
VB-Trend 2019
plan>b
VolgaBlob
Smart Code
SIEM для продуктов Код Безопасности
Smart Monitor > Splunk > Plan-B

Цели и задачи Smart Code

- Централизованный мониторинг СЗИ Кода Безопасности
- Выявление инцидентов информационной безопасности на основании корреляционных правил
- Сквозная аналитика в режиме реального времени
- Минимизация временных и человеческих ресурсов на диагностику и устранение инцидентов
- Снижение операционных затрат за счет автоматизации процессов обработки и управления событиями ИБ от различных источников

Архитектура решения

- **Smart Monitor** *Core*
- **Smart Monitor** *Incident Manager*
- **Smart Monitor** *Risk Scoring*
- **Smart Monitor** *Inventory*
- **Smart Monitor** *Cyber Security*
- **Smart Monitor** *Penetration Testing*

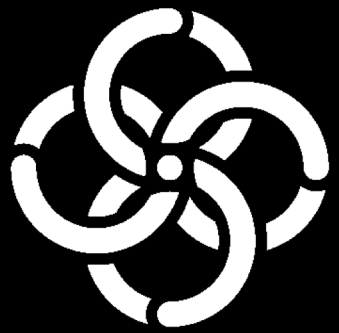
Комплектация SIEM

Интеграция ключевых продуктов

КОД БЕЗОПАСНОСТИ

Единая консоль мониторинга всех средств защиты, управления инцидентами информационной безопасности и оценки соответствия нормативным требованиям

VB-Trend 2019 plan>b VolgaBlob



КОД БЕЗОПАСНОСТИ

VB-Trend 2019
plan>b
VolgaBlob

- Secret Net Studio
- Secret Net LSP

→ СЗИ от НСД

- vGate

→ Защита платформ виртуализации

- АПКШ «Континент»
- СКЗИ «Континент АП»
- СОВ «Континент»

→ Криптозащита каналов связи

- Континент WAF

→ Предотвращение сетевых атак

- Континент TLS

→ Защита WEB-приложений

Возможности Smart Code

VB-Trend 2019 plan>b VolgaBlob

- Сбор, хранение, нормализация событий и метрик производительности от СЗИ Кода Безопасности
- Выявление инцидентов ИБ
- Контроль изменения конфигурации СЗИ
- Контроль соответствия настроек требованиям ИБ
- Корреляции событий безопасности от различных средств защиты
- Отображение статистики

Готовые коннекторы к СЗИ, перенос опыта интеграции Smart Monitor на Open Source-платформу
Наработанные за 6 лет сценарии выявления инцидентов информационной безопасности
Реализовано более 10 проектов, где подобная интеграция уже проведена на Splunk

Описание стенда

СБ SNS
Клиенты SNS

Континент 4.0 МК
Континент 4.0 ЦУС

Континент 4.0
Кластер КШ+СД

Клиенты
Континент АП

Примеры дашбордов

VB-Trend 2019 plan>b VolgaBlob

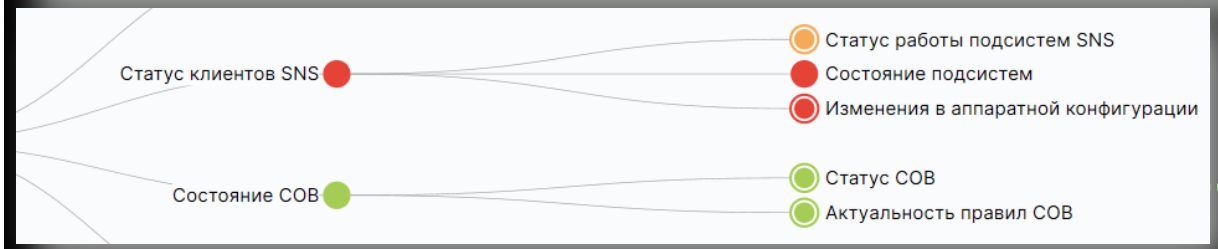
Инциденты

58	21	7
ТРЕВОГА	ПРЕДУПРЕЖДЕНИЕ	НОРМА

Search...

Критичность инцидента | Статус инцидента | Ответственный

Дата и время	Инцидент	Статус	Ответственный
2019-11-11 19:03:00	SmartCode: [SNS] Обнаружен вирус системой SNS на АРМ (ARM7.vbtrend.local)	Новый	Не задан
2019-11-11 19:02:00	SmartCode: [SNS] Обнаружена сетевая атака на АРМ (ARM6.vbtrend.local)	Новый	Не задан
2019-11-11 19:01:00	SmartCode: [SNS] Потеря связи со службой Антивируса на АРМ (ARM10.vbtrend.local)	Новый	Не задан
2019-11-11 16:09:00	SmartCode: [SNS] Антивирусные базы устарели на АРМ (ARM6.vbtrend.local)	Новый	Не задан
2019-11-11 16:08:00	SmartCode: [SNS] Запрет входа пользователя в систему на АРМ (ARM7.vbtrend.local)	Новый	Не задан



