U SACL, kalit vaqti, boshqa registr yo‘llari yoki butun kompyuterning xavfsizligini tasdiqlamaydi. Tajriba tugagach dalillar saqlanadi, shu tajribada o‘zgartirilgan audit sozlamalari oldingi holatiga qaytariladi va laboratoriya kaliti olib tashlanadi. Mavjud umumiy audit siyosatini ko‘r-ko‘rona o‘chirish mumkin emas.

6-jadval. Windows laboratoriyasida tekshiriladigan kutiladigan holatlar

Amal	Kutiladigan dalil	Qabul qilish mezoni
Boshlang‘ich nusxa	Mode va Counter, tur va ma’lumot	Nusxa o‘qiladi, qiymatlar aniq
Mode va Counter o‘zgarishi	Holat farqi, mos yozish hodisasi	Kalit va yozuvchi jarayon mos
Marker qo‘shilishi	Yangi qiymat va tegishli telemetriya	Yangi yozuv alohida ajratilgan
.reg importi	Mode va Counter tiklangan, Marker qolgan	Import chegarasi ko‘rsatilgan
Marker o‘chirilishi	Tekshirilgan qiymatlar farqi yo‘q	Xulosa faqat shu doira bilan cheklangan
Audit sozlanmagan nazorat holati	4657 chiqmasligi mumkin	Bu holat xavfsizlik dalili deb olinmagan

4.6. Sun’iy ma’lumotlarda bajarilgan hisoblash tajribasi

Balli mezonning xatti-harakatini tekshirish uchun qo‘lda tuzilgan 16 ta ssenariy ishlatildi: sakkiztasi zararli deb belgilangan M1–M8, sakkiztasi qonuniy deb belgilangan B1–B8. Bu belgilar laboratoriya loyihasining berilgan shartlaridir; ular ekspert tekshirgan haqiqiy hodisalar korpusi emas. Har bir ssenariy uchun K, W, L, U, C va A belgilari oldindan berildi. Hisoblash Python muhitida bajarilib, natija jadvali dastur chiqishidan olindi.

Tajriba qora quti mahsulotni baholamaydi. U savolga javob beradi: «Bir xil formula turli kontekst belgilariga qanday qaror chiqaradi?» Windows’dan yig‘ilgan loglar yo‘qligi sababli real hodisalardagi ma’lumot yetishmasligi, sensor yo‘qotishlari, vaqt kechikishi va hujumchilar moslashuvi bu tajribada o‘lchanmaydi. Testlar vaznlarni avtomatik tanlash yoki o‘qitish uchun ishlatilmagan.

7-jadval. Hisoblash tajribasidagi sun’iy ssenariylar

ID	Ssenariy	K W L U C A	R	θ = 4 qarori
M1	Run va profil katalogidagi skript	1 1 1 1 1 0	8	Ogohlantirish
M2	IFEO va kutilmagan bajariluvchi fayl	1 1 0 1 1 0	6	Ogohlantirish
M3	Xizmat yo‘lining o‘zgartirilishi	1 1 0 1 1 0	6	Ogohlantirish
M4	Himoya siyosati va bog‘liq hodisa	1 0 0 1 1 0	4	Ogohlantirish
M5	COM yozuvi va foydalanuvchi DLL yo‘li	1 1 0 1 0 0	5	Ogohlantirish
M6	Run yozuvi va noodatiy interpretator	1 0 1 0 1 0	5	Ogohlantirish
M7	Ishonchli vosita orqali zararli o‘zgarish	1 0 0 0 1 0	3	Ajratilmadi
M8	Faqat kritik kalit belgisi mavjud	1 0 0 0 0 0	2	Ajratilmadi
B1	Tasdiqlangan foydalanuvchi yangilagichi	1 1 0 0 0 1	2	Ajratilmadi
B2	Tasdiqlangan xizmat yangilanishi	1 0 0 0 0 1	0	Ajratilmadi
B3	Oddiy interfeys sozlamasi	0 0 0 0 0 0	0	Ajratilmadi
B4	Ruxsat etilgan profil skripti	1 1 1 0 0 1	4	Ogohlantirish
B5	Ruxsati tizimda qayd etilmagan ilova	1 1 0 1 0 0	5	Ogohlantirish
B6	Tasdiqlangan siyosat yangilanishi	1 0 0 0 0 1	0	Ajratilmadi
B7	Kritik bo‘lmagan ilova konfiguratsiyasi	0 1 0 1 0 0	3	Ajratilmadi
B8	Qo‘shimcha belgisi yo‘q qonuniy Run yozuvi	1 0 0 0 0 0	2	Ajratilmadi

