



Система мониторинга событий ИБ

Дмитрий Донской
Директор по развитию

Современная таргетированная атака = спецоперация



Векторы атак. 14 тактик с более чем 500 техник взлома

MATRICES

- Enterprise
- PRE
- Windows
- macOS
- Linux
- Cloud
- AWS
- GCP
- Azure
- Office 365
- Azure AD
- SaaS
- Network
- Mobile
- Android
- iOS
- ICS

Home > Matrices > Enterprise

Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, PRE, AWS, GCP, Azure, Azure AD, Office 365, SaaS, Network.

[View on the ATT&CK® Navigator](#)
[About the Enterprise domain](#)
[Version Permalink](#)

layouts show sub-techniques hide sub-techniques help

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
10 techniques	6 techniques	9 techniques	10 techniques	18 techniques	12 techniques	37 techniques	15 techniques	25 techniques	9 techniques	17 techniques	16 techniques	9 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Size Limit (1)
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (12)	Access Token Manipulation (5)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocols (1)
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (12)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over Cloud Channels (1)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Scheduled Task/Job (6)	Browser Extensions	Boot or Logon Initialization Scripts (5)	Direct Volume Access	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Data from Configuration Repository (2)	Exfiltration Over Network Channels (1)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Create or Modify System Process (4)	Domain Policy Modification (2)	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Dynamic Resolution (3)	Exfiltration Over Network Media Channels (1)
Search Closed Sources (2)		Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Domain Policy Modification (2)	Execution Guardrails (1)	Man-in-the-Middle (2)	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories (2)	Encrypted Channel (2)	Exfiltration Over Physical Media Channels (1)
Search Open Technical Databases (5)		Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Event Triggered Execution (15)	Exploitation for Defense Evasion	Modify Authentication Process (4)	File and Directory Discovery	Taint Shared Content	Data from Local System	Fallback Channels	Exfiltration Over Service Channels (1)
Search Open Websites/Domains (2)		Valid Accounts (4)	User Execution (2)	Create or Modify System Process (4)	Event Triggered Execution (15)	File and Directory Permissions Modification (2)	Network Sniffing	Network Service Scanning	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Ingress Tool Transfer	Exfiltration Over Network Media Channels (1)
Search Victim-Owned Websites			Windows Management Instrumentation	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Hide Artifacts (7)	Network Share Discovery	Network Share Discovery		Data from Removable Media	Multi-Stage Channels	Schedule Task (1)
				External Remote Services	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Network Sniffing	Password Policy Discovery		Data from Removable Media	Non-Application Layer Protocol	Schedule Task (1)
				Hijack Execution Flow (11)	Process Injection (11)	Impair Defenses (7)	OS Credential Dumping (3)	Peripheral Device Discovery		Data Staged (2)	Non-Standard Port	Transfer Data to Cloud Storage (1)
						Indicator Removal on Host (6)	Steal Application Access Token					

Как своевременно обнаруживать таргетированные атаки?



