



Инструкция по подключению пограничных контроллеров сессий Eltex ESBC к системе Wazuh SIEM

Версия ПО ESBC 1.9.0

Версия Wazuh 4.14.5

СОДЕРЖАНИЕ

1. Описание взаимодействия с Wazuh SIEM	3
1.1 Поддерживаемые группы событий	4
2. Конфигурация ESBC	5
2.1 Включение логирования событий	5
2.2 Настройка удалённого Syslog-сервера (Wazuh manager).....	6
2.3 Формат передаваемого сообщения	7
3. Конфигурация Wazuh manager	8
3.1 Приём сообщений Syslog	8
3.2 Сетевые доступы	8
4. Внедрение декодера и правил Wazuh	9
4.1 Создание файла декодера	9
4.2 Добавление правил корреляции	9
4.3 Применение изменений	9
4.4 Проверка статуса и возможных ошибок.....	9
4.5 Тестирование	10
5. Декодеры	11
6. Правила корреляции.....	12
7. Создание дашбордов и визуализаций Wazuh	14
7.1 Создание визуализации	14
7.2 Создание дашборда	14
Приложение А. Содержимое файла декодера /var/ossec/etc/decoders/esbc.xml.....	15
Приложение Б. Содержимое правил ESBC (для local_rules.xml).....	17
ТЕХНИЧЕСКАЯ ПОДДЕРЖКА.....	23

1. Описание взаимодействия с Wazuh SIEM

На пограничных контроллерах сессий ESBC реализован модуль Syslog, формирующий сообщения об аутентификации, изменении состояния системы, работе межсетевого экрана, событиях VoIP и прочих событиях в формате RFC 5424. Полный перечень сообщений описан в документе «ESBC-series. Руководство по сообщениям Syslog».

Wazuh SIEM обеспечивает сбор этих сообщений, извлечение параметров с помощью декодеров, корреляцию и классификацию событий с помощью правил, сопоставление с тактиками MITRE ATT&CK и наглядную визуализацию в веб-интерфейсе Wazuh dashboard.

Схематичное представление присоединения ESBC к Wazuh SIEM:

- Пограничный контроллер сессий ESBC передаёт сообщения Syslog по UDP/TCP на удалённый syslog-сервер.
- Wazuh manager принимает сообщения на встроенном syslog-слушателе (порт 514) и записывает их в индексы OpenSearch: wazuh-archives-* (все события) и wazuh-alerts-* (алерты по правилам).
- Декодеры (decoders) разбирают каждое сообщение и извлекают параметры: пользователя, IP-адрес, порт, интерфейс, причину блокировки и другие поля.
- Правила (rules) сопоставляют декодированное событие с условием и присваивают описанию уровень (level 0–15), группы (например, authentication_failed, attack) и ссылку на MITRE ATT&CK.
- Оператор анализирует события в Wazuh dashboard: дашборды, визуализации, поиск по индексу wazuh-alerts-*.

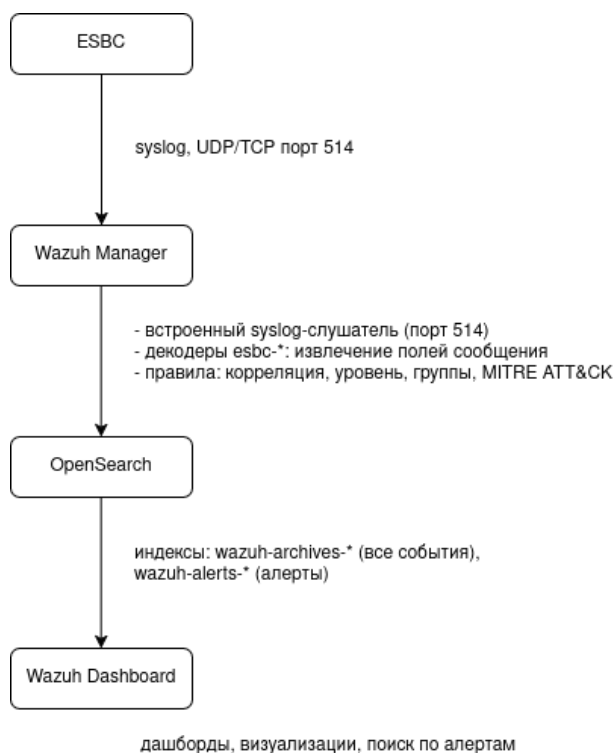


Рисунок 1 – Обобщённая схема интеграции ESBC с Wazuh SIEM

1.1 Поддерживаемые группы событий

Примеры декодеров ([Приложение А](#)) и правил ([Приложение Б](#)) покрывают не все события, описанные в документе «ESBC-series. Руководство по сообщениям Syslog», а только указанные в таблице ниже, и могут быть использованы в качестве примера для описания остальных событий:

Группа сообщений	Мнемоники	Пункты руководства
Аутентификация AAA	%AAA-*, %AAA-I-SSH	1.1–1.5, 1.11.1–1.11.2
Состояние системы (reboot/shutdown)	%SYS-C-REBOOT, %SYS-W-EVENT	2.1, 2.3
Перезапуск ПО ESBC	%ESBC-C-EVENT	2.2
Изменение конфигурации (commit/confirm)	%CLI-I-CRIT, %SYS-W-EVENT	2.5–2.9
Защита от DoS/DDoS (screen)	%FIREWALL-W-EVENT_WARN: screen	4.1
Zone-based firewall	%FIREWALL-I-EVENT_LOG: zone-pair	4.2
Динамический брандмауэр SIP	%ESBC-W-EVENT: Banned IP / Firewall	4.5
Действия пользователя в ESBC	%ESBC-W-EVENT: User ... requested	6.1–6.3
Срабатывание ограничителей SIP	%ESBC-W-EVENT: ... limit is reached	6.4

Не покрываемые правилами группы сообщений регистрируются в Wazuh как обычные syslog-события (архив), но детализированных правил в Приложениях А и Б настоящей инструкции не содержится.

2. Конфигурация ESBC

2.1 Включение логирования событий

Для того чтобы соответствующие сообщения формировались и передавались в SIEM, на ESBC необходимо включить логирование соответствующих типов событий (команды режима CONFIG, уровень привилегий 10–15):

Команда CLI	Назначение	Раздел руководства Syslog
logging login on-failure	Неудачные попытки подключения к CLI: неверный пароль, неизвестный пользователь, отклонение аутентификации	1.2–1.4
logging userinfo	Изменение учётных данных и привилегий пользователей (создание/удаление, смена пароля и уровня привилегий), ввод команд	1.6–1.10, 1.12.1, 2.10
logging firewall screen dos-defense <TYPE>	Логирование защиты от DoS/DDoS-атак (тип: syn-flood, udp-threshold, icmp-threshold, land, limit-session-source, limit-session-destination)	4.1
logging nat	Логирование NAT-трансляции	4.3
logging firewall arp-inspection	Логирование срабатываний ARP inspection (в связке с ip arp inspection)	4.4
log (в правиле zone-pair)	Логирование разрешённого/заблокированного трафика межзональным брандмауэром — задаётся в параметрах правила zone-pair при задании action	4.2

Пример включения логирования основных групп событий:

```
vesbc(config)# logging login on-failure
vesbc(config)# logging userinfo
vesbc(config)# logging firewall screen dos-defense syn-flood
vesbc(config)# logging firewall screen dos-defense udp-threshold
vesbc(config)# logging nat
```

Сообщения аутентификации (успешный/неуспешный вход, SSH), события reboot/shutdown, commit/confirm и события ESBC формируются без дополнительных команд.

2.2 Настройка удалённого Syslog-сервера (Wazuh manager)

Назначьте Wazuh manager в качестве удалённого syslog-сервера. Команда `syslog host` включает передачу сообщений и переводит в режим CONFIG-SYSLOG-HOST, в котором задаются адрес, порт, транспорт и уровень важности. Пример настройки:

```
vesbc# config
vesbc(config)# syslog host WAZUH
vesbc(config-syslog-host)# remote-address 192.168.10.100
vesbc(config-syslog-host)# port 514
vesbc(config-syslog-host)# transport udp
vesbc(config-syslog-host)# severity info
vesbc(config-syslog-host)# exit
vesbc(config)# exit
vesbc# commit
vesbc# confirm
```

Параметры:

- `remote-address 192.168.10.100` — IP-адрес Wazuh manager;
- `port 514` — номер UDP/TCP-порта удалённого сервера;
- `transport udp` — транспортный протокол передачи (`udp` | `tcp`);
- `severity info` — минимальный уровень важности передаваемых сообщений (`none`, `emerg`, `alert`, `crit`, `error`, `warning`, `notice`, `info`, `debug`). Для передачи событий SIEM рекомендуется указывать `info`.

Проверьте конфигурацию командой `show syslog configuration hosts`:

```
vesbc# show syslog configuration hosts
```

Name	IP Address	Severity	Transport	Port	Filters
WAZUH	192.168.10.100	info	udp	514	No

2.3 Формат передаваемого сообщения

Сообщения передаются в формате RFC 5424. Пример полной записи, формируемой ESBC (шаблон <PRI>1 \$ISODATE \$HOSTNAME \$APP-NAME - - - \$SEQNUM: \$MSG):

```
<86>1 2026-09-22T10:16:27+00:00 esbc-01 login - - - 1: %AAA-LOCAL-I-SESSION: console: session opened  
for user admin
```

Wazuh manager распознаёт syslog-шапку (PRI, временную метку, имя узла и приложения), а содержимое MSG разбирается декодерами ESBC.

3. Конфигурация Wazuh manager

3.1 Приём сообщений Syslog

Wazuh manager по умолчанию слушает входящие syslog-сообщения на UDP-порту 514. При необходимости порт и протокол изменяются в файле `/var/ossec/etc/ossec.conf`:

```
<ossec_config>
  <ports>
    <syslog_port>514</syslog_port>
    <protocol>udp</protocol>
  </ports>
</ossec_config>
```

3.2 Сетевые доступы

Откройте в файрволе Wazuh manager доступ на порт 514 (UDP) с адресом ESBC.