Jadvaldagi belgilar aynan K W L U C A tartibida yozilgan. $\theta = 4$ chegarasida $R \geq 4$ bo‘lgan ssenariy tekshiruvga ajratiladi. B4 holati tasdiqlangan bo‘lsa ham kritik kalit, profilga yozish mumkinligi va interpretator belgilarining yig‘indisi tufayli ogohlantirish beradi. B5 holatida esa ruxsat haqidagi axborot tizimda qayd etilmagani ortiqcha shubha tug‘diradi. Demak, qoidaning xatosi ba’zan yetarli kontekst yo‘qligidan kelib chiqadi.

M7 va M8 holatlari past ball olgani uchun o‘tkazib yuboriladi. Ular zararli harakatning har doim noodatiy fayl yoki noma’lum yozuvchi jarayonga ega bo‘lmasligini modellashtiradi. Shu sababli ishonchli dastur nomini umumiy istisnoga aylantirish va bitta balli mezonni yagona himoya sifatida ishlatish tavsiya etilmaydi. Qo‘shimcha qat’iy qoidalar, tarixiy profil va jarayon zanjiri ushbu kamchilikni kamaytirish yo‘nalishlaridir.

4.7. Baholash mezonlari va natijalarni talqin qilish

TP — zararli deb belgilangan va ogohlantirilgan holat; FP — qonuniy bo‘lsa ham ogohlantirilgan holat; TN — qonuniy va ogohlantirilmagan holat; FN — zararli deb belgilangan, ammo o‘tkazib yuborilgan holat. Precision ogohlantirishlar ichidagi to‘g‘ri ulushni, recall esa zararli deb belgilangan holatlardan topilgan ulushni bildiradi.

Precision = TP / (TP + FP)

Recall = TP / (TP + FN)

F1 = 2 × Precision × Recall / (Precision + Recall)

FPR = FP / (FP + TN)

Quyidagi kod tekshirishning hisoblash qismini beradi. cases ro‘yxatidagi har bir element (yorliq, K, W, L, U, C, A) tartibida tuziladi; qiymatlar 7-jadvaldan olinadi. 1 — zararli deb belgilangan, 0 — qonuniy ssenariyni ifodalaydi. Dastur registrga murojaat qilmaydi.