Необходимо отслеживать признаки нарушения ИБ



Авторизация: как успешная,
так и неуспешная



Срабатывания
антивирусного ПО,
IDS\IPS, DLP, СЗИ



Бесконтрольный выход в
Internet и соцсети



Подозрительные
запросы к СУБД



Нетипичное
поведение
пользователя



Удаленный доступ

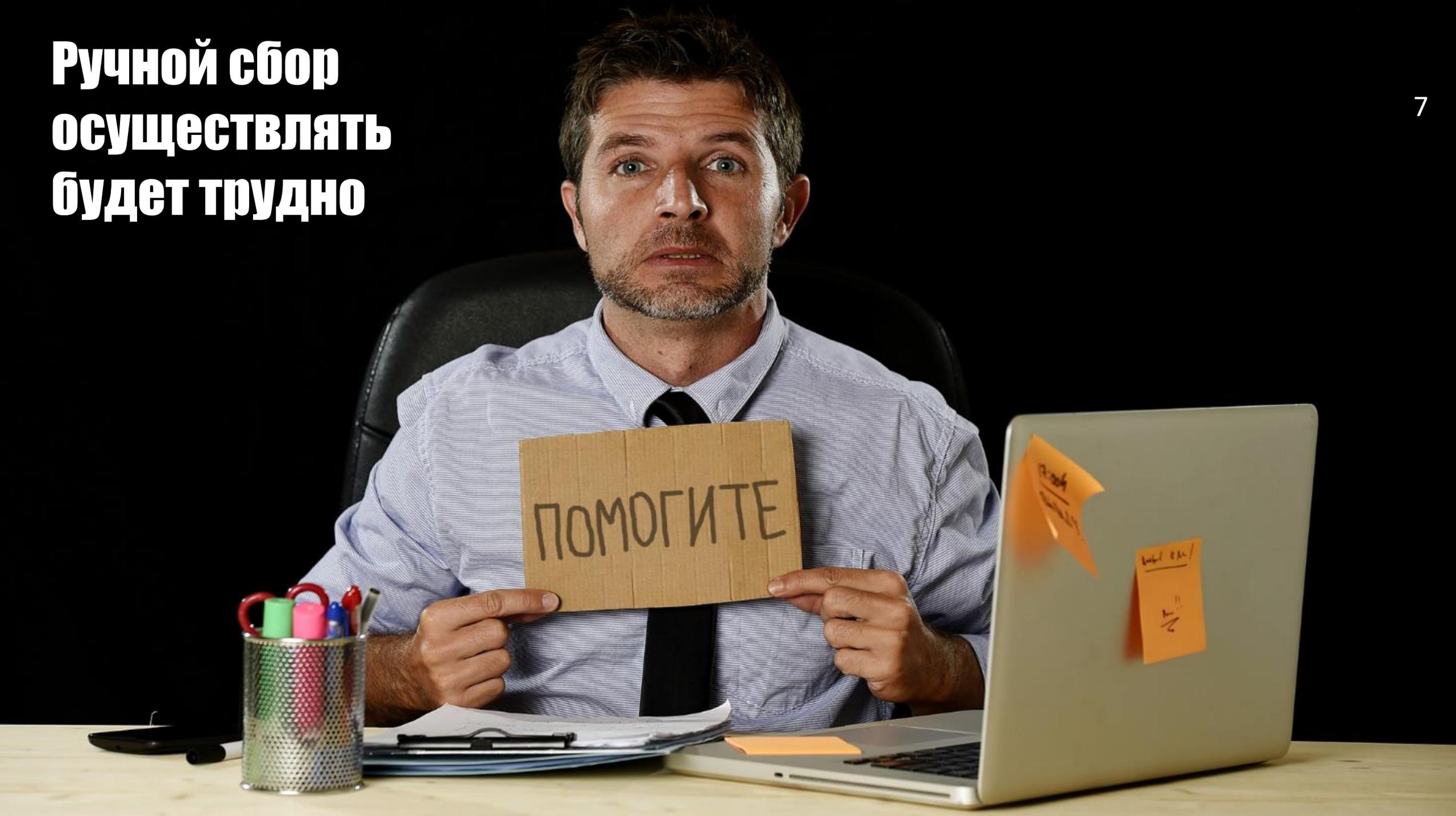
Для этого надо осуществлять мониторинг **критичных** сегментов инфраструктуры

Соответствующее требование
включено в:

Приказ ФСТЭК России N 17
Приказ ФСТЭК России N 21
Приказ ФСТЭК России N 31
Приказ ФСТЭК России N 239