Примеры для firewall-cmd (firewalld) и ufw:

```
firewall-cmd --permanent --add-rich-rule='rule family="ipv4" source address="10.0.1.0/24" port
protocol="udp" port="514" accept'
firewall-cmd --reload
ufw allow from 10.0.1.0/24 to any port 514 proto udp
```

После изменения `ossec.conf` перезапустите `wazuh-manager` ([раздел 4.3](#)).

4. Внедрение декодера и правил Wazuh

4.1 Создание файла декодера

Создайте файл `/var/ossec/etc/decoders/esbc.xml` и добавьте в него содержимое декодера (полный текст приведён в [Приложении А](#)):

```
cd /var/ossec/etc/decoders/  
sudo vi esbc.xml # вставить содержимое Приложения А
```

4.2 Добавление правил корреляции

Для добавления правил отредактируйте файл `/var/ossec/etc/rules/local_rules.xml` и вставьте в него содержимое правил ESBC (полный текст — в [Приложении Б](#)). Правила размещаются внутри корневого тега `<rule_list>` до закрывающего тега `</rule_list>`:

```
<rule_list>  
  <!-- существующие правила local_rules.xml -->  
  
  <!-- Eltex ESBC - правила (Приложение Б) -->  
  <group name="esbc,aaa,authentication,syslog">  
    ...  
  </group>  
</rule_list>
```

4.3 Применение изменений

Для внесения изменений перезагрузите `wazuh-manager`:

```
sudo systemctl restart wazuh-manager
```

4.4 Проверка статуса и возможных ошибок

```
sudo systemctl status wazuh-manager
```

Ошибки разбора XML-файлов (несоответствие тега, дублирование id правил) выводятся в журнал `/var/ossec/logs/ossec.log`:

```
sudo tail -n 100 /var/ossec/logs/ossec.log | grep -i "error\|decode\|rule"
```

4.5 Тестирование

Протестируйте внесённые изменения утилитой `wazuh-logtest` и передайте ей тестовое сообщение в формате MSG (например, событие неуспешной аутентификации по SSH из пункта 1.11.2 руководства Syslog):

```
sudo /var/ossec/bin/wazuh-logtest
```

Ожидаемый результат — сообщение распознано декодером `esbc-aaa-ssh`, сработало правило 100151 с уровнем 7:

```
**Phase 1: Completed pre-decoding.
content: %AAA-I-SSH: Failed password for admin from 10.0.0.1 port 54560 ssh2

**Phase 2: Completed decoding.
decoder_name: esbc-aaa-ssh
ssh_result: Failed
ssh_user: admin
srcip: 10.0.0.1
ssh_port: 54560
ssh_proto: ssh2

**Phase 3: Completed filtering (rules).
id: 100151
level: 7
rule_name: ESBC: Неуспешная аутентификация по SSH: неверный пароль для пользователя admin с адреса
10.0.0.1 на устройстве vesbc
```

Реальную передачу можно проверить, инициировав на ESBC, например, попытку SSH-входа с неверным паролем, и убедившись в появлении алерта в Wazuh dashboard ([раздел 7.2](#)).

5. Декодеры

Декодеры определяют мнемонику сообщения (prematch), извлекают параметры регулярным выражением (regex) и присваивают им имена (order). Имена полей используются в описаниях правил: \$(user2), \$(srcip) и т. д.

Декодер	Prematch	Извлекаемые поля
esbc-aaa-ssh	%AAA-I-SSH:	esbc_model, ssh_result, ssh_user, srcip, ssh_port, ssh_proto
esbc-aaa	%AAA-	esbc_model, aaa_mnemonic, aaa_session_type, aaa_msg, user2, dstuser, tty, rhost
esbc-sys-reboot	%SYS-C-REBOOT: CLI: System shutdown	sys_action, sys_reboot_user, sys_reboot_source
esbc-sys-reboot-other	%SYS-C-REBOOT:	sys_reboot_reason
esbc-cli-crit	%CLI-I-CRIT:	user2, cli_source, acl_action
esbc-fw-screen-event	%FIREWALL-W-EVENT_WARN: screen	fw_screen_name, fw_vrf, fw_action, fw_protocol, srcip, src_interface, src_mac, dstip, fw_dscp
esbc-fw-zonepair-event	%FIREWALL-I-EVENT_LOG: zone-pair	fw_zonepair, fw_rule_id, fw_vrf, fw_action, fw_protocol, srcip, srcport, src_interface, src_mac, dstip, dstport, fw_dscp
esbc-ban	%ESBC-W-EVENT: Banned	srcip, ban_reason, ban_attr_type, ban_attr_name, ban_errors
esbc-attr	%ESBC-W-EVENT: Firewall	esbc_fw_type, esbc_fw_key, esbc_ip_count, ban_reason
esbc-usr	%ESBC-W-EVENT: User	user2, cli_source, esbc_srcip, esbc_action
esbc-limit	%ESBC-W-EVENT:	object_type, name_object, limit_type
esbc-reload	%ESBC-C-EVENT: User	user2, cli_source, esbc_srcip

6. Правила корреляции

Правила сгруппированы по типам событий. Уровень (level) отражает значимость события: 0 — базовое правило группы, 3–5 — информационные события, 6–8 — требующие внимания, 9 — критичные. Сопоставление с MITRE ATT&CK указано для событий, относящихся к типичным действиям нарушителя.

