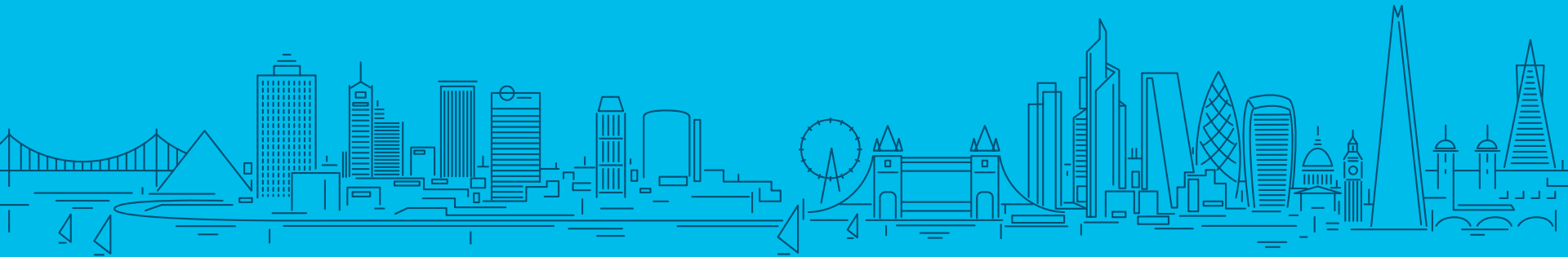


5 советов, от которых зависит успешность вашего SOC

Опыт 100 построенных SOC

Алексей Лукацкий
Бизнес-консультант по кибербезопасности
18 апреля 2019

Сфокусируемся на 3-х темах из 7-ми

Стратегия

Миссия / цели

Команда

Процессы

Окружение

Технологии

Intelligence

Совет 1: сначала внедрите то, что вы хотите мониторить

- Прежде чем строить SOC или отдавать мониторинг на аутсорсинг в внешний SOC (ОЦИБ), сначала внедрите то, что будет отдавать данные

- Для мониторинга МСЭ на периметре и антивируса на ПК SOC не нужен!

Сейчас вы увидите видео

Посчитайте количество передач мяча, сделанных людьми в белых футболках!

Правильный ответ – 16

Вы заметили гориллу?!

Вы заметили уход девушки в черной футболке?!

Вы заметили уход смену цвета штор на заднем плане?!

Совет 2: учитывайте физиологию работы аналитика

- После 12-ти минут непрерывного мониторинга аналитик пропускает 45% активности на мониторе. После 22-х – 95%
- После 20-40 минут активного мониторинга у аналитика наступает психологическая слепота
- Подумайте о ротации смен, режиме отдыха аналитиков и, возможно, замене L1 машинным обучением или иными технологиями

Какие данные собирает ваш SOC?

События ИБ

- МСЭ
- IDS
- AV / EPP / EDR
- DLP
- VPN
- Web-доступ
- Обманные системы
- WAF

Сетевые события

- Маршрутизаторы
- Коммутаторы
- Точки доступа
- DNS-сервера
- Частные облака
- Публичные облака

Приложения и устройства

- Базы данных
- Сервера приложений
- Web-приложения
- SaaS-приложения
- Мобильные устройства
- Десктопы и лэптопы

ИТ-инфраструктура

- Конфигурации
- Геолокация
- Владельцы
- Инвентаризация
- Сетевые карты
- Уязвимости

Особенности обрабатываемых в SOC данных

- Некоторые нормативные акты требуют хранения данных от одного года до семи лет (PCI DSS, HIPAA, SOX и др.)
- Данные для анализа бывают в виде логов (syslog, Event Log и др.), потоков (Netflow, IPFIX и др.), а также захваченных сетевых сессий (pcap)
- Сырые данные необходимо также обогащать за счет внешних источников

«Сколько вешать в граммах» или сколько данных вам нужно собирать?

$$\frac{\text{\# событий безопасности}}{\text{период времени в сек}} = \text{EPS (event per second)}$$

События в день = (Total Peak Events per Day + Total Normal Events per Day) * 110% (про запас) * 110% (на рост)

Total Peak Events per Day = (Number of Peaks per Day * Duration in Seconds of a Peak) * Peak EPS

Total Normal Events per Day = (Total Seconds – Total Peak Seconds per Day) * Normal EPS

На интервале в 90 дней

Знайте ваши средства защиты

- Разный уровень регистрации событий (от Informational до Debug)
- Средняя длина события – 300 байт (может меняться)
- Не забывайте про Flow Per Second (FPS) и PCAP