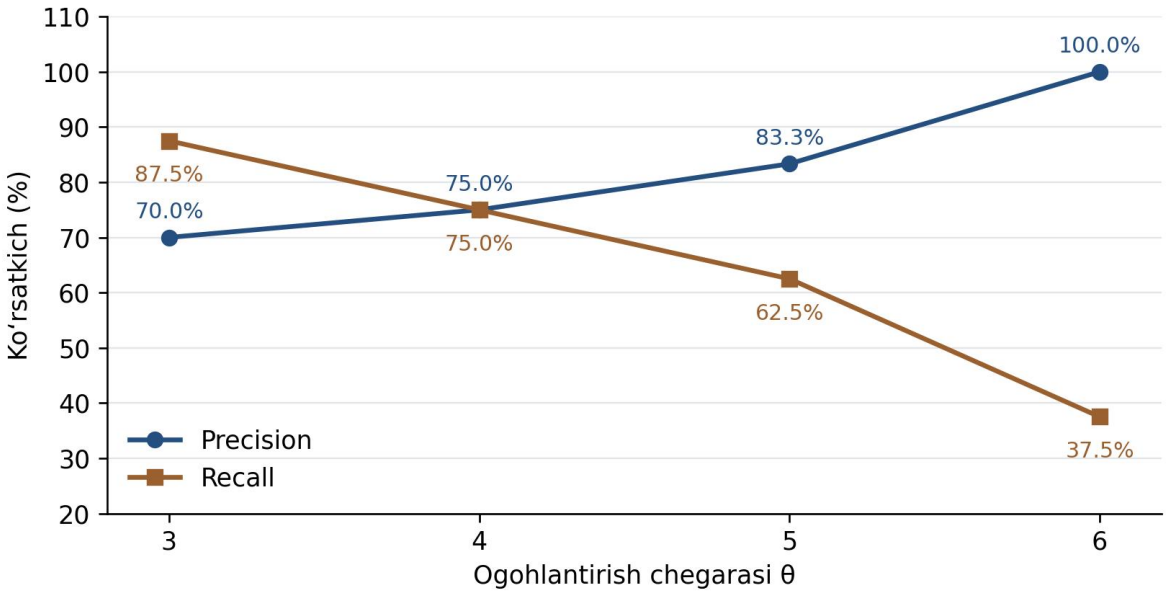
```
def score(bits):
k, w, l, u, c, a = bits
return max(0, 2*k + 2*w + 2*l + u + c - 2*a)
def evaluate(cases, threshold=4):
tp = fp = tn = fn = 0
for label, *bits in cases:
alert = score(bits) >= threshold
tp += int(alert and label == 1)
fp += int(alert and label == 0)
tn += int(not alert and label == 0)
fn += int(not alert and label == 1)
p = tp / (tp + fp) if tp + fp else 0
r = tp / (tp + fn) if tp + fn else 0
f1 = 2*p*r / (p+r) if p+r else 0
return tp, fp, tn, fn, p, r, f1
```

6-listing. Balli mezon natijalarini hisoblash

8-jadval. Turli chegaralarda hisoblangan natijalar

θ	TP / FP / TN / FN	Precision	Recall	F1
3	7 / 3 / 5 / 1	70,0%	87,5%	77,8%
4	6 / 2 / 6 / 2	75,0%	75,0%	75,0%
5	5 / 1 / 7 / 3	83,3%	62,5%	71,4%
6	3 / 0 / 8 / 5	100,0%	37,5%	54,5%

θ = 4 holatida TP = 6, FP = 2, TN = 6 va FN = 2; precision = recall = F1 = 0,75, FPR = 0,25. θ = 3 holatida ko‘proq zararli ssenariy topiladi, biroq uchta qonuniy ssenariy ham ogohlantiriladi. θ = 6 da bu kichik to‘plamdagi FP nol bo‘ladi, ammo sakkiz zararli ssenariydan beshtasi o‘tkazib yuboriladi. Shuning uchun faqat precision ko‘rsatkichiga qarab tizimni «mukammal» deb baholash noto‘g‘ri.



3-rasm. Sun’iy ssenariylarda chegara o‘zgarganda precision va recall

To‘plam ataylab teng ikki sinfga ajratilgan. Haqiqiy ish joyida hodisalar soni va zararli holatlar ulushi boshqacha bo‘ladi, shuning uchun bu precision qiymatlarini ishlab chiqarish muhitiga ko‘chirish mumkin emas. Ssenariylar qo‘lda tanlanganligi sababli ulardan umumiy statistik ishonch oralig‘i chiqarilmadi. Ushbu natija modelning mantiqiy cheklovlarini ko‘rsatadi; real baholash uchun mustaqil, vaqt bo‘yicha ajratilgan va ishonchli belgilangan hodisalar to‘plami zarur.