Ручной сбор осуществлять будет трудно



```

vmware - Notepad
File Edit Format View Help
Apr 27 09:55:34: vmx| Log for VMware workstation pid=2548 version=5.1
Apr 27 09:55:34: vmx| Command line: "C:\Program Files\VMware\VMware v
Apr 27 09:55:34: vmx| UI Connecting to pipe '\\.\pipe\vmxc28be6e39c18
Apr 27 09:55:34: vmx| CPU #0 TSC = 7336583627359
Apr 27 09:55:34: vmx| CPU #1 TSC = 7336583626617
Apr 27 09:55:34: vmx| TSC delta 742
Apr 27 09:55:34: vmx| VMMon_getkHzEstimate: calculated 2793030 khz
Apr 27 09:55:34: vmx| cpuids[0].id81.ecx = 0x0
Apr 27 09:55:34: vmx| cpuids[1].id81.ecx = 0x0
Apr 27 09:55:34: vmx| pcpu #0 CPUID numEntries=5 Genuntelnei
Apr 27 09:55:34: vmx| pcpu #0 CPUID version=0xf34 id1.edx=0xbfebfbff
Apr 27 09:55:34: vmx| pcpu #0 CPUID id80.eax=80000008 id81.edx=0x0 id
Apr 27 09:55:34: vmx| pcpu #1 CPUID numEntries=5 Genuntelnei
Apr 27 09:55:34: vmx| pcpu #1 CPUID version=0xf34 id1.edx=0xbfebfbff
Apr 27 09:55:34: vmx| pcpu #1 CPUID id80.eax=80000008 id81.edx=0x0 id
Apr 27 09:55:34: vmx| CPUID id1.edx: 0xbfebfbff id1.ecx: 0x441d id81.
Apr 27 09:55:34: vmx| CPUID id88.ecx: 0 id88.edx: 0
Apr 27 09:55:34: vmx| ACL_InitCapabilities: here 1 (bug 63252)
Apr 27 09:55:34: vmx| changing directory to C:\virtual\XP\
Apr 27 09:55:34: vmx| Config file: C:\virtual\XP\windows XP Professio
Apr 27 09:55:34: vmx| VMXvmbdcbvmvmmxExecState: Exec state change requ
Apr 27 09:55:34: vmx| PowerOn
Apr 27 09:55:34: vmx| Host: WIN32 highest NUMA node 0
Apr 27 09:55:34: vmx| Host: WIN32 NUMA node 0, CPU mask 0x000000000000
Apr 27 09:55:34: vmx| HOST windows version 5.1, build 2600, platform
Apr 27 09:55:34: vmx| DICT --- USER PREFERENCES
Apr 27 09:55:34: vmx| DICT pref.view.navBar.type = favorites
Apr 27 09:55:34: vmx| DICT webupdate.checkLast = 1146144710

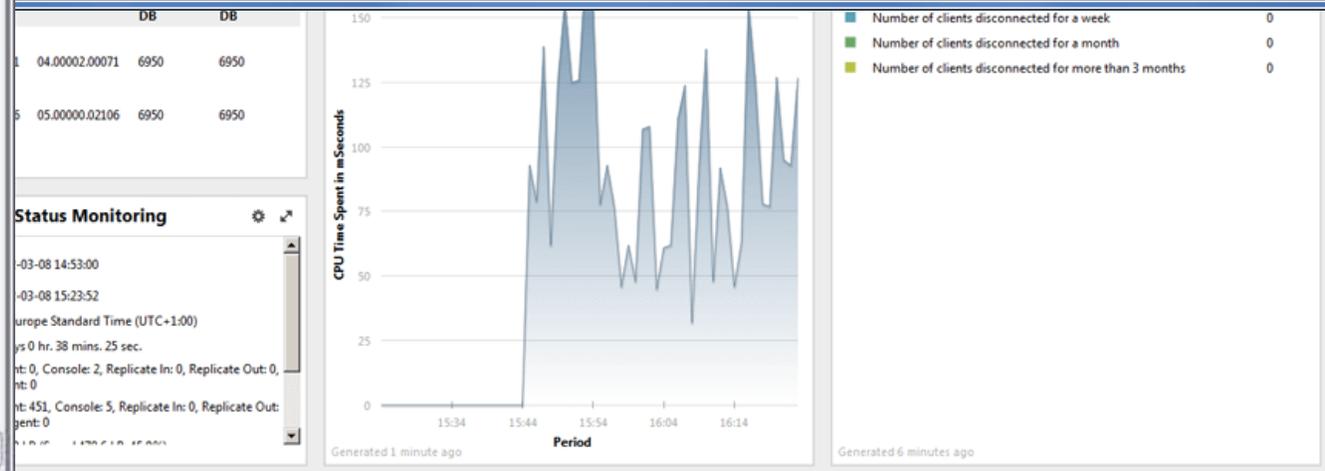
```

```

127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET / HTTP/1.1" 200 729 "-" "Mozilla/5.0
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET /icons/blank.gif HTTP/1.1" 200 431 "ht
Firefox/56.0"
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET /icons/folder.gif HTTP/1.1" 200 509 "h
Firefox/56.0"
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET /icons/text.gif HTTP/1.1" 200 513 "ht
Firefox/56.0"
127.0.0.1 - - [31/Oct/2017:11:11:38 +0530] "GET /favicon.ico HTTP/1.1" 404 500 "-" "M
127.0.0.1 - - [31/Oct/2017:11:12:05 +0530] "GET /tecmint/ HTTP/1.1" 200 787 "http://lo
"
127.0.0.1 - - [31/Oct/2017:11:12:05 +0530] "GET /icons/back.gif HTTP/1.1" 200 499 "ht
01 Firefox/56.0"
127.0.0.1 - - [31/Oct/2017:11:13:58 +0530] "GET /tecmint/Videos/ HTTP/1.1" 200 817 "h
01 Firefox/56.0"
127.0.0.1 - - [31/Oct/2017:11:13:58 +0530] "GET /icons/compressed.gif HTTP/1.1" 200 1
) Gecko/20100101 Firefox/56.0"
127.0.0.1 - - [31/Oct/2017:11:13:58 +0530] "GET /icons/movie.gif HTTP/1.1" 200 527 "h
o/20100101 Firefox/56.0"
:1 - - [31/Oct/2017:11:26:57 +0530] "GET /ravi HTTP/1.1" 404 494 "-" "Mozilla/5.0 (X
36"
:1 - - [31/Oct/2017:11:26:57 +0530] "GET /favicon.ico HTTP/1.1" 404 500 "http://loca
ome/60.0.3112.90 Safari/537.36"
:1 - - [31/Oct/2017:11:27:20 +0530] "GET /anusha HTTP/1.1" 404 496 "-" "Mozilla/5.0
37.36"

