

Мониторинг событий информационной безопасности на объектах КИИ с помощью KOMRAD Enterprise SIEM

Дорофеев Александр, CISSP, CISA, CISM



План

1. Ключевые требования ФСТЭК России и ФСБ России к мониторингу КИИ
2. Принцип работы SIEM-систем
3. KOMRAD Enterprise SIEM

Приказ ФСТЭК России от 25 декабря 2017 г. N 239

- АУД.4 Регистрация событий безопасности
- АУД.7 Мониторинг безопасности
- ИНЦ.0 Регламентация правил и процедур
- ИНЦ.1 Выявление компьютерных инцидентов
- ИНЦ.2 Информирование о компьютерных инцидентах
- ИНЦ.3 Анализ компьютерных инцидентов
- ИНЦ.4 Устранение последствий компьютерных инцидентов
- ИНЦ.5 Принятие мер по предотвращению повторного возникновения компьютерных инцидентов
- ИНЦ.6 Хранение и защита информации о компьютерных инцидентах

Приказ ФСБ РОССИИ от 24 июля 2018 года N 367

5. Информация, указанная в [пункте 5 Перечня](#), направляется субъектом критической информационной инфраструктуры в НКЦКИ не позднее 24 часов с момента обнаружения компьютерного инцидента.

Перечень:

5. Информация о компьютерных инцидентах, связанных с функционированием объектов критической информационной инфраструктуры:

- дата, время, место нахождения или географическое местоположение объекта критической информационной инфраструктуры, на котором произошел компьютерный инцидент;
- наличие причинно-следственной связи между компьютерным инцидентом и компьютерной атакой;
- связь с другими компьютерными инцидентами (при наличии);
- состав технических параметров компьютерного инцидента;
- последствия компьютерного инцидента.

Центр мониторинга информационной безопасности (Security Operations Center)

подразделение организации, осуществляющее мониторинг информационной безопасности и улучшающее защищенность организации путем предотвращения, обнаружения, анализа и реагирования на инциденты кибербезопасности.

SOC выступает в роли центрального командного пункта, в который стекаются события со всей ИТ-инфраструктуры.



MITRE ATT@CK (1)

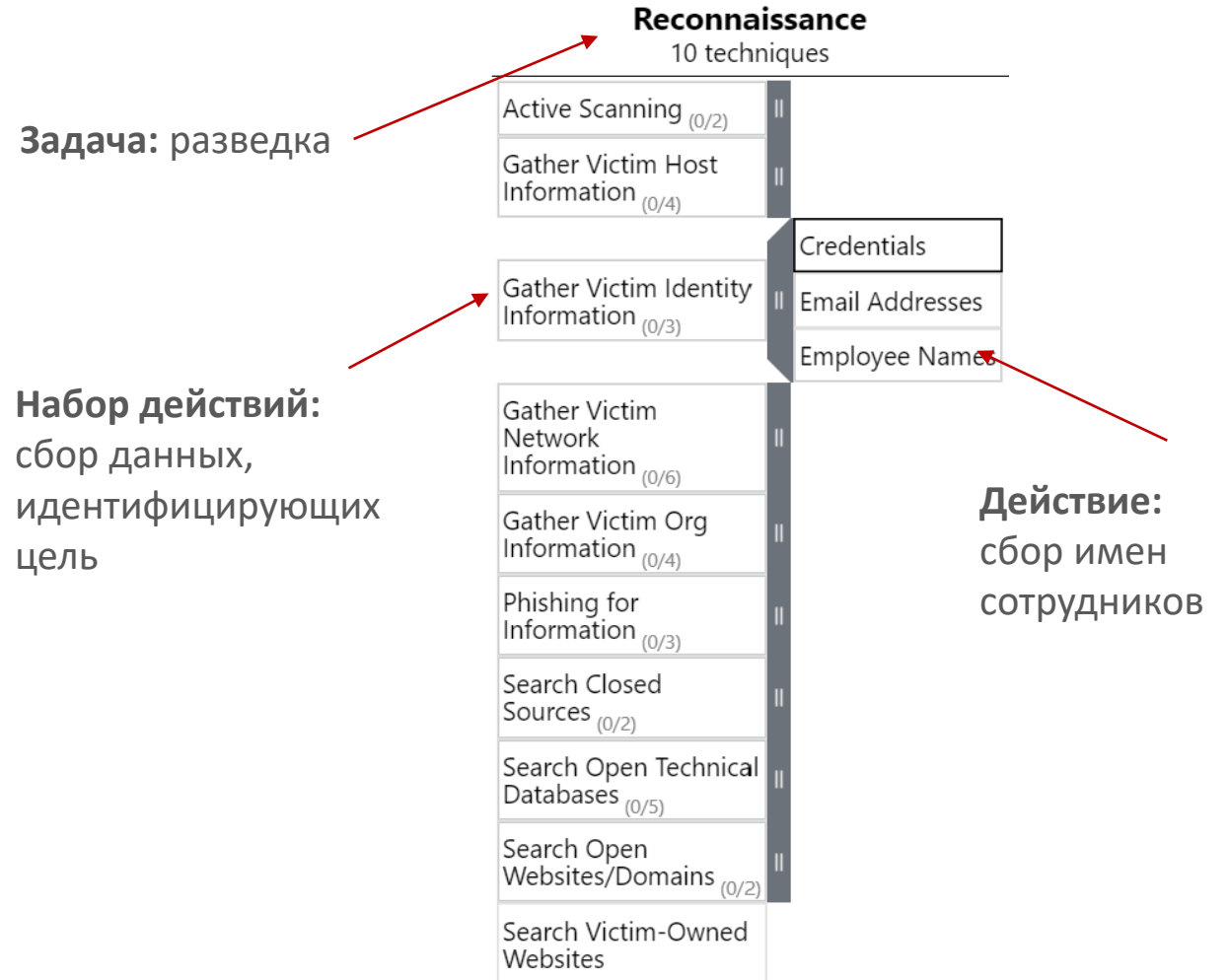
1. Reconnaissance – сбор информации о цели снаружи
2. Resource Development – подготовка ресурсов для нападения
3. Initial Access – первоначальный доступ
4. Execution – попытка запуска вредоносного ПО
5. Persistence – организация постоянного доступа к целевой инфраструктуре
6. Privilege Escalation – повышение уровня доступа
7. Defense Evasion – обход средств защиты информации