5. ZARARLI O‘ZGARISHLARNI BARTARAF ETISH VA OLDINI OLISH

5.1. Dalilni saqlash va hodisa doirasini aniqlash

Aniqlangan yozuvni darhol o‘chirish undan oldingi holat va sababni yo‘qotishi mumkin. Birinchi navbatda kalit, qiymat turi va ma’lumoti, foydalanuvchi, tegishli jarayon, fayl yo‘li, loglar hamda olish vaqti qayd etiladi. Faol zarar davom etayotgan bo‘lsa, dalil yig‘ish bilan birga zararni cheklash zarurati baholanadi. NIST yondashuvi javob berish va tiklashni xavfni boshqarishning uzluksiz qismi sifatida ko‘radi [32].

Hodisa kartasida «aniqlangan fakt», «taxmin» va «bajarilgan amal» alohida yoziladi. Masalan, «Run qiymati profil katalogidagi faylga ishora qiladi» — fakt; «bu fayl zararli bo‘lishi mumkin» — taxmin; «yozuv vaqtincha o‘chirildi» — bajarilgan amal. Bu ajratish keyingi mutaxassisga tekshiruvni davom ettirish va qaror sababini baholash imkonini beradi.

Qurilmani tarmoqdan ajratish ehtiyoji jarayon faolligi, tarqalish xavfi va xizmatning uzluksizligi bilan baholanadi. Faol hodisada foydalanuvchini qayta kirishga majbur qilish yoki qurilmani darhol qayta yuklash ayrim dalillarni yo‘qotishi mumkin. Aksincha, xavfli jarayonni cheklamasdan uzoq kuzatish ham zarar yetkazishi mumkin. Javob harakati texnik vaziyatga mos tanlanadi va sababi hujjatlashtiriladi.

5.2. To‘g‘ri tiklash usulini tanlash

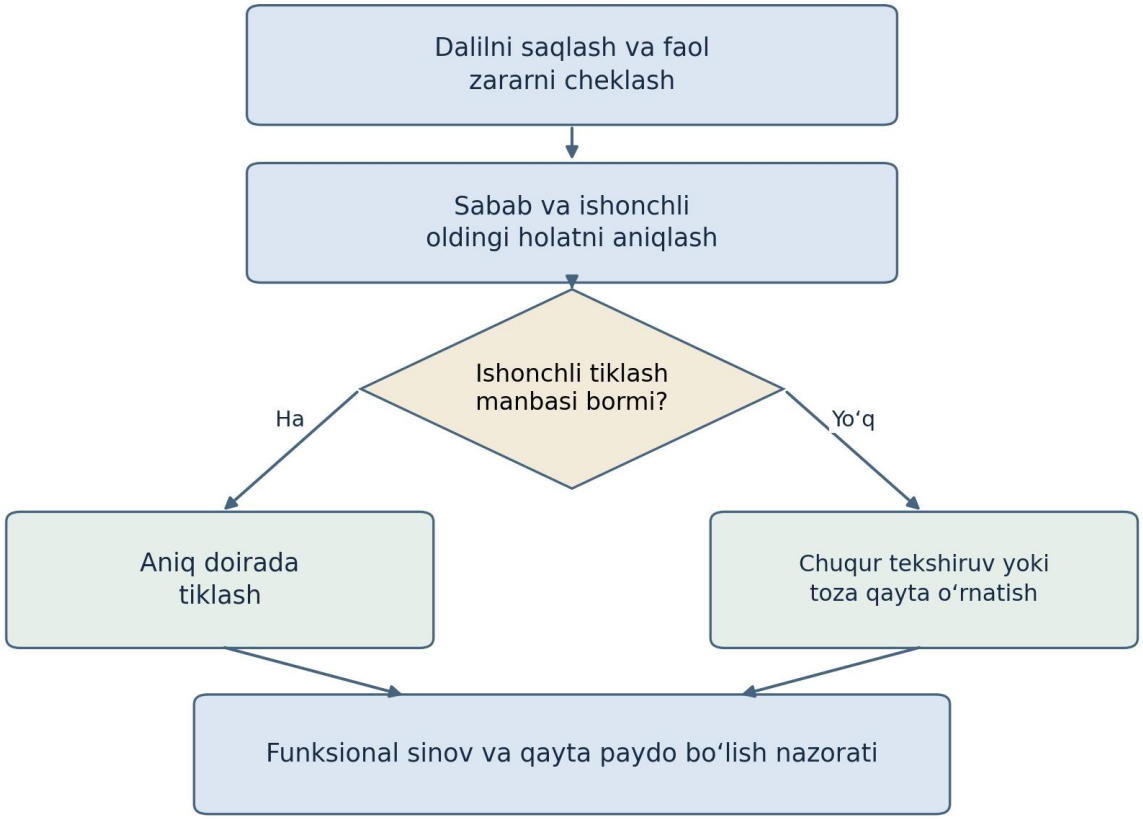
Tiklashning manbasi aniqlangan zararli holatdan oldingi ishonchli konfiguratsiya bo‘lishi kerak. Boshqa kompyuterdan tasodifiy ko‘chirilgan registr fayli Windows yig‘masi, dastur versiyasi va qurilma roliga mos kelmasligi mumkin. Domen yoki MDM orqali boshqariladigan sozlama mahalliy tahrirdan