Ресурсно-сервисная модель состояния СЗИ

Примеры дашбордов

VB-Trend 2019 plan>b VolgaBlob

События СЗИ

Событие	АРМ	IP источника	IP назначения	Порт назначения	Порт источника	Причина	Подсистема
СОВ заблокировала удаленный узел (событий: 1)	ARM1.vbtrend.local	152.110.40.67	172.10.0.1	11132	7654	Детектор вторжений заметил подозрительную сетевую активность	Детектор сканирования портов
СОВ заблокировала удаленный узел (событий: 1)	ARM3.vbtrend.local	10.15.3.2	172.10.0.3	11654	1132	Детектор вторжений заметил подозрительную сетевую активность	Детектор сканирования портов
СОВ заблокировала удаленный узел (событий: 1)	ARM10.vbtrend.local	124.130.34.9	172.10.0.10	2124	14561	Детектор вторжений заметил подозрительную сетевую активность	Детектор аномального трафика
СОВ заблокировала удаленный узел (событий: 1)	ARM3.vbtrend.local	72.110.2.14	172.10.0.3	11654	5655	Детектор вторжений заметил подозрительную сетевую активность	Детектор DDoS
СОВ заблокировала удаленный узел (событий: 1)	ARM3.vbtrend.local	152.110.40.67	172.10.0.3	11654	7654	Детектор вторжений заметил подозрительную сетевую активность	Детектор сканирования портов

Детальное описание событий и тревог СЗИ

Обнаружен вирус	Зараженный файл перемещен в карантин. Имя процесса: SNS.scan_service.exe. ID процесса: 3224. Файл: /Device/HarddiskVolume2/Install/quake2.exe Вирус: ILOVEYOU. ID файла в карантине: 1.	Антивирус	ARM9.vbtrend.local	User9
Обнаружено новое устройство	Категория конфиденциальности: без учета категории конфиденциальности	Контроль конфигурации	ARM8.vbtrend.local	User8
Обнаружено новое устройство	Категория конфиденциальности: без учета категории конфиденциальности	Контроль конфигурации	ARM8.vbtrend.local	User8
Потеря связи со службой Антивируса	Имя процесса: SNS.scan_worker.exe. ID процесса: 3808.	Антивирус	ARM5.vbtrend.local	User5
Запрет входа пользователя в систему	Имя пользователя: User8 Причина: Не предъявлен идентификатор	Вход/выход	ARM8.vbtrend.local	User8

Примеры дашбордов

VB-Trend 2019 plan>b VolgaBlob

Сертификаты пользователей Континент АП

7	3	2
Активные сертификаты	Истекает в ближайшем месяце	Просроченные сертификаты

Истекающие сертификаты

Серийный номер	УЦ	Выданное имя	Выданный email	Выданная организация	Выданное подразделение	Актуальность	Дата вступления сертификата в силу	Дата окончания срока действия сертификата
0400000000010F8626E60D	RootCA	Иванов Иван	ivanov.i@it-srv.com	ИТ-Сервис	Отдел ИБ	Истекающий	11/05/2019 20:43:07	11/30/2019 20:43:07
02050F0A0051015FEA3621	RootCA	Иван Кравцов	kravcov.i@ity.ru	АйТи Юг	Отдел ИТ	Истекающий	11/04/2019 12:13:07	11/15/2019 12:13:07
0205000100510F56FAE61F	RootCA	Федор Мельников	melnikov.f@ity.ru	АйТи Юг	Отдел ИТ	Истекающий	11/04/2019 10:43:07	11/29/2019 10:43:07

Корреляции событий

Несанкционированный доступ к файлу	1. Запрет доступа к файлу или каталогу. Имя процесса: \device\harddiskvolume2\windows\explorer.exe ID процесса: 3144 Имя объекта: c:\users\sns\desktop\freecommanderportable\секретная информация.txt Запрошенный доступ: Чтение данных Запись данных Разрешенный доступ: Чтение данных Изменение прав доступа 2. Отключена защитная подсистема. Подсистема: Управление файлами Процесс: C:\Program Files\Secret Net Studio\Client\OmsHost.exe 3. Выполнена попытка получения доступа к объекту. Субъект: ИД безопасности: VBTREND\User10 Имя учетной записи: User10 Домен учетной записи: VBTREND Объект: Сервер объекта: Security Тип объекта: File Имя объекта: C:\Документы\Секретная информация.txt Сведения о процессе: Имя процесса: C:\Windows\System32\notepad.exe Сведения о запросе на доступ: Операции доступа: Запись данных (или добавление файла) Добавление данных (или добавление подкаталогов, или создание копии канала)	ARM10.vbtrend.local	User10
Запрещённая печать	1. Запрет печати документа. Имя процесса: C:\Windows\system32\NOTEPAD.EXE ID процесса: 4304 Принтер: Microsoft XPS Document Writer Название документа: eula.1028 — Блокнот Категория конфиденциальности: Неконфиденциально Имя файла: Причина: Пользователю не разрешено печатать на данном принтере 2. Отключена защитная подсистема. Подсистема: Контроль печати Процесс: C:\Program Files\Secret Net Studio\Client\OmsHost.exe 3. Печать документа. Принтер: Microsoft XPS Document Writer АРМ: ARM9.vbtrend.local Пользователь: User9	ARM9.vbtrend.local	User9
Обнаружен вирус	1. Отключена защитная подсистема Антивирус. 2. Включена защитная подсистема Антивирус. 3. Обнаружен вирус. Зараженный файл перемещен в карантин. Имя процесса: SNS.scan_service.exe. ID процесса: 1248. Файл: \Device \HarddiskVolume2\Tmp\eicar2\eicar.com. Вирус: Eicar-Signature. ID файла в карантине: 4.	ARM01.vbtrend.local	СИСТЕМА