В данной инструкции, в качестве примера, используются индексы (ID) для правил ESBC 100140-100159. При настройке правил необходимо заменить индексы в соответствии с правилами распределения индексов вашей системы SIEM.

ID	Уровень	Описание	MITRE	Пункт руководства	Декодер
100140	0	Базовое правило AAA-событий (декодер esbc-aaa)	—	1.1–1.5	esbc-aaa
100141	5	Сессия открыта для пользователя \$(dstuser)	T1078	1.1	esbc-aaa
100142	3	Сессия закрыта для пользователя \$(dstuser)	—	1.5	esbc-aaa
100143	5	Неверный пароль для пользователя \$(user2)	T1110, T1110.001	1.3	esbc-aaa
100144	5	Попытка входа неизвестным пользователем \$(user2)	T1110, T1110.003	1.4	esbc-aaa
100150	0	Базовое правило SSH-аутентификации (декодер esbc-aaa-ssh)	—	1.11.1–1.11.2	esbc-aaa-ssh
100151	7	Неуспешная аутентификация по SSH: неверный пароль	T1110, T1110.001	1.11.2	esbc-aaa-ssh
100152	3	Успешная аутентификация по SSH	T1078	1.11.1	esbc-aaa-ssh
100154	5	Неудачная попытка входа в систему (authenticate failed)	T1110	1.2	esbc-aaa
100155	0	Базовое правило критичных событий ESBC (%ESBC-C-)	—	2.2	esbc-reload
100156	8	Перезапуск ПО ESBC: перезагрузка модулей по запросу пользователя	—	2.2	esbc-reload
100160	0	Базовое правило событий состояния системы (%SYS-)	—	2.1, 2.3, 2.6–2.9	—
100162	9	Выключение или перезагрузка устройства инициировано (shutdown initiated)	T1091	2.1	esbc-sys-reboot
100165	9	Выключение или перезагрузка устройства запланировано (shutdown scheduled)	T1091	2.1	esbc-sys-reboot
100163	8	Перезагрузка устройства по иным причинам	—	2.3	esbc-sys-reboot-other
100164	7	Конфигурация успешно применена (при загрузке системы)	—	2.6	—
100166	6	Предупреждение: таймер подтверждения конфигурации истечёт через 60 с	—	2.8	—
100167	5	Таймер подтверждения истёк, конфигурация отменена	—	2.9	—
100170	0	Базовое правило критичных действий в CLI (%CLI-I-CRIT:)	—	2.5, 2.7	esbc-cli-crit

100171	4	Применение изменения конфигурации (commit)	T1078	2.5	esbc-cli-crit
100172	4	Подтверждение изменения конфигурации (confirm)	—	2.7	esbc-cli-crit
100180	0	Базовое правило событий ESBC (%ESBC-W-EVENT)	—	4.5, 6.x	—
100181	8	Блокировка IP-адреса динамическим брандмауэром	T1220	4.5.1	esbc-ban
100182	7	Блокировка атрибутов динамическим брандмауэром	—	4.5.2	esbc-attr
100183	3	Действие пользователя в ESBC (чёрный список, вызовы, регистрации)	—	6.1.1–6.3.3	esbc-usr
100184	3	Срабатывание ограничителя (limit is reached)	—	6.4	esbc-limit
100190	0	Базовое правило защиты от DoS/DDoS (screen)	—	4.1	esbc-fw-screen-event
100191	7	DoS/DDoS-атака заблокирована (screen denied)	T1498	4.1	esbc-fw-screen-event
100192	5	DoS/DDoS-атака обнаружена (screen detected)	—	4.1	esbc-fw-screen-event
100193	0	Базовое правило zone-based firewall (zone-pair)	—	4.2	esbc-fw-zonepair-event
100194	7	Трафик заблокирован межзоновым брандмауэром (denied)	T1562	4.2	esbc-fw-zonepair-event
100195	4	Трафик разрешён межзоновым брандмауэром (permitted)	—	4.2	esbc-fw-zonepair-event

7. Создание дашбордов и визуализаций Wazuh

7.1 Создание визуализации

1. В верхнем левом меню Wazuh dashboard перейдите в Explore → Visualize.
2. Нажмите Create new visualization.
3. В окне New Visualization выберите тип визуализации (Metric, Bar, Line, Pie, Data table и др.).
4. Выберите индекс-источник (index pattern): wazuh-alerts-.*.
5. Настройте агрегации в панели Data: Metrics (что считаем — Count, Average, ...) и Buckets (как группируем — Terms, Date histogram, ...).
6. Нажмите Update — график отрисуется.
7. Нажмите Save в правом верхнем углу и задайте заголовок визуализации.