```

Source	Thread...	Severity	Event Id	Text	
12:09:25...	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 194.28.7...
12:09:28...	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 194.28.7...
12:12:40...	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 222.36.7...
12:14:55...	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 64.62.19...
12:19:08...	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 49.238.2...
12:19:10...	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 49.238.2...
12:25:54...	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 81.89.5.5...
12:28:10...	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 115.68.2...
12:28:13...	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 115.68.2...
12:35:04...	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 146.145....
12:35:06...	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 146.145....
12:37:48...	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 189.47.1...
12:37:51...	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 189.47.1...
12:59:12...	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 118.26.1...
12:59:13...	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 79.125.1...
13:19:09...	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 124.114...





**Решение:
применение
SIEM-системы**

Что такое SiEM-система?

SiEM-система – это единая точка входа событий с разных источников, и управление этими событиями

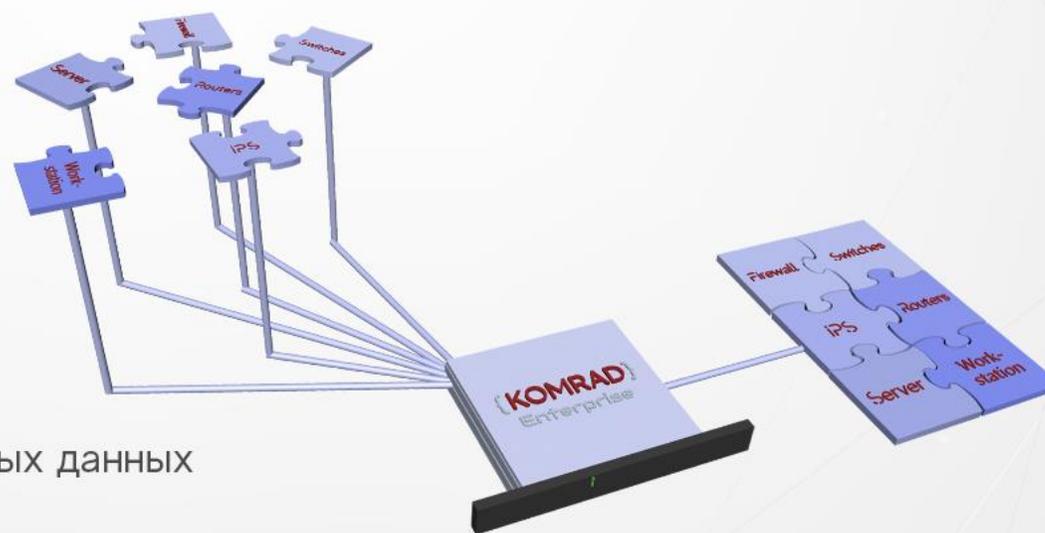
Собирает события из различных источников (Windows, Linux, IDS, DLP, СЗИ, сетевые устройства)