keyin qayta yozilishi ehtimoli hisobga olinadi. Bunday vaziyatda tuzatish tegishli boshqaruv manbasida bajariladi.

reg save va reg restore kalit yoki hive darajasidagi saqlash va tiklash uchun xizmat qiladi [27, 28]. Bular .reg matnli importidan boshqa mexanizmdir. Faol tizim hive'larini tiklashda huquqlar, foydalanilayotgan kalitlar va tiklash muhiti bo'yicha cheklovlar mavjud; bunday operatsiya o'quv misolidagi oddiy qiymatni tuzatish bilan teng emas. Keng ko'lamli tizim shikastlanishida tasdiqlangan zaxira yoki toza qayta o'rnatish rejasiga murojaat qilinadi.

9-jadval. Tiklash usullarini tanlash

Usul	Qachon qo'llash mumkin	Chegarasi
Bitta qiymatni tuzatish	Eski to'g'ri tur va ma'lumot ma'lum bo'lsa	Boshqa persistence nuqtalarini tuzatmaydi
Aniq yangi qiymatni o'chirish	Yozuvning hodisada qo'shilgani tasdiqlansa	Ishlayotgan jarayonni tugatmaydi
.reg import	Cheklangan qiymatlarni qayta yozish uchun	Keyin qo'shilgan yozuvlarni umumiy tarzda olib tashlamaydi
Hive yoki kalit nusxasidan tiklash	Mos, ishonchli nusxa va tiklash tartibi bo'lsa	Noto'g'ri doira tizim ishlashini buzishi mumkin
Boshqaruv siyosatini tiklash	Sozlama GPO yoki MDM orqali boshqarilsa	Siyosat tarqalishi va amaldagi holat tekshiriladi
Toza qayta o'rnatish	Keng kompрometatsiya yoki ishonchni tiklash imkonsiz bo'lsa	Ma'lumot, identifikator va xizmatlarni qayta tiklash rejasi kerak



4-rasm. Dalilga asoslangan bartaraf etish va qayta tekshirish qarorlari

5.3. Sababni bartaraf etish va qayta paydo bo‘lishni tekshirish

Zararli qiymatni yozib turadigan jarayon faol qolsa, o‘chirilgan yozuv qayta paydo bo‘lishi mumkin. Shu sababli manba jarayon, bog‘liq xizmat, fayl va boshqa ishga tushish nuqtalari birgalikda tekshiriladi. Qaror faqat bir xil nomli yozuv yo‘qolganiga emas, zararli bajarilish zanjiri uzilganiga asoslanadi. Qaysi fayl yoki xizmatga tegilgan bo‘lsa, uning qonuniy vazifasiga ta’sir ham baholanadi.