7.2 Создание дашборда

1. Меню → Explore → Dashboards → Create new dashboard.
2. Нажмите Add и выберите созданные визуализации для добавления на холст.
3. Упорядочите виджеты перетаскиванием, измените размеры за края.
4. Добавьте общий фильтр rule.groups: esbc и временной промежуток в верхней панели — они применятся ко всем виджетам дашборда.
5. Нажмите Save (правый верхний угол). При сохранении выберите Save (обновить текущий) или Save as (новая копия).

Редактирование: наведите на виджет → меню (три точки) → Edit; либо Explore → Visualize → открыть нужную визуализацию, править, Save. Фильтрация по значению — кликом по элементу графика → Filter for value или Exclude.

Приложение А. Содержимое файла декодера /var/ossec/etc/decoders/esbc.xml

```
<!-- ===== -->
<!-- Eltex ESBC - Decoders -->
<!-- ===== -->

<decoder name="esbc-aaa-ssh">
  <prematch>%AAA-I-SSH:</prematch>
  <regex type="pcre2">(?:\[^\]]*model="([^\"]*)"?)\s*%AAA-I-SSH:\s*(Accepted|Failed) password for (\S+) from
  (\S+) port (\d+) (\S+)$</regex>
  <order>esbc_model,ssh_result,ssh_user,srcip,ssh_port,ssh_proto</order>
</decoder>

<!-- AAA parent decoder -->
<decoder name="esbc-aaa">
  <prematch>%AAA-</prematch>
  <regex type="pcre2">(?:\[^\]]*model="([^\"]*)"?)\s*%AAA-([A-Z_]+-[A-Z]+(?:-[A-Z]+)?):\s*(?:([a-zA-Z][\w-
  ]*):\s*)?(.*?)(?:\s+(?:for )?user '([^\']+)'|for user (\S+)))(?:\s+tty=(\S+))?(?:\s+rhost=(\S+))?$</regex>
  <order>esbc_model,aaa_mnemonic,aaa_session_type,aaa_msg,user2,dstuser,TTY,rhost</order>
</decoder>

<!-- SYS: standalone decoders -->
<decoder name="esbc-sys-reboot">
  <prematch>%SYS-C-REBOOT: CLI: System shutdown </prematch>
  <regex type="pcre2">%SYS-C-REBOOT: CLI: System shutdown (initiated|scheduled) by user (\S+) from
  (console|ssh(?:\s+[0-9a-fA-F:. ]+)?|telnet(?:\s+[0-9a-fA-F:. ]+)?</regex>
  <order>sys_action,sys_reboot_user,sys_reboot_source</order>
</decoder>

<decoder name="esbc-sys-reboot-other">
  <prematch>%SYS-C-REBOOT: </prematch>
  <regex type="pcre2">%SYS-C-REBOOT: (.+)</regex>
  <order>sys_reboot_reason</order>
</decoder>

<decoder name="esbc-cli-crit">
  <prematch>%CLI-I-CRIT: </prematch>
  <regex type="pcre2">%CLI-I-CRIT:\s*user\s+(\S+)\s+from\s+(console|ssh\s+[0-9a-fA-F:. ]+|telnet\s+[0-9a-fA-
  F:. ]+|ssh|telnet)\s+input:\s*(.+)</regex>
  <order>user2,cli_source,acl_action</order>
</decoder>

<decoder name="esbc-fw-screen-event">
  <prematch>%FIREWALL-W-EVENT_WARN: screen</prematch>
  <regex type="pcre2">%FIREWALL-W-EVENT_WARN: screen '([^\']+)'(?: \((([^\]]*)\))?)? (detected|denied) (\S+) (\[[0-9a-
  fA-F:. ]+\])?(?: \(((\S+)(?: (\S+))?\))?)? -> (\[[0-9a-fA-F:. ]+\])?(?: dscp (\d+))?$</regex>
  <order>fw_screen_name,fw_vrf,fw_action,fw_protocol,srcip,src_interface,src_mac,dstip,fw_dscp</order>
</decoder>

<decoder name="esbc-fw-zonepair-event">
  <prematch>%FIREWALL-I-EVENT_LOG: zone-pair</prematch>
  <regex type="pcre2">%FIREWALL-I-EVENT_LOG:\s*zone-pair '([^\']+)\' rule (\d+)(?: \((([^\]]*)\))?)? (permitted|denied)
  (\S+) (\S+)(?::(\d+))?(?: \(((\S+)(?: (\S+))?\))?)? -> (\S+)(?::(\d+))?(?: dscp (\d+))?$</regex>
```

```

<order>fw_zonepair, fw_rule_id, fw_vrf, fw_action, fw_protocol, srcip, srcport, src_interface, src_mac, dstip, dstport, fw_ds
cp</order>
</decoder>

<!-- ESBC: Banned IP record (4.5.1) -->
<decoder name="esbc-ban">
  <prematch>%ESBC-W-EVENT: Banned </prematch>
  <regex type="pcre2">Banned IP record:\s*IP:\s*(\S+),\s*ban reason:\s*([\^,]+)(?:,\s*([A-Za-
z]+):\s*(\S+))?,\s*errors:\s*(\d+)</regex>
  <order>srcip, ban_reason, ban_attr_type, ban_attr_name, ban_errors</order>
</decoder>

<!-- ESBC: Firewall attr record blocked (4.5.2) -->
<decoder name="esbc-attr">
  <prematch>%ESBC-W-EVENT: Firewall </prematch>
  <regex type="pcre2">Firewall\s+(\S+)\s+record:\s*key:\s*(\S+),\s*IP count:\s*(\d+),\s*ban reason:\s*(.+)</regex>
  <order>esbc_fw_type, esbc_fw_key, esbc_ip_count, ban_reason</order>
</decoder>

<!-- ESBC: user action (blacklist/terminate/registrations 6.x) -->
<decoder name="esbc-usr">
  <prematch>%ESBC-W-EVENT: User </prematch>
  <regex type="pcre2">User\s+(\S+)\s+from\s+(console|ssh|telnet)(?:\s+([0-9a-fA-
F:.]+))?\s+(requested\s+.*)*$</regex>
  <order>user2, cli_source, esbc_srcip, esbc_action</order>
</decoder>

<!-- ESBC: limiter reached (6.4) -->
<decoder name="esbc-limit">
  <prematch>%ESBC-W-EVENT: </prematch>
  <regex type="pcre2">%ESBC-W-EVENT: ([^\s]+)(\[^\s\])*\)? (.*) limit is reached$</regex>
  <order>object_type, name_object, limit_type</order>
</decoder>

<!-- ESBC: ESBC modules reload requested (C-level event) -->
<decoder name="esbc-reload">
  <prematch>%ESBC-C-EVENT: User</prematch>
  <regex type="pcre2">User\s+(\S+)\s+from\s+(\S+)(?:\s+(\S+))?\s+requested\s+reload\s+of\s+ESBC\s+modules</regex>
  <order>user2, cli_source, esbc_srcip</order>
</decoder>