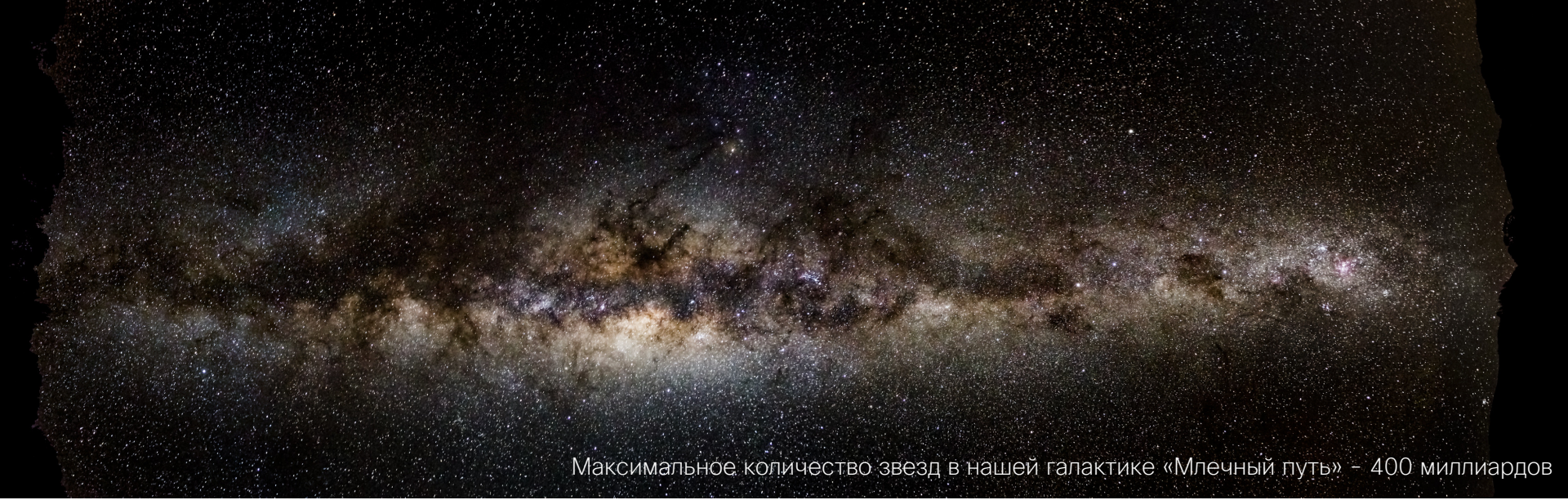
Table 1: Baseline Network Device EPS Averages

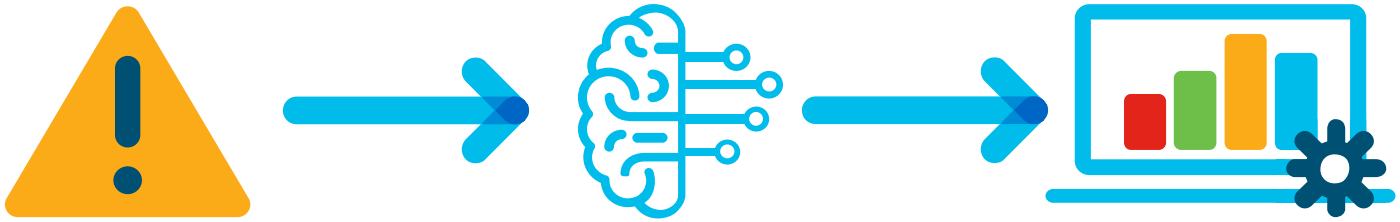
Qty	Type	Description	Avg EPS	Total Peak EPS	Average Peak EPS
750	Employees/Endpoints (Windows XP)	Desktops & laptops at 5 locations	Included at domain servers	Included at domain servers	Included at domain servers
7	Cisco Catalyst Switches	One at each location, one in DMZ and one in the Trusted network	5.09	51.88	26.35
7	Cisco Gateway/Routers	One at each location	0.60	380.50	154.20
5	Windows 2003 Domain Servers	One at each location	40.00	404.38	121.75
3	Windows 2003 Application Servers	In high availability cluster at data center	1.38	460.14	230.07
3	MS SQL Database Servers running on Windows 2003 Server	High availability cluster at data center	1.83	654.90	327.45
6	Microsoft Exchange Servers	One at each location with two (cluster) at the data center	3.24	1,121.50	448.60
3	MS IIS Web Servers on Windows 2003	High availability cluster at data center	1.17	2,235.10	1,117.55
2	Windows DNS Servers	At data center – failover	0.72	110.80	110.80
2	Linux Legacy Application Servers	At data center	0.12	43.60	21.80
1	Linux MySQL Database Server	One in Trusted network for legacy application	0.12	21.80	21.80
7	NitroGuard IPS	One at each location, one in DMZ and one in the Trusted network	40.53	5,627.82	1,607.95
1	Netscreen Firewall	Netscreen facing the Internet	0.58	2,414.00	2,414.00
3	Cisco Pix Firewalls	Between the data center and the other four sites, in front of Trusted network, between Trusted and the DMZ	39.00	1,734.00	1,178.00
1	Cisco VPN Concentrator	Located at data center Facing the Internet	0.83	69.45	69.45
1	Squid Proxy	Located at data center	14.58	269.03	269.03
		Totals:	**149.79**	**15,598.90**	**8,118.80**