The image shows the MITRE ATT&CK Navigator interface, which is a grid-based tool for visualizing and customizing attack paths. The grid is organized into columns representing different phases of an attack, with each cell containing a specific technique and its associated icon and ID.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning (002)	Acquire Infrastructure (005)	Drive-by Compromise (001)	Command and Scripting Interpreter (004)	Account Manipulation (004)	Abuse Elevation Control Mechanism (004)	Abuse Elevation Control Mechanism (004)	Brute Force (004)	Account Discovery (004)	Exploitation of Remote Services (004)	Archive Collected Data (004)	Application Layer Protocol (004)	Automated Exfiltration (004)	Account Access Removal (004)
Gather Victim Host Information (006)	Compromise Accounts (002)	Exploit Public-Facing Application (002)	Container Administration Command (002)	BITS Jobs (002)	Access Token Manipulation (002)	Access Token Manipulation (002)	Credentials from Password Stores (002)	Application Window Discovery (002)	Internal Spearphishing (002)	Audio Capture (002)	Communication Through Removable Media (002)	Data Transfer Size Limits (002)	Data Destruction (002)
Gather Victim Identify Information (003)	Compromise Infrastructure (003)	External Remote Services (003)	Container Administration Command (003)	Boot or Logon Autostart Execution (003)	Boot or Logon Autostart Execution (003)	Boot or Logon Autostart Execution (003)	Browser Bookmarks (003)	Browser Bookmark Discovery (003)	Automated Collection (003)	Automated Collection (003)	Exfiltration Over Alternative Protocol (003)	Data Encrypted for Impact (003)	Data Encrypted for Impact (003)
Gather Victim Network Information (004)	Develop Capabilities (004)	Hardware Additions (004)	Deploy Container (004)	Boot or Logon Autostart Execution (004)	Boot or Logon Autostart Execution (004)	Boot or Logon Autostart Execution (004)	Cloud Infrastructure Discovery (004)	Cloud Infrastructure Discovery (004)	Clipboard Data Transfer (004)	Clipboard Data Transfer (004)	Data Manipulation (004)	Data Manipulation (004)	Data Manipulation (004)
Gather Victim Org Information (005)	Establish Accounts (005)	Phishing (005)	Exploitation for Client Execution (005)	Boot or Logon Initialization Scripts (005)	Boot or Logon Initialization Scripts (005)	Boot or Logon Initialization Scripts (005)	Deobfuscate/Decode Files or Information (005)	Deobfuscate/Decode Files or Information (005)	Remote Service Session Hijacking (005)	Data from Cloud Storage Object (005)	Data Encoding (005)	Exfiltration Over C2 Channel (005)	Data Encrypted for Impact (005)
Phishing for Information (007)	Obtain Capabilities (007)	Replication Through Removable Media (007)	Inter-Process Communication (007)	Browser Extensions (007)	Create or Modify System Process (007)	Create or Modify System Process (007)	Direct Volume Access (007)	Cloud Service Dashboard (007)	Remote Services (007)	Data from Configuration Repository (007)	Data Obfuscation (007)	Exfiltration Over Other Network Medium (007)	Defacement (007)
Search Closed Sources (008)	Stage Capabilities (008)	Supply Chain Compromise (008)	Native API (008)	Compromise Client Software Binary (008)	Domain Policy Modification (008)	Domain Policy Modification (008)	Domain Policy Modification (008)	Cloud Service Dashboard (008)	Replication Through Removable Media (008)	Data from Information Repositories (008)	Dynamic Resolution (008)	Exfiltration Over Other Network Medium (008)	Disk Wipe (008)
Search Open Technical Databases (009)	Trusted Relationship (009)	Valid Accounts (009)	Scheduled Task/Job (009)	Create Account (009)	Event Triggered Execution (009)	Event Triggered Execution (009)	Execution Guards (009)	Container and Resource Discovery (009)	Data from Local System (009)	File and Directory Discovery (009)	Failback Channels (009)	Exfiltration Over Physical Medium (009)	Endpoint Denial of Service (009)
Search Open Websites/Domains (010)	User Execution (010)	Windows Management Instrumentation (010)	Software Deployment Tools (010)	Create or Modify System Process (010)	Event Triggered Execution (010)	Event Triggered Execution (010)	Exploitation for Defense Evasion (010)	Domain Trust Discovery (010)	Software Deployment Tools (010)	Network Service Scanning (010)	Ingress Tool Transfer (010)	Exfiltration Over Web Service (010)	Network Denial of Service (010)
Search Victim-Owned Websites (011)	System Services (011)	System Services (011)	System Services (011)	Event Triggered Execution (011)	Event Triggered Execution (011)	Event Triggered Execution (011)	File and Directory Permissions Modification (011)	File and Directory Discovery (011)	Software Deployment Tools (011)	Network Service Scanning (011)	Multi-Stage Channels (011)	Scheduled Transfer (011)	Resource Hijacking (011)
	External Remote Services (012)	External Remote Services (012)	External Remote Services (012)	External Remote Services (012)	External Remote Services (012)	External Remote Services (012)	Hide Artifacts (012)	Network Service Scanning (012)	Software Deployment Tools (012)	Network Service Scanning (012)	Non-Application Layer-Protocol (012)	Transfer Data to Cloud Account (012)	System Shutdown/Reboot (012)
	External Remote Services (013)	External Remote Services (013)	External Remote Services (013)	External Remote Services (013)	External Remote Services (013)	External Remote Services (013)	Hijack Execution Flow (013)	Network Service Scanning (013)	Software Deployment Tools (013)	Network Service Scanning (013)	Non-Standard Port (013)	Protocol Tunneling (013)	