```

Приложение Б. Содержимое правил ESBC (для local_rules.xml)

```

<!-- ===== -->
<!-- Eltex ESBC - Правила -->
<!-- ===== -->

<!-- ===== -->
<!-- 1. События AAA (аутентификация) -->
<!-- ===== -->
<group name="esbc,aaa,authentication,syslog">

    <rule id="100140" level="0">
        <decoded_as>esbc-aaa</decoded_as>
        <description>ESBC: AAA событие</description>
    </rule>

    <rule id="100141" level="5">
        <if_sid>100140</if_sid>
        <field name="aaa_msg" type="pcre2">^session opened</field>
        <description>ESBC: Сессия открыта для пользователя $(dstuser) (тип: $(aaa_session_type), адрес: $(rhost)) на
        устройстве $(esbc_model)</description>
        <mitre>
            <id>T1078</id>
        </mitre>
        <group>authentication_success,pci_dss_10.2.5,gdpr_IV_32.2,hipaa_164.312.b,nist_800_53_AU.14,</group>
    </rule>

    <rule id="100142" level="3">
        <if_sid>100140</if_sid>
        <field name="aaa_msg" type="pcre2">^session closed</field>
        <description>ESBC: Сессия закрыта для пользователя $(dstuser) (тип: $(aaa_session_type), адрес: $(rhost)) на
        устройстве $(esbc_model)</description>
        <group>authentication_success,pci_dss_10.2.5,</group>
    </rule>

    <rule id="100143" level="5">
        <if_sid>100140</if_sid>
        <field name="aaa_msg" type="pcre2">^Incorrect password</field>
        <description>ESBC: Неверный пароль для пользователя $(user2) tty=$(tty) с $(rhost) на устройстве
        $(esbc_model)</description>
        <mitre>
            <id>T1110</id>
            <id>T1110.001</id>
        </mitre>
        <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
    </rule>

    <rule id="100144" level="5">
        <if_sid>100140</if_sid>
        <field name="aaa_msg" type="pcre2">^Unknown</field>
        <description>ESBC: Попытка входа неизвестным пользователем $(user2) tty=$(tty) с $(rhost) на устройстве
        $(esbc_model)</description>
        <mitre>
            <id>T1110</id>
            <id>T1110.003</id>
        </mitre>
    </rule>
</group>