Анализирует поступившие события

Управляет событиями ИТ и ИБ

Предупреждает об угрозах и инцидентах

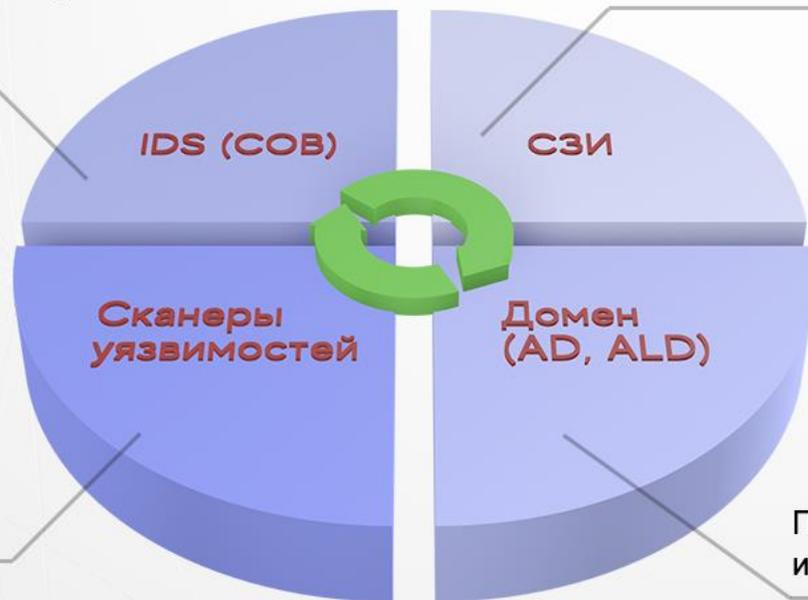
Хранит все события для просмотра детализированных данных



SiEM – централизованная система управления событиями ИБ

События бывают разными?

Распознает только сигнатуры угроз
в пакетах и протоколах



Находят уязвимости
в активах

Видят файлы, имена хостов,
контролируемые процессы

Пользователи, активные службы,
изменения конфигураций

SIEM-система КОМРАД

- Аналитический инструмент для ИТ и ИБ
- Единый центр входа всех событий
- Позволяет держать руку на пульсе всех событий
- КОМРАД собирает и выявляет – человек думает

KOMRAD Enterprise SIEM 4.0

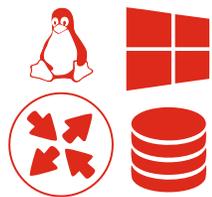
Гибкая и производительная система централизованного управления событиями информационной безопасности, совместимая с отечественными средствами защиты информации.



Отличительные особенности



Высокая
производительность



Широкий спектр
поддерживаемых
источников событий
«из коробки»



Возможность
подключения
любого
источника событий



Гибкость при создании
фильтров и директив
корреляции



Оперативное оповещение
об инциденте



Возможность автоматического
реагирования на инциденты



Возможность передачи
инцидентов
в систему ГОССОПКА



Дистрибутив под
Astra Linux и Windows

Минимальные требования к аппаратному обеспечению

- ОЗУ: 4 GB
- CPU: 2 ядра
- SDD: 100 GB



Имеющиеся коннекторы

- Astra Linux
- МЭ и СОБ «Рубикон»/«Рубикон-К»
- Сканер-ВС
- Kaspersky Security Center/
- Kaspersky Endpoint Security
- Dr.Web
- SecretNet Studio
- DallasLock
- vGate R2
- ViPNet Coordinator HW2000
- ViPNet IDS
- TLS Континент
- DeviceLock