	External Remote Services (014)	External Remote Services (014)	External Remote Services (014)	External Remote Services (014)	External Remote Services (014)	External Remote Services (014)	Impair Defenses (014)	Network Service Scanning (014)	Software Deployment Tools (014)	Network Service Scanning (014)	Proxy (014)		
	External Remote Services (015)	External Remote Services (015)	External Remote Services (015)	External Remote Services (015)	External Remote Services (015)	External Remote Services (015)	Indicator Removal on Host (015)	Network Service Scanning (015)	Software Deployment Tools (015)	Network Service Scanning (015)	Remote Access Software (015)		
	External Remote Services (016)	External Remote Services (016)	External Remote Services (016)	External Remote Services (016)	External Remote Services (016)	External Remote Services (016)	Indirect Command Execution (016)	Network Service Scanning (016)	Software Deployment Tools (016)	Network Service Scanning (016)	Traffic Signaling (016)		
	External Remote Services (017)	External Remote Services (017)	External Remote Services (017)	External Remote Services (017)	External Remote Services (017)	External Remote Services (017)	Invalid Accounts (017)	Network Service Scanning (017)	Software Deployment Tools (017)	Network Service Scanning (017)	Web Service (017)		
	External Remote Services (018)	External Remote Services (018)	External Remote Services (018)	External Remote Services (018)	External Remote Services (018)	External Remote Services (018)	Office Application Startup (018)	Network Service Scanning (018)	Software Deployment Tools (018)	Network Service Scanning (018)	Video Capture (018)		
	External Remote Services (019)	External Remote Services (019)	External Remote Services (019)	External Remote Services (019)	External Remote Services (019)	External Remote Services (019)	Pre-OS Boot (019)	Network Service Scanning (019)	Software Deployment Tools (019)	Network Service Scanning (019)			
	External Remote Services (020)	External Remote Services (020)	External Remote Services (020)	External Remote Services (020)	External Remote Services (020)	External Remote Services (020)	Scheduled Task/Job (020)	Network Service Scanning (020)	Software Deployment Tools (020)	Network Service Scanning (020)			
	External Remote Services (021)	External Remote Services (021)	External Remote Services (021)	External Remote Services (021)	External Remote Services (021)	External Remote Services (021)	Server Software Component (021)	Network Service Scanning (021)	Software Deployment Tools (021)	Network Service Scanning (021)			
	External Remote Services (022)	External Remote Services (022)	External Remote Services (022)	External Remote Services (022)	External Remote Services (022)	External Remote Services (022)	Modify Registry (022)	Network Service Scanning (022)	Software Deployment Tools (022)	Network Service Scanning (022)			
	External Remote Services (023)	External Remote Services (023)	External Remote Services (023)	External Remote Services (023)	External Remote Services (023)	External Remote Services (023)	Modify Registry (023)	Network Service Scanning (023)	Software Deployment Tools (023)	Network Service Scanning (023)			
	External Remote Services (024)	External Remote Services (024)	External Remote Services (024)	External Remote Services (024)	External Remote Services (024)	External Remote Services (024)	Modify Registry (024)	Network Service Scanning (024)	Software Deployment Tools (024)	Network Service Scanning (024)			
	External Remote Services (025)	External Remote Services (025)	External Remote Services (025)	External Remote Services (025)	External Remote Services (025)	External Remote Services (025)	Modify Registry (025)	Network Service Scanning (025)	Software Deployment Tools (025)	Network Service Scanning (025)			
	External Remote Services (026)	External Remote Services (026)	External Remote Services (026)	External Remote Services (026)	External Remote Services (026)	External Remote Services (026)	Modify Registry (026)	Network Service Scanning (026)	Software Deployment Tools (026)	Network Service Scanning (026)			
	External Remote Services (027)	External Remote Services (027)	External Remote Services (027)	External Remote Services (027)	External Remote Services (027)	External Remote Services (027)	Modify Registry (027)	Network Service Scanning (027)	Software Deployment Tools (027)	Network Service Scanning (027)			
	External Remote Services (028)	External Remote Services (028)	External Remote Services (028)	External Remote Services (028)	External Remote Services (028)	External Remote Services (028)	Modify Registry (028)	Network Service Scanning (028)	Software Deployment Tools (028)	Network Service Scanning (028)			
	External Remote Services (029)	External Remote Services (029)	External Remote Services (029)	External Remote Services (029)	External Remote Services (029)	External Remote Services (029)	Modify Registry (029)	Network Service Scanning (029)	Software Deployment Tools (029)	Network Service Scanning (029)			
	External Remote Services (030)	External Remote Services (030)	External Remote Services (030)	External Remote Services (030)	External Remote Services (030)	External Remote Services (030)	Modify Registry (030)	Network Service Scanning (030)	Software Deployment Tools (030)	Network Service Scanning (030)			
	External Remote Services (031)	External Remote Services (031)	External Remote Services (031)	External Remote Services (031)	External Remote Services (031)	External Remote Services (031)	Modify Registry (031)	Network Service Scanning (031)	Software Deployment Tools (031)	Network Service Scanning (031)			