```

```

<!-- ===== -->
<!--  Вход по SSH (Accepted/Failed password) -->
<!-- ===== -->
<group name="esbc,aaa,authentication,syslog">

  <rule id="100150" level="0">
    <decoded_as>esbc-aaa-ssh</decoded_as>
    <description>ESBC: Событие аутентификации по SSH</description>
  </rule>

  <rule id="100151" level="7">
    <if_sid>100150</if_sid>
    <match>%AAA-I-SSH: Failed password for </match>
    <description>ESBC: Неудачная аутентификация по SSH: неверный пароль для пользователя $(ssh_user) с адреса $(srcip) на устройстве $(esbc_model)</description>
    <mitre>
      <id>T1110</id>
      <id>T1110.001</id>
    </mitre>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  </rule>

  <rule id="100152" level="3">
    <if_sid>100150</if_sid>
    <match>%AAA-I-SSH: Accepted password for </match>
    <description>ESBC: Успешная аутентификация по SSH: пользователь $(ssh_user) вошёл с адреса $(srcip) на устройство $(esbc_model)</description>
    <mitre>
      <id>T1078</id>
    </mitre>
    <group>authentication_success,pci_dss_10.2.5,</group>
  </rule>

  <rule id="100154" level="5">
    <if_sid>100140</if_sid>
    <match>authenticate failed</match>
    <description>ESBC: Неудачная попытка входа в систему (аутентификация отклонена): $(aaa_msg) на устройстве $(esbc_model)</description>
    <mitre>
      <id>T1110</id>
    </mitre>
    <group>authentication_failed,pci_dss_10.2.4,</group>
  </rule>
</group>

<group name="esbc,syslog,system_reboot,configuration_changes">

  <rule id="100155" level="0">
    <match>%ESBC-C-</match>
    <description>ESBC: Перезапуск ПО ESBC</description>
  </rule>

  <rule id="100156" level="8">
    <if_sid>100155</if_sid>
    <decoded_as>esbc-reload</decoded_as>
    <match> reload of ESBC </match>
    <description>ESBC: Перезапуск ПО ESBC: пользователь $(user2) из $(cli_source) $(esbc_srcip) запросил перезагрузку модулей ESBC</description>
  </rule>

```

```

</rule>

</group>

<!-- ===== -->
<!-- 2. Изменение состояния системы (reboot/shutdown/commit) -->
<!-- ===== -->
<group name="esbc,syslog,system_reboot,configuration_changes">

  <rule id="100160" level="0">
    <match>%SYS-</match>
    <description>ESBC: Событие изменения состояния системы</description>
  </rule>

  <rule id="100162" level="9">
    <if_sid>100160</if_sid>
    <match>%SYS-C-REBOOT: CLI: System shutdown</match>
    <field name="sys_action">^initiated$</field>
    <description>ESBC: Выключение или перезагрузка устройства инициировано пользователем $(sys_reboot_user) из
$(sys_reboot_source)</description>
    <mitre>
      <id>T1091</id>
    </mitre>
    <group>system_shutdown,</group>
  </rule>

  <rule id="100165" level="9">
    <if_sid>100160</if_sid>
    <match>%SYS-C-REBOOT: CLI: System shutdown</match>
    <field name="sys_action">^scheduled$</field>
    <description>ESBC: Выключение или перезагрузка устройства запланировано пользователем $(sys_reboot_user) из
$(sys_reboot_source) командами at/in</description>
    <mitre>
      <id>T1091</id>
    </mitre>
    <group>system_shutdown,</group>
  </rule>

  <rule id="100163" level="8">
    <if_sid>100160</if_sid>
    <match>%SYS-C-REBOOT: </match>
    <description>ESBC: Перезагрузка устройства по иным причинам: $(sys_reboot_reason)</description>
    <group>system_reboot,</group>
  </rule>

  <rule id="100164" level="7">
    <if_sid>100160</if_sid>
    <match>%SYS-W-EVENT: Configuration is applied</match>
    <description>ESBC: Конфигурация успешно применена на устройстве</description>
    <group>configuration_changes,pci_dss_10.2.5,</group>
  </rule>

  <rule id="100166" level="6">
    <if_sid>100160</if_sid>
    <match>%SYS-W-EVENT: board commit confirmation timer expires in </match>
    <description>ESBC: Установка таймера подтверждения изменения конфигурации: истечёт через 60
секунд</description>
    <group>configuration_changes,</group>

```

```

</rule>

<rule id="100167" level="5">
  <if_sid>100160</if_sid>
  <match>%SYS-W-EVENT: board commit confirmation timer expired</match>
  <description>ESBC: Истечение таймера подтверждения изменения конфигурации, конфигурация отменена</description>
  <group>configuration_changes,</group>
</rule>
</group>

<!-- ===== -->
<!-- 2.5/2.7 Ввод команд commit/confirm (CLI) -->
<!-- ===== -->
<group name="esbc,syslog,configuration_changes">

  <rule id="100170" level="0">
    <match>%CLI-I-CRIT:</match>
    <description>ESBC: Критичное действие в CLI</description>
  </rule>

  <rule id="100171" level="4">
    <if_sid>100170</if_sid>
    <match>commit</match>
    <description>ESBC: Применение изменения конфигурации (commit) пользователем $(user2) из
$(cli_source)</description>
    <mitre>
      <id>T1078</id>
    </mitre>
    <group>configuration_changes,pci_dss_10.2.5,</group>
  </rule>

  <rule id="100172" level="4">
    <if_sid>100170</if_sid>
    <match>confirm</match>
    <description>ESBC: Подтверждение изменения конфигурации (confirm) пользователем $(user2) из
$(cli_source)</description>
    <group>configuration_changes,pci_dss_10.2.5,</group>
  </rule>
</group>

<!-- ===== -->
<!-- 4.5/6.x События ESBC (блокировки, лимиты, действия) -->
<!-- ===== -->
<group name="esbc,syslog,firewall">

  <rule id="100180" level="0">
    <match>%ESBC-W-EVENT</match>
    <description>ESBC: Событие ESBC</description>
  </rule>

  <rule id="100181" level="8">
    <if_sid>100180</if_sid>
    <match>Banned IP record: IP: </match>
    <description>ESBC: Блокировка IP-адреса $(srcip) динамическим брандмауэром: причина $(ban_reason), связанная
запись $(ban_attr_type) '$(ban_attr_name)', число ошибок $(ban_errors)</description>
    <mitre>
      <id>T1220</id>
    </mitre>
    <group>firewall_block,</group>
  </rule>
</group>