А также:

- **Windows** (системные журналы и журналы приложений)
- **Linux** (журналы: стандартные, Auth, Dpkg, LAST, LASTB, WHO, Apport, Cups, Samba, Kernel, Qume, KVM, LibVirt, Auditd)
- **Suricata**
- **Zeek**
- **Postfix**
- **Nginx**
- **Apache HTTP-server**
- **IPtables**
- **OSquery**



Примеры директив

malware Заражение вредоносным программным обеспечением. Берутся из средств антивирусной защиты

malware distribution Распространение вредоносного программного обеспечения.
Берутся из средств антивирусной защиты

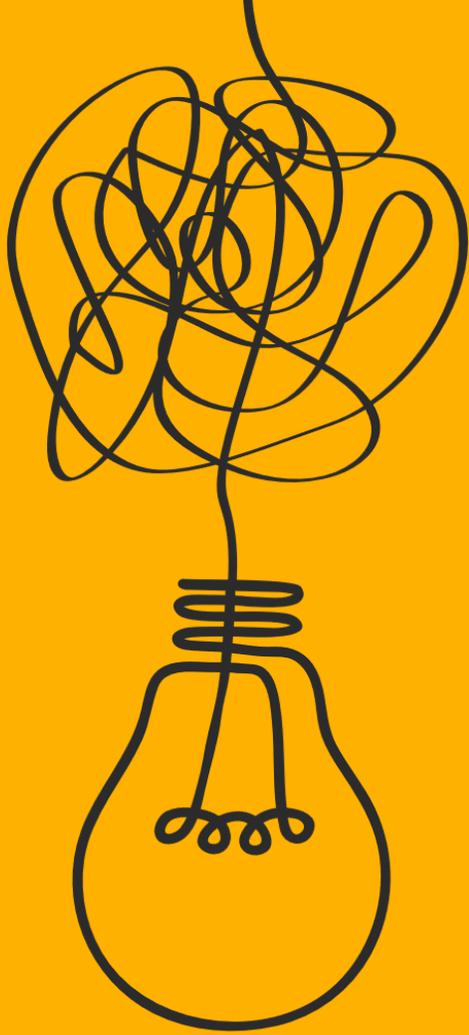
intrusion Несанкционированный доступ в систему. Берутся из журналов аутентификации

intrusion attempt Попытки несанкционированного доступа в систему или к информации.
Берутся из журналов аутентификации

information gathering Сбор сведений с использованием ИКТ. Мониторинг событий связанных со сканированием сети и активов

abusive content Распространение информации с неприемлемым содержанием.
Данные берутся из DLP систем

vulnerability Уязвимость. Данные берутся из сканеров уязвимостей



SIEM-система может
быть простой в использовании

ПРЕИМУЩЕСТВА, КАК ЕСТЬ

- 10 Нет ничего лишнего, за что нужно доплачивать
- 10 Модульная система, покупаете то, что нужно
- 10 Возможность купить минимальную конфигурацию и расширять функционал по мере потребностей
- 10 Минимальная стоимость владения после покупки
- 10 Оперативное принятие мер на изменение требований регуляторов к реагированию на инциденты



- 10 Не требуются высокоспециализированные специалисты
- 10 Директивы корреляции можно писать самим
- 10 Онлайн и оффлайн курсы, вебинары, собственный учебный центр

Условия лицензирования

В отличие от большинства других SIEM-систем, дистрибутив КОМРАД работает как на коммерческих, так и открытых ОС



- ✓ Стоимость лицензии не привязана к операционной системе
- ✓ Стоимость лицензии зависит от функционала
- ✓ Стоимость лицензии зависит от наличия сертификата соответствия ФСТЭК России

Для кого мы сделали новую версию KOMRAD Enterprise SIEM?