	External Remote Services (032)	External Remote Services (032)	External Remote Services (032)	External Remote Services (032)	External Remote Services (032)	External Remote Services (032)	Modify Registry (032)	Network Service Scanning (032)	Software Deployment Tools (032)	Network Service Scanning (032)			
	External Remote Services (033)	External Remote Services (033)	External Remote Services (033)	External Remote Services (033)	External Remote Services (033)	External Remote Services (033)	Modify Registry (033)	Network Service Scanning (033)	Software Deployment Tools (033)	Network Service Scanning (033)			
	External Remote Services (034)	External Remote Services (034)	External Remote Services (034)	External Remote Services (034)	External Remote Services (034)	External Remote Services (034)	Modify Registry (034)	Network Service Scanning (034)	Software Deployment Tools (034)	Network Service Scanning (034)			
	External Remote Services (035)	External Remote Services (035)	External Remote Services (035)	External Remote Services (035)	External Remote Services (035)	External Remote Services (035)	Modify Registry (035)	Network Service Scanning (035)	Software Deployment Tools (035)	Network Service Scanning (035)			
	External Remote Services (036)	External Remote Services (036)	External Remote Services (036)	External Remote Services (036)	External Remote Services (036)	External Remote Services (036)	Modify Registry (036)	Network Service Scanning (036)	Software Deployment Tools (036)	Network Service Scanning (036)			
	External Remote Services (037)	External Remote Services (037)	External Remote Services (037)	External Remote Services (037)	External Remote Services (037)	External Remote Services (037)	Modify Registry (037)	Network Service Scanning (037)	Software Deployment Tools (037)	Network Service Scanning (037)			
	External Remote Services (038)	External Remote Services (038)	External Remote Services (038)	External Remote Services (038)	External Remote Services (038)	External Remote Services (038)	Modify Registry (038)	Network Service Scanning (038)	Software Deployment Tools (038)	Network Service Scanning (038)			
	External Remote Services (039)	External Remote Services (039)	External Remote Services (039)	External Remote Services (039)	External Remote Services (039)	External Remote Services (039)	Modify Registry (039)	Network Service Scanning (039)	Software Deployment Tools (039)	Network Service Scanning (039)			
	External Remote Services (040)	External Remote Services (040)	External Remote Services (040)	External Remote Services (040)	External Remote Services (040)	External Remote Services (040)	Modify Registry (040)	Network Service Scanning (040)	Software Deployment Tools (040)	Network Service Scanning (040)			
	External Remote Services (041)	External Remote Services (041)	External Remote Services (041)	External Remote Services (041)	External Remote Services (041)	External Remote Services (041)	Modify Registry (041)	Network Service Scanning (041)	Software Deployment Tools (041)	Network Service Scanning (041)			
	External Remote Services (042)	External Remote Services (042)	External Remote Services (042)	External Remote Services (042)	External Remote Services (042)	External Remote Services (042)	Modify Registry (042)	Network Service Scanning (042)	Software Deployment Tools (042)	Network Service Scanning (042)			
	External Remote Services (043)	External Remote Services (043)	External Remote Services (043)	External Remote Services (043)	External Remote Services (043)	External Remote Services (043)	Modify Registry (043)	Network Service Scanning (043)	Software Deployment Tools (043)	Network Service Scanning (043)			
	External Remote Services (044)	External Remote Services (044)	External Remote Services (044)	External Remote Services (044)	External Remote Services (044)	External Remote Services (044)	Modify Registry (044)	Network Service Scanning (044)	Software Deployment Tools (044)	Network Service Scanning (044)			
	External Remote Services (045)	External Remote Services (045)	External Remote Services (045)	External Remote Services (045)	External Remote Services (045)	External Remote Services (045)	Modify Registry (045)	Network Service Scanning (045)	Software Deployment Tools (045)	Network Service Scanning (045)			
	External Remote Services (046)	External Remote Services (046)	External Remote Services (046)	External Remote Services (046)	External Remote Services (046)	External Remote Services (046)	Modify Registry (046)	Network Service Scanning (046)	Software Deployment Tools (046)	Network Service Scanning (046)			
	External Remote Services (047)	External Remote Services (047)	External Remote Services (047)	External Remote Services (047)	External Remote Services (047)	External Remote Services (047)	Modify Registry (047)	Network Service Scanning (047)	Software Deployment Tools (047)	Network Service Scanning (047)			
	External Remote Services (048)	External Remote Services (048)	External Remote Services (048)	External Remote Services (048)	External Remote Services (048)	External Remote Services (048)	Modify Registry (048)	Network Service Scanning (048)	Software Deployment Tools (048)	Network Service Scanning (048)			
	External Remote Services (049)	External Remote Services (049)	External Remote Services (049)	External Remote Services (049)	External Remote Services (049)	External Remote Services (049)	Modify Registry (049)	Network Service Scanning (049)	Software Deployment Tools (049)	Network Service Scanning (049)			
	External Remote Services (050)	External Remote Services (050)	External Remote Services (050)	External Remote Services (050)	External Remote Services (050)	External Remote Services (050)	Modify Registry (050)	Network Service Scanning (050)	Software Deployment Tools (050)	Network Service Scanning (050)			