Совет 2: продумайте, где вы будете хранить данные до внедрения SOC

Для хранения 1000 EPS (86.4 миллиона событий в день) и средней длине события в 300 байт вам потребуется:

- 25.9 Гб в день
- 777 Гб в месяц
- 9.331 Тб в год





1,2 триллиона событий ИБ

22 инцидента ИБ

Источник: служба ИБ Cisco

Совет 2: продумайте, где вы будете хранить данные до внедрения SOC

- Учтите формат хранения – flat file, реляционная база данных или Hadoop
- Данные можно хранить на своих серверах или в облаке
- Многие SIEMы сжимают данные 1 к 8
- Вам нужно резервирование данных или их длительное хранение?

Угрозы на Cisco **за один день**

Не каждый SIEM подойдет

1.2 триллиона
События безопасности в день по всей сети

28 миллиарда
Netflows анализируется в день (Stealthwatch)

47 ТБ
Internet-трафика инспектируется

7.6 миллиарда
DNS-запросов в день (Umbrella)

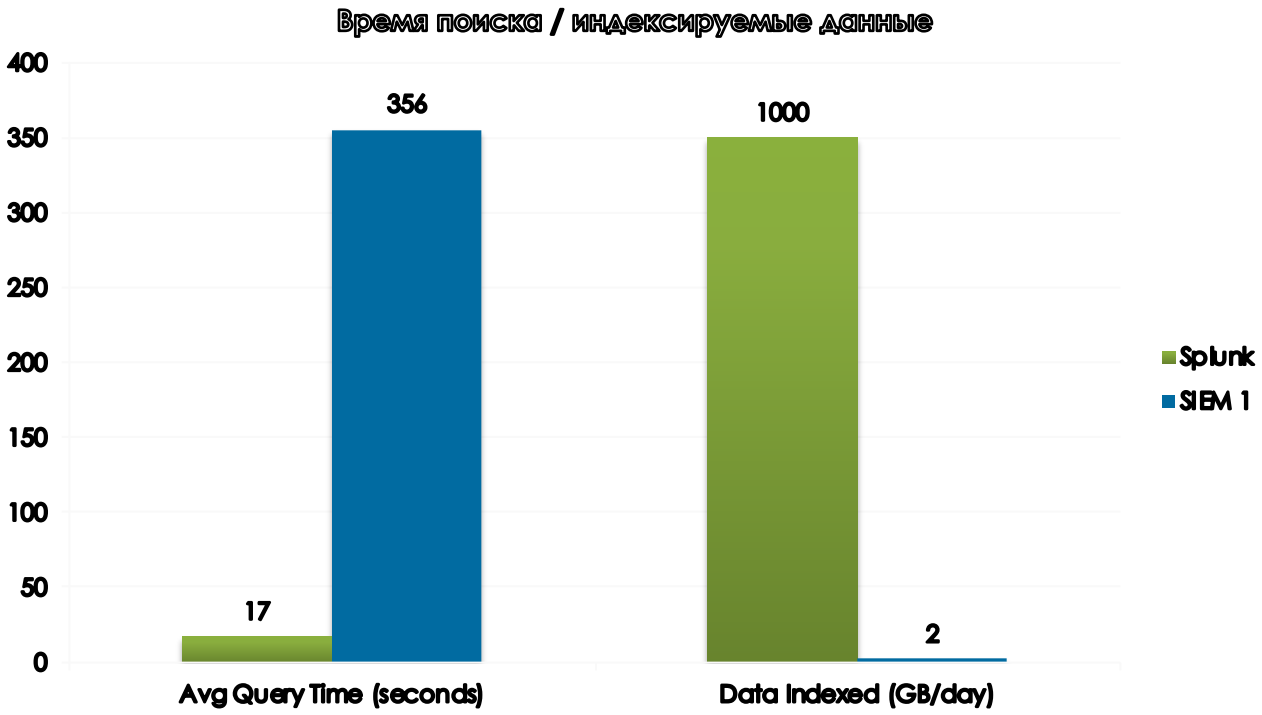
13.4 миллиона
Срабатываний NGIPS в день

4.4 миллиона
Emails получается в день (ESA)
1000 фишинговых писем от службы ИБ

Корзина – индексированные данные

Hot	· Новые индексированные данные · Открыты для записи · Поиск возможен
Warm	· Данные, перенесенные из hot bucket · Данные активно не записываются · Поиск возможен
Cold	· Данные, перенесенные из warm bucket · Данные не записываются · Поиск возможен
Frozen	· Данные, перенесенные из cold bucket · По умолчанию удаляются, но можно настроить на архивное хранение · Поиск невозможен
Thawed	· Данные, восстановленные из архива · Поиск возможен