Microsoft Defender Offline odatiy Windows ish muhitidan tashqarida tekshiruv o‘tkazishga yordam beradi va qurilmani qayta ishga tushiradi [31]. Uni boshlashdan oldin ishlar saqlanadi hamda zarur dalillar yig‘iladi. Oflayn tekshiruv foydali qo‘shimcha vosita bo‘lsa ham, u barcha siyosat va konfiguratsiyani kerakli qiymatga avtomatik qaytaradi degan kafolat yo‘q.

Tiklashdan so‘ng registr qayta o‘qiladi, muhim ilovalar ishlashi tekshiriladi va boshqaruv siyosati yangilanganidan keyin ham to‘g‘ri holat saqlanishi kuzatiladi. Qayta kirish yoki qayta yuklash sinovi faqat hodisa cheklangandan va tiklash rejasi tayyor bo‘lgandan keyin bajariladi. Kuzatuv davomiyligi ilovaning ishga tushish shartlariga mos tanlanadi; barcha muhit uchun bitta universal muddat belgilanmaydi.

5.4. Monitoringni markazlashtirish va dashboard

Bir nechta kompyuter uchun loglarni markaziy saqlash va qidirish foydali. Mahalliy agent ishlayotganini, oxirgi hodisa kelgan vaqtni va kuzatiladigan qurilmalar qamrovini alohida ko‘rsatish kerak. Faqat «zararli hodisalar soni: 0» yozuvi bilan cheklangan dashboard agent uzilib qolgan vaziyatni yashirishi mumkin. Ma’lumot kelmayotgan qurilma xavfsiz qurilmaga tenglashtirilmaydi.

Tavsiya etilayotgan dashboard hodisa kartasida vaqt, qurilma, SID, kalit, qiymat nomi, amal, jarayon, baholash sababi va tekshiruv holatini ko‘rsatadi. Holatlar «yangi», «tekshirilmoqda», «qonuniy deb tasdiqlandi», «bartaraf etildi» va «qayta tekshirildi» kabi aniq ma’noga ega bo‘ladi. «Bartaraf etildi» belgisi avtomatik ravishda «yopildi» degani emas; qayta tekshirish natijasi ham bo‘lishi kerak.

Loglarni saqlash muddati va ulardan foydalanish huquqi tashkilot ehtiyojiga mos belgilanadi. Registrda yoki buyruq argumentlarida maxfiy sozlamalar bo‘lishi mumkin. Shu sababli tahlilchi uchun kerakli dalil saqlangan holda kirish huquqi cheklanadi; ochiq hisobotlarga shaxsiy yo‘llar yoki maxfiy qiymatlar keraksiz ko‘chirilmaydi. Qoidalar, istisnolar va konfiguratsiya versiyalari ham tarix bilan saqlanadi.

5.5. Oldini olish va boshqaruv intizomi

Eng kam huquq tamoyili oddiy foydalanuvchining tizim miqyosidagi konfiguratsiyaga ta’sirini cheklaydi. Biroq HKCU darajasidagi yozuvlar mavjudligi sababli administrator huquqi yo‘qligi barcha persistence xavfini yo‘qotmaydi. Kritik kalitlar ruxsatini o‘zgartirishdan oldin dasturlar ehtiyoji va meroslanish tekshiriladi; tizim bo‘limlaridan yozish huquqini yalpi olib tashlash ishlashga zarar yetkazishi mumkin.

Dastur yangilanishlari uchun tasdiqlangan o‘zgarishlar ro‘yxati yuritilsa, monitoring shovqini aniqroq tushuntiriladi. Istisno mahsulot nomi bilangina emas, qurilma guruhi, bajariluvchi yo‘l, imzo, kutilgan kalitlar va vaqt doirasi bilan chegaralanadi. Istisnoga amal qilish muddati ham belgilanadi. Tasdiqlangan fayl yoki jarayon nomi hujumchi tomonidan suiiste’mol qilinishi mumkinligi sababli uning keyingi xatti-harakati kuzatuvdan chiqarilmaydi.