MITRE ATT@CK (2)

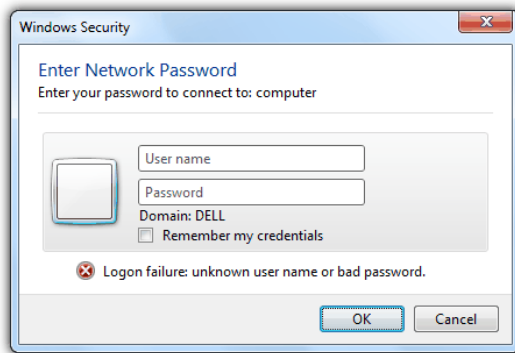
8. Credential Access – получение доступа с помощью действующих учетных записей
9. Discovery – сбор информации о цели изнутри
10. Lateral Movement – перемещение внутри целевой ИТ-инфраструктуры
11. Collection – сбор интересующих данных
12. Command and Control – организация внешнего управления
13. Exfiltration – передача интересующих данных вовне
14. Impact – разрушающее воздействие на ИТ-инфраструктуру



Как своевременно обнаруживать таргетированные атаки?



Необходимо отслеживать признаки нарушения ИБ



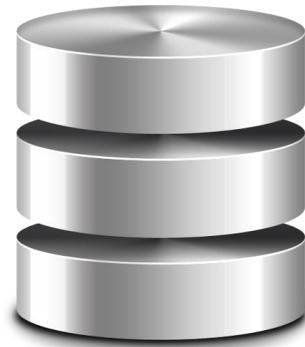
Авторизация: как успешная,
так и неуспешная



Срабатывания
антивирусного ПО,
СОВ



Нетипичное
поведение
пользователя



Подозрительные
запросы к СУБД

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

Соответствующее требование
включено в:

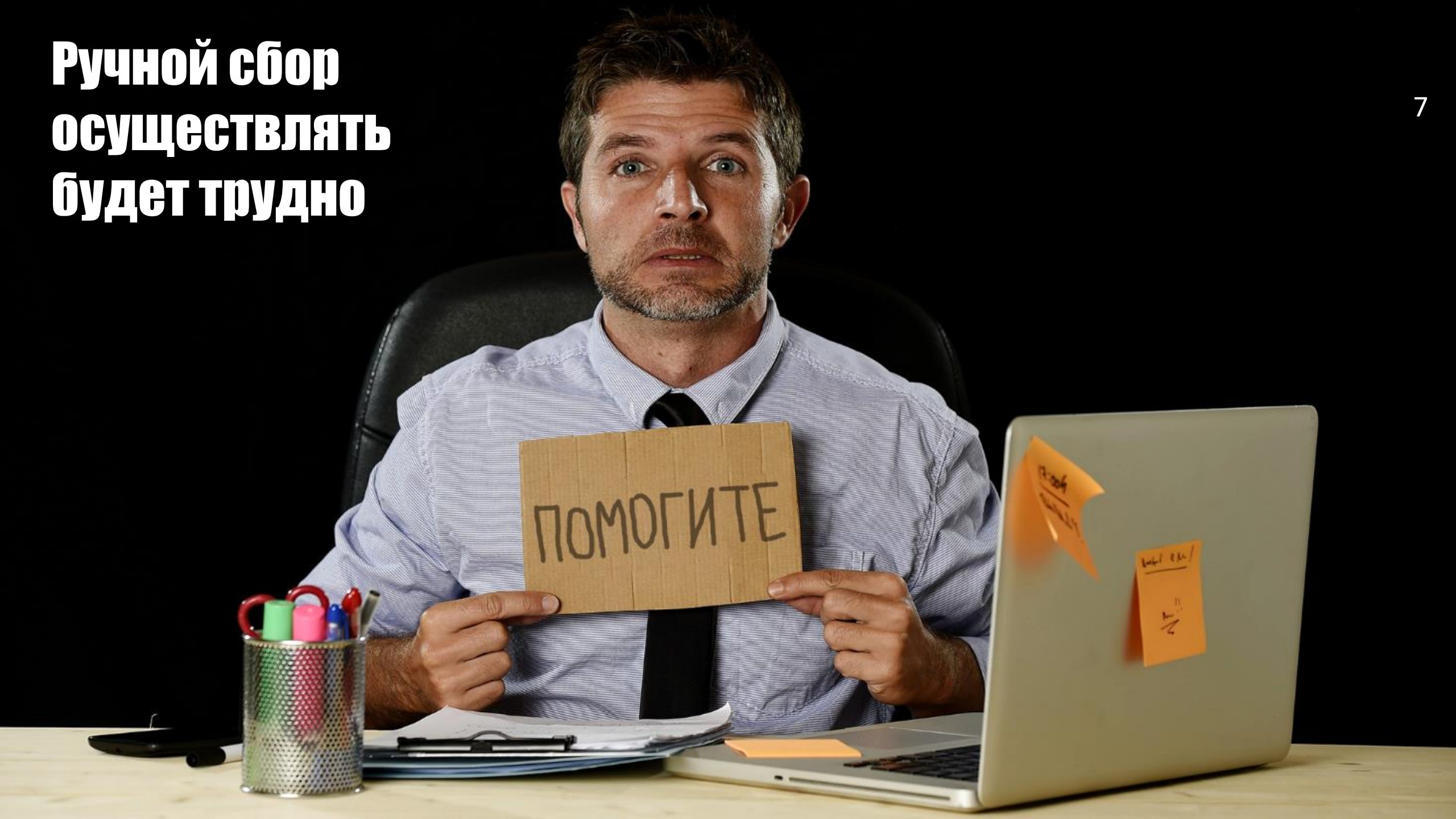
Приказ ФСТЭК России N 17
Приказ ФСТЭК России N 21
Приказ ФСТЭК России N 31
Приказ ФСТЭК России N 239