- Средний и крупный бизнес
- Государственные структуры
- Банки и финансовые организации
- Субъекты КИИ
- Соискатели лицензии ФСТЭК России

SIEM-система должна защищать вашу инфраструктуру так же, как и антивирус!

Когда нужна SIEM-система

Обеспечение безопасности бизнеса

- Вовремя пресечь сетевые атаки и попытки компрометации ИС
- Узнать о веерных вирусных заражениях
- Заблокировать попытки несанкционированного доступа
- Выявить слабые места в инфраструктуре
- Донастроить средства защиты информации

Соответствие стандартам и требованиям регуляторов

- **ФСТЭК России**
(приказы 17,21,31,235 приказы)
- **ФинЦЕРТ**
(382-П, СТО БР ИББС-1.3-2016,
СТО БР БФБО-1.5-2018, ГОСТ Р 57580.1-2017)
- **ГосСОПКА**
(приказы ФСБ 367, 368)
- **PCI DSS**
- **ISO 27001**

5 шагов по развёртыванию SIEM

I. ПОДГОТОВИТЕЛЬНЫЙ ЭТАП

- Обследование инфраструктуры
- Формирование ТЗ и выбор функционала

II. ВНЕДРЕНИЕ/ПИЛОТ

- Установка и базовая настройка
- Настройка источников событий
- Разработка правил реагирования (корреляции)

III. ТЕСТОВАЯ ЭКСПЛУАТАЦИЯ

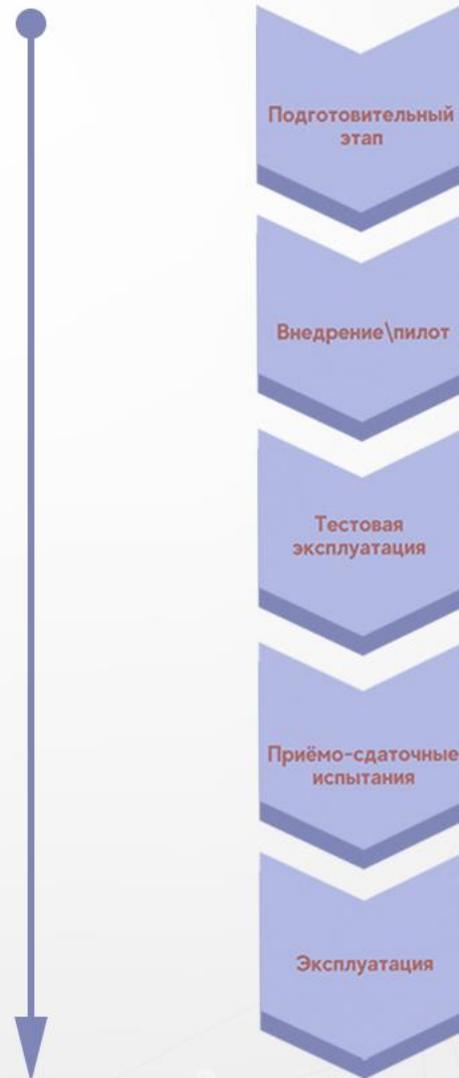
- Тонкая настройка системы
- Корректировка и дополнение правил корреляции

IV. ПРИЁМО-СДАТОЧНЫЕ ИСПЫТАНИЯ

- Проверка срабатывания правил корреляции на инциденты

V. ЭКСПЛУАТАЦИЯ

- Проведение внешних и внутренних пентестов
- Тонкая настройка средств защиты информации



КАК ПОЛУЧИТЬ ДЕМО-ВЕРСИЮ?

- ✓ Получите демо-версию, написав нам на адрес getkomrad@npo-echelon.ru
- ✓ Вступите в группу в Telegram:
<https://t.me/joinchat/DGLERFfkEY5F7SOnUmwPvg>
- ✓ Есть вопросы и предложения – пишите на partners@npo-echelon.ru





Эшелон
комплексная безопасность

Дмитрий Донской
Директор по развитию
+7 495 223-23-92 # 733
+7 909 678-60-90
+7 915 433-42-83
d.donskoy@npo-echelon.ru