Преимущества решения

Гибкая архитектура

- Платформенное решение по обработке логов от всех типов источников
- Встроенные средства управления инцидентами, подсистема уведомлений и отчетности
- Легкая сборка, позволяющая быстро внедрить SIEM силами партнеров и клиентов

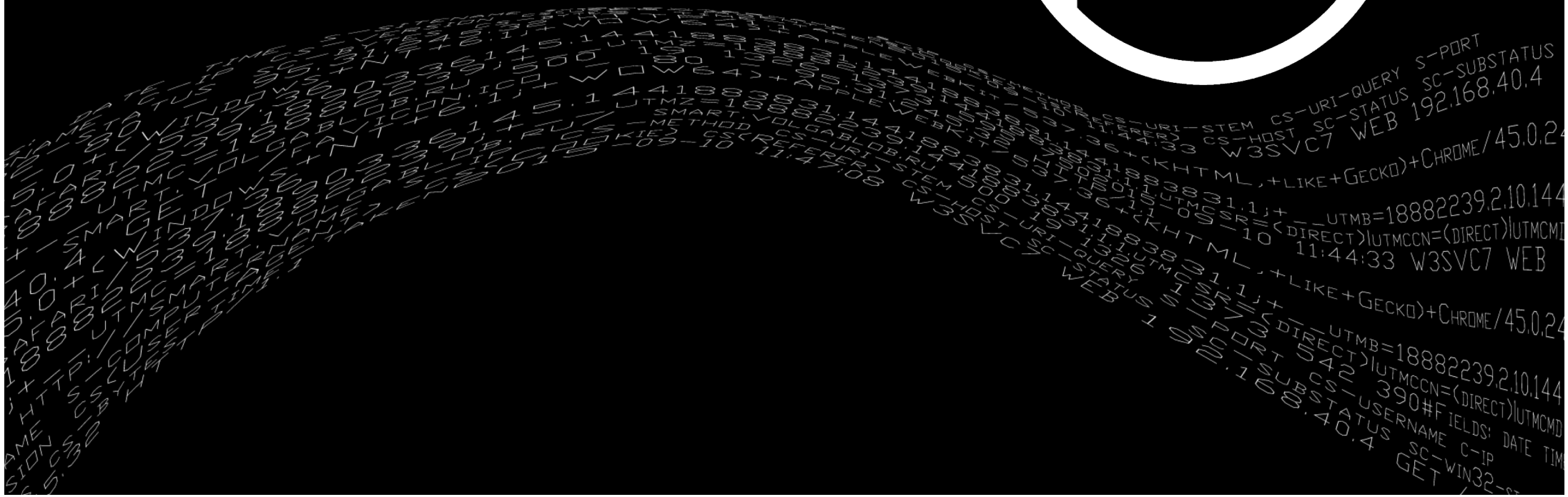
Готовая интеграция с продуктами Код Безопасности

- Готовые коннекторы к СЗИ, перенос опыта интеграции Splunk на Open Source-платформу
- Наработанные за 6 лет сценарии выявления инцидентов информационной безопасности
- Реализовано более 10 проектов, где подобная интеграция уже проведена на Splunk

Российский продукт

- Продукт построен на базе решений с открытым исходным кодом (лицензия Apache)
- В планах 2020 года внесение в реестр российского ПО и сертификация ФСТЭК (ОУД)
- Свидетельство Роспатент, уже есть партнерские и дистрибьюторский договор (RRC)

Демонстрация



Опрос

VB-Trend 2019 plan>b VolgaBlob

Что бы Вы хотели получить СЕГОДНЯ в качестве ПОДАРКА от Романа Лопатина и компании Код Безопасности?

- Бессрочную лицензию Secret Net Studio на 1000 пользователей
- Техническую поддержку на АПКШ Континент любой модели уровня VIP на 3 года
- Лицензию vGate на неограниченного количество CPU

Опрос

VB-Trend 2019
plan>b
VolgaBlob

Чего Вам больше всего не хватает в штатных средствах мониторинга продуктов Кода Безопасности и СЗИ других вендоров?

- ❑ Централизованной консоли мониторинга всех СЗИ Вашей ИТ-Инфраструктуры
- ❑ Средств корреляции событий безопасности от различных СЗИ
- ❑ Возможности управления инцидентами ИБ
- ❑ Ваш вариант

Поделитесь мнением, пожалуйста!

Спасибо за внимание!

Вопросы?

VB-Trend 2019

plan>b

VolgaBlob