**Ручной сбор
осуществлять
будет трудно**

7

ПОМОГИТЕ




```

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 Genunteline1
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 Genunteline1
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| VMXvmbDbvMmxExecState: 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

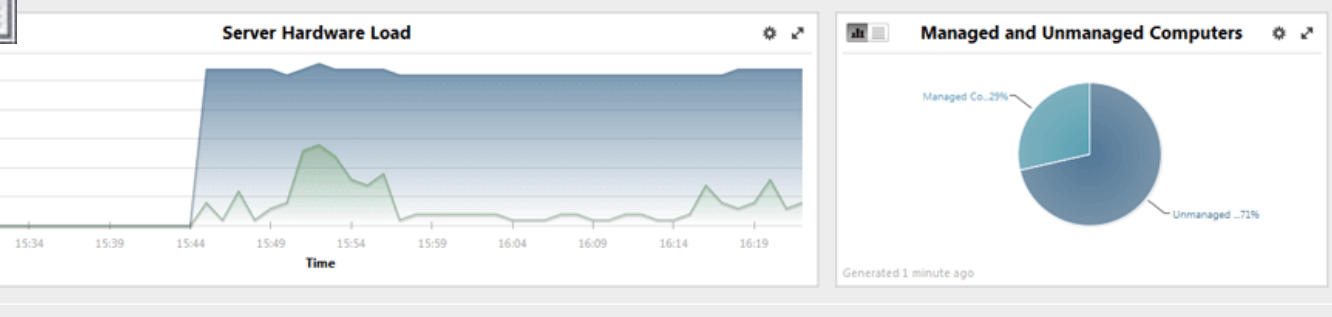
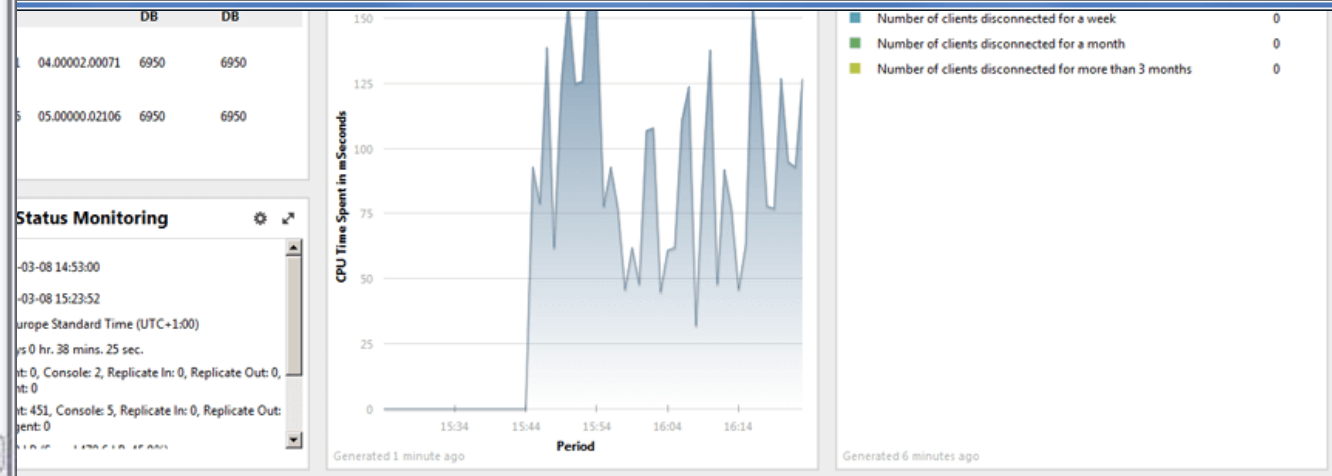
```

```

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 "ht
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 "ht
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 "ht
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**

KOMRAD Enterprise SIEM 4.0

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



Принцип работы SIEM-системы



Нормализация



Корреляция



Реакция



Уведомление



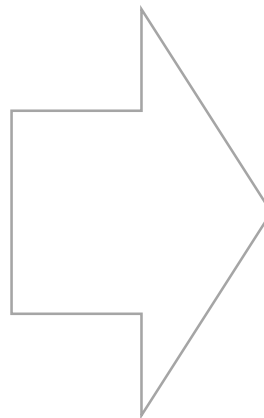
Фильтрация



Нормализация (разбор) событий

Сырое событие:

Jun 26 2021 09:02:35 fw.network.lan CEF:0
npo-echelon.ru|echelon|
1.1.1111|021|block connection|5|
src=8.8.8.10 spt=56117 dst=8.8.8.1 dpt=76
act=block



Разобранное событие:

Информация о событии 1624712561-00000013-00000004

Создать инцидент

Событие Контекст события

Поля коллектора

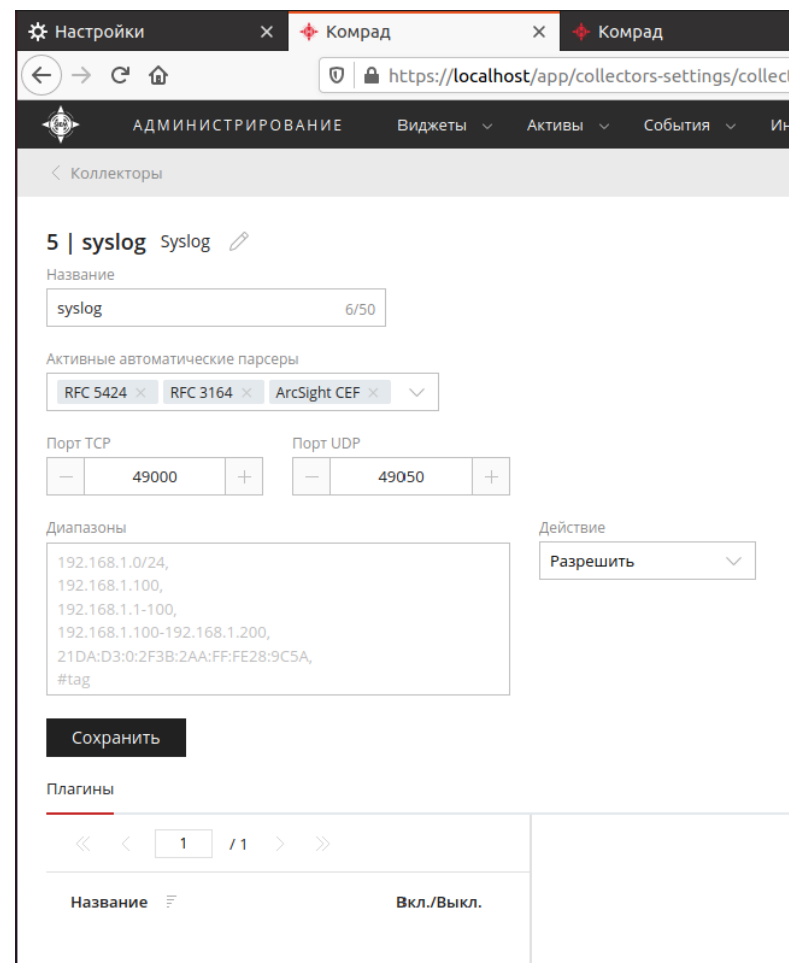
ПО	echelon
CEP.DeviceProduct	
Версия	1.1.1111
CEP.DeviceVersion	
Сигнатура	021
CEP.DeviceEventClassID	
Имя события	block connection
CEP.EventName	
Важность	5
CEP.Severity	
Производитель	npo-echelon.ru
CEP.DeviceVendor	

Elastic Common Schema

IP назначения	8.8.8.1
ECS.Destination.IP	
Порт назначения	76
ECS.Destination.Port	
Действие	block

Поддерживаемые стандарты и технологии разбора событий

- Поддержка стандартов:
 - RFC 5424
 - RFC 3164
 - ArcSight CEF
- Поддержка возможности разработки плагинов с помощью регулярных выражений (реализован стандарт RE2)
- Поддержка стандарта структурирования события: Elastic Common Schema



Хранение событий