5.6. Ishlash sifati va tadqiqot cheklovlari

Monitoring sifati faqat nechta ogohlantirish topilgani bilan baholanmaydi. Qamrab olingan kritik kalitlar ulushi, agent uzilishlari, hodisa kelish kechikishi, tekshiruv vaqti, qayta paydo bo‘lish holatlari va tiklashdan keyingi funksional xatolar ham o‘lchanadi. Aniqlash kechikishini hisoblash uchun hodisa va qabul qilish vaqtlarining ma’nosi hamda soatlarning muvofiqligi oldindan belgilanishi kerak.

Mazkur ishning empirik chegarasi — 16 ta qo‘lda tuzilgan sun’iy ssenariy. Natijalar real zararli dasturlar kolleksiyasi, tashkilot trafigi yoki turli Windows versiyalarida to‘plangan loglarga asoslanmaydi. PowerShell va Sysmon listinglari rasmiy interfeyslarga tayangan laboratoriya protokoli bo‘lib, ushbu ish doirasida Windows qurilmasida bajarilib tasdiqlangan deb hisoblanmaydi. Kelgusi tekshiruvda protokol alohida VMda bajarilib, xom EVTX va PML dalillari, konfiguratsiya versiyalari hamda mustaqil belgilangan hodisalar to‘plami yig‘ilishi lozim.

XULOSA

Windows registridagi zararli o‘zgarishlarni aniqlash konfiguratsiya farqini uning sababi va oqibati bilan bog‘lashni talab qiladi. Ishda registr tuzilishi, qiymat turlari, foydalanuvchi konteksti, ruxsatlar va 32 hamda 64 bitli ko‘rinishlarni hisobga oluvchi yondashuv ishlab chiqildi. Bu omillar to‘g‘ri qayd etilmasa, turli foydalanuvchilarning yozuvlari aralashishi yoki muhim o‘zgarish kuzatuvdan chetda qolishi mumkin.

Run, xizmatlar, Winlogon, IFEO, COM va himoya sozlamalari ustuvor tekshiruv nuqtalaridir. Ularning qonuniy qo‘llanishi ham mavjudligi sababli xavflilik qarori jarayon zanjiri, fayl xususiyatlari va

tasdiqlangan ma’muriy ish bilan asoslanishi kerak. Bazaviy holat nima o‘zgarganini, hodisa telemetriyasi esa o‘zgarishning vaqti va manbasini tushuntiradi. Audit qamrovi tekshirilmaguncha hodisa yo‘qligi xavfsizlik isboti emas.

Taklif etilgan laboratoriya muhim tizim sozlamalariga tegmasdan registrga yozish, farqlarni ajratish va aniq tiklashni o‘rganishga xizmat qiladi. .reg importidan keyin yangi qiymat qolishi mumkinligi qayta tekshirish zarurligini ko‘rsatadi. Faqat tekshirilgan qiymatlarning mosligi butun kompyuter tozalanganini tasdiqlamaydi.

16 ta sun’iy ssenariydagi hisoblashda $\theta = 4$ uchun precision va recall 0,75 bo‘ldi. Chegarani oshirish noto‘g‘ri ogohlantirishlarni kamaytirib, o‘tkazib yuborilgan holatlarni ko‘paytirdi. Bu natijalar real zararli dasturlarni aniqlash ko‘rsatkichi sifatida umumlashtirilmaydi; mustaqil ma’lumotlar va haqiqiy Windows loglarida tekshirish zarur.

Amaliy bartaraf etish dalilni saqlash, sababni aniqlash, ishonchli oldingi holatni tanlash, aniq doirada tiklash va qayta paydo bo‘lishni kuzatishdan iborat. Ushbu bosqichlar birgalikda bajarilganda monitoring natijasi tekshiriladigan xavfsizlik qaroriga aylanadi.