```

```

</rule>

<rule id="100182" level="7">
  <if_sid>100180</if_sid>
  <match> record: key: </match>
  <description>ESBC: Блокировка атрибутов динамическим брандмауэром: запись $(esbc_fw_type) '$(esbc_fw_key)',
число связанных адресов $(esbc_ip_count), причина $(ban_reason)</description>
  <group>firewall_block,</group>
</rule>

<rule id="100183" level="3">
  <if_sid>100180</if_sid>
  <match> requested </match>
  <description>ESBC: Пользователь $(user2) выполнил действие в ESBC: $(esbc_action)</description>
  <group>configuration_changes,</group>
</rule>

<rule id="100184" level="3">
  <if_sid>100180</if_sid>
  <match>limit is reached</match>
  <description>ESBC: Срабатывание ограничителя $(limit_type) - $(object_type)$(name_object)</description>
  <group>esbc_limits,</group>
</rule>
</group>

<!-- ===== -->
<!-- 4.1 Защита от DoS/DDoS (screen) -->
<!-- ===== -->
<group name="esbc,firewall,syslog,attack">

  <rule id="100190" level="0">
    <match>%FIREWALL-W-EVENT_WARN: screen</match>
    <description>ESBC: Событие защиты от DoS/DDoS (screen)</description>
  </rule>

  <rule id="100191" level="7">
    <if_sid>100190</if_sid>
    <match> denied </match>
    <description>ESBC: DoS/DDoS-атака заблокирована: атака '$(fw_screen_name)', протокол $(fw_protocol), источник
$(srcip) -> цель $(dstip) (VRF $(fw_vrf))</description>
    <mitre>
      <id>T1498</id>
    </mitre>
    <group>attack,</group>
  </rule>

  <rule id="100192" level="5">
    <if_sid>100190</if_sid>
    <match>detected</match>
    <description>ESBC: DoS/DDoS-атака обнаружена: атака '$(fw_screen_name)', протокол $(fw_protocol), источник
$(srcip) -> цель $(dstip) (VRF $(fw_vrf))</description>
    <group>attack,</group>
  </rule>
</group>

<!-- ===== -->
<!-- 4.2 Срабатывания zone-based firewall -->
<!-- ===== -->

```

```
<group name="esbc,firewall,syslog">

  <rule id="100193" level="0">
    <match>%FIREWALL-I-EVENT_LOG: zone-pair</match>
    <description>ESBC: Событие zone-based firewall</description>
  </rule>

  <rule id="100194" level="7">
    <if_sid>100193</if_sid>
    <match> denied </match>
    <description>ESBC: Трафик заблокирован межзоновым брандмауэром: zone '$(fw_zonepair)', действие denied,
    протокол $(fw_protocol), $(srcip):$(srcport) -> $(dstip):$(dstport) (VRF $(fw_vrf))</description>
    <mitre>
      <id>T1562</id>
    </mitre>
    <group>firewall_denied,</group>
  </rule>

  <rule id="100195" level="4">
    <if_sid>100193</if_sid>
    <match> permitted </match>
    <description>ESBC: Трафик разрешён межзоновым брандмауэром: zone '$(fw_zonepair)', действие permitted,
    протокол $(fw_protocol), $(srcip):$(srcport) -> $(dstip):$(dstport) (VRF $(fw_vrf))</description>
    <group>firewall_permitted,</group>
  </rule>
</group>
```

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для получения технической консультации по вопросам эксплуатации оборудования ООО «Предприятие «ЭЛТЕКС» вы можете обратиться в Сервисный центр компании:

Форма обратной связи на сайте: <https://eltex.ru/support/>

Servicedesk: <https://servicedesk.eltex-co.ru/>

На официальном сайте компании вы можете найти техническую документацию и программное обеспечение для продукции ООО «Предприятие «ЭЛТЕКС», обратиться к базе знаний, оставить интерактивную заявку или проконсультироваться у инженеров Сервисного центра:

Официальный сайт компании: <https://eltex.ru/>

База знаний: <https://docs.eltex-co.ru/display/EKB/Eltex+Knowledge+Base>

Центр загрузок: <https://eltex.ru/download/>