- Подсистема сохраняет нормализованные события в СУБД ClickHouse, также возможна интеграция с PostgreSQL с расширением TimescaleDB для работы с временными рядами.

ClickHouse
не тормозит

Фильтры событий

Конструктор фильтра Код

И ИЛИ +

Поле	Операция	Значение	
ECS.Host.Hostname	Равно	skud.network.lan	16/50

СОБЫТИЯ Виджеты Активы **События** Инциденты Администрирование Ru

1 / 1

События, поступающие от С

26.06.2021, 00:00 — 26.06.2021, 23:59

Найти

ID источника	Тип источника	Сырой текст	Время записи
syslog 5	syslog	Jun 26 2021 11:20:56 skud.network.lan CEF:0 ...	26.06.2021, 18:21:02
syslog 5	syslog	Jun 26 2021 11:20:56 skud.network.lan CEF:0 ...	26.06.2021, 18:21:02
syslog 5	syslog	Jun 26 2021 11:00:22 skud.network.lan CEF:0 ...	26.06.2021, 18:00:28
syslog 5	syslog	Jun 26 2021 11:00:22 skud.network.lan CEF:0 ...	26.06.2021, 18:00:28

Директивы корреляции

- Простой вариант: ссылка на директиву
- Продвинутой:
 - Определение последовательности событий с временными окнами
 - Работа с переменными
 - Проверка отсутствия события

ИНЦИДЕНТЫ Виджеты Активы События

< Директивы

Настройка директивы

Сохранить

Название

Admin access incident 21/120

Конструктор директивы Код Дополнительные настройки

Проверить

и или +

Тип

Событие Ветвление

Фильтр

admin access

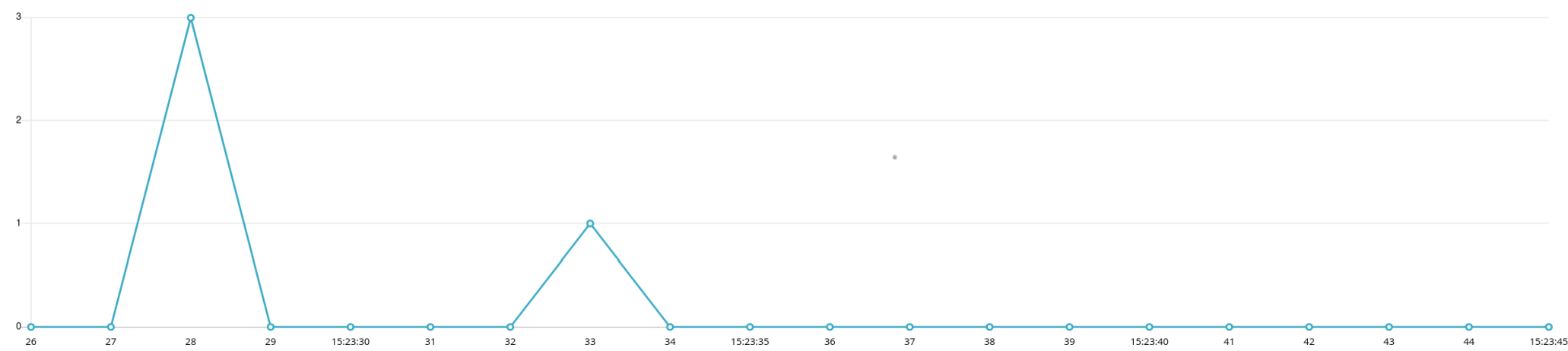
Выражение

Введите выражение...

> Переменные

Уведомление: в интерфейсе и по SMTP

Размер таблицы (строки) - 40 +



ID источника	Тип источника	Сырой текст	Время записи
5	syslog	Jun 27 2021 15:23:22 http.network.lan CEF:0 npo-echelon.ru e...	27.06.2021, 15:23:33
5	syslog	Jun 27 2021 15:23:22 fw.network.lan CEF:0 npo-echelon.ru e...	27.06.2021, 15:23:33
5	syslog	Jun 27 2021 15:23:22 fw.network.lan CEF:0 npo-echelon.ru e...	27.06.2021, 15:23:33
5	syslog	Jun 27 2021 15:23:22 fw.network.lan CEF:0 npo-echelon.ru e...	27.06.2021, 15:23:33
5	syslog	Jun 27 2021 15:11:08 http.network.lan CEF:0 npo-echelon.ru e...	27.06.2021, 15:11:19

Новый инцидент ✕

06.2021, 15:23:28

Директива «Потенциальная атака на веб-сервер (получен административный доступ)» (10004)