FOYDALANILGAN ADABIYOTLAR

1. Elektron manbalarga murojaat sanasi: 18.11.2026. Microsoft Learn va MITRE ATT&CK sahifalarining amaldagi matni tekshirildi.
2. Microsoft. Structure of the Registry. https://learn.microsoft.com/en-us/windows/win32/sysinfo/structure-of-the-registry
3. Microsoft. Predefined Keys. https://learn.microsoft.com/en-us/windows/win32/sysinfo/predefined-keys
4. Microsoft. Registry Hives. https://learn.microsoft.com/en-us/windows/win32/sysinfo/registry-hives
5. Microsoft. Registry value types. https://learn.microsoft.com/en-us/windows/win32/sysinfo/registry-value-types
6. Microsoft. 32-bit and 64-bit Application Data in the Registry. https://learn.microsoft.com/en-us/windows/win32/sysinfo/32-bit-and-64-bit-application-data-in-the-registry
7. Microsoft. HKEY_CLASSES_ROOT Key. https://learn.microsoft.com/en-us/windows/win32/sysinfo/hkey-classes-root-key
8. Microsoft. Registry Key Security and Access Rights. https://learn.microsoft.com/en-us/windows/win32/sysinfo/registry-key-security-and-access-rights
9. Microsoft. Run and RunOnce Registry Keys. https://learn.microsoft.com/en-us/windows/win32/setupapi/run-and-runonce-registry-keys
10. MITRE ATT&CK. Registry Run Keys / Startup Folder — T1547.001. https://attack.mitre.org/techniques/T1547/001/
11. MITRE ATT&CK. Windows Service — T1543.003. https://attack.mitre.org/techniques/T1543/003/
12. MITRE ATT&CK. Image File Execution Options Injection — T1546.012. https://attack.mitre.org/techniques/T1546/012/
13. MITRE ATT&CK. Component Object Model Hijacking — T1546.015. https://attack.mitre.org/techniques/T1546/015/
14. MITRE ATT&CK. Winlogon Helper DLL — T1547.004. https://attack.mitre.org/techniques/T1547/004/

15. MITRE ATT&CK. Modify Registry — T1112. https://attack.mitre.org/techniques/T1112/
16. Microsoft Sysinternals. Process Monitor. https://learn.microsoft.com/en-us/sysinternals/downloads/procmon
17. Microsoft Sysinternals. Autoruns. https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns
18. Microsoft Sysinternals. Sysmon. https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
19. Microsoft. Sysmon events. https://learn.microsoft.com/en-us/windows/security/operating-system-security/sysmon/sysmon-events
20. Microsoft. Audit Registry. https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/audit-registry
21. Microsoft. 4657 A registry value was modified. https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4657
22. Microsoft. Command line process auditing. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing
23. Microsoft. DeviceRegistryEvents table. https://learn.microsoft.com/en-us/defender-xdr/advanced-hunting-deviceregistryevents-table
24. Microsoft. Get-AuthenticodeSignature. https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.security/get-authenticodesignature
25. Microsoft. Get-WinEvent. https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.diagnostics/get-winevent
26. Microsoft. reg export. https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/reg-export
27. Microsoft. reg import. https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/reg-import
28. Microsoft. reg save. https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/reg-save
29. Microsoft. reg restore. https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/reg-restore
30. Microsoft. Tamper protection overview. https://learn.microsoft.com/en-us/defender-endpoint/prevent-changes-to-security-settings-with-tamper-protection
31. Microsoft. Protect Microsoft Defender Antivirus exclusions with tamper protection. https://learn.microsoft.com/en-us/defender-endpoint/tamper-protection-antivirus-exclusions
32. Microsoft. Microsoft Defender Offline scan in Windows. https://learn.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/microsoft-defender-offline
33. Nelson A., Rekhi S., Souppaya M., Scarfone K.. Incident Response Recommendations and Considerations for Cybersecurity Risk Management — NIST SP 800-61 Rev. 3. April 2025. https://doi.org/10.6028/NIST.SP.800-61r3
34. Microsoft. wevtutil. https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/wevtutil
35. Microsoft. RegQueryInfoKeyW function. https://learn.microsoft.com/en-us/windows/win32/api/winreg/nf-winreg-regqueryinfokeyw
36. Microsoft. Get-Acl. https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.security/get-acl