Важность высокая

Скрыть 27.06.2021, 15:24:05

Инцидент может быть передан в ГОССОПКА автоматически или в ручном режиме

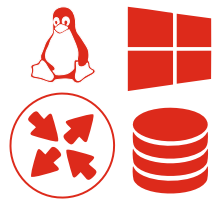
The screenshot shows a web application interface for incident management. The top navigation bar includes 'ИНЦИДЕНТЫ', 'Виджеты', 'Активы', 'События', 'Инциденты', and 'Администрирование'. Below this is a secondary navigation bar with 'Инциденты', 'Информация', 'История', 'События', 'Рекомендации', 'Активы', and 'ГосСОПКА'. The main content area is titled 'Передача в ГосСОПКА' and contains several form fields:

- Описание:** A text input field with the placeholder 'Введите описание...' and a character count '0/500'.
- Тип инцидента в НЦКИ:** A dropdown menu with the placeholder 'Выберите тип...'.
- Статус реагирования на инцидент:** A text input field with the value 'Проводятся мероприятия по реагированию на инцидент'.
- Информация о категорировании ОКИИ:** A text input field with the value 'Объект КИИ без категории значимости'.
- Наличие подключения к сети Интернет:** A toggle switch that is currently turned on.
- Сфера функционирования субъекта:** A text input field with the value 'Банковская сфера и иные сферы финансового рынка'.
- Наименование контролируемого ресурса, на котором был выявлен:** A text input field that is currently empty.

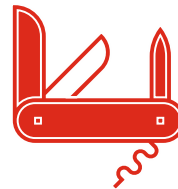
Отличительные особенности



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

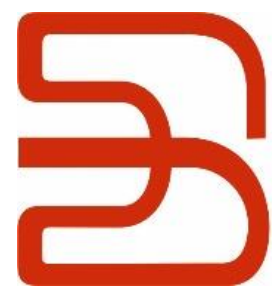
КОМРАД Enterprise SIEM предъявляет минимальные требования к аппаратному обеспечению

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



Полезные ссылки

- getkomrad@npo-echelon.ru – email для получения демо-лицензии KOMRAD Enterprise SIEM;
- <https://t.me/komrad4> - чат пользователей продукта
- <https://www.youtube.com/channel/UCIwZEG8EcL7tnZN4Qzjt13w>
канал учебного центра «Эшелон» с обучающими видео



Эшелон
комплексная безопасность