Время поиска и индексации – ключевые параметры

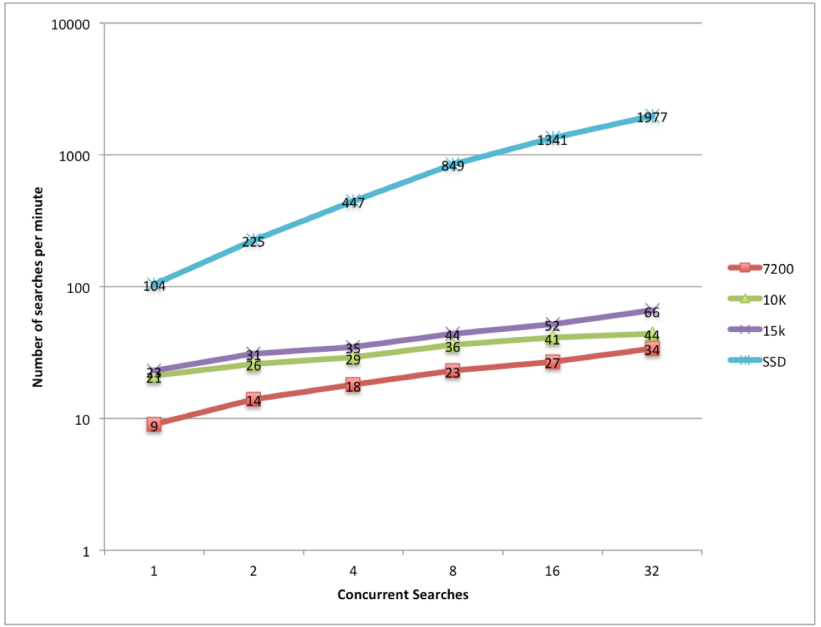


Два типа поиска

- Компактный. Например, «*найди мне среднее время отклика приложения A за последние 24 часа*». Последовательное обращение к диску на чтение.
- «Поиск иголки в стогу сена». Например, «*найди мне UserID во всех моих данных за последний год*». Случайные обращения к диску на чтение.

Выбор дисков для SIEM очень важен

- При компактном поиске разницы между SSD и SATA/SAS HDD почти нет
- При поиску «иголки в стогу сена» диски SSD имеют многократное преимущество (на порядки)



Совет 4: правильно выбирайте жесткие диски

- Чем крупнее объект мониторинга для SOC, тем больше данных будет собираться
- Для небольших объектов может потребоваться поиск на длительном интервале времени
- При крупных объектах или длительном интервале времени поиска лучше выбирать SSD-диски (хоть они и дороже)

Про шифрование тоже подумайте...

Еще одно видео! Смотрите внимательно!

Топ10 use case для SOC

- Мониторинг привилегированных субъектов доступа
- Множественные неудачные попытки аутентификации (brute force)
- Аномалии аутентификации
  - Сервисные учетные записи использованы для интерактивного входа
  - Сервисные учетные записи использованы с неавторизованных систем
  - Пользователь входит в локальную сеть сразу после входа в VPN
  - Пользователь входит в систему за 1+ час до и через 1+ час после нормальных рабочих часов
  - Интерактивный вход сразу из нескольких источников под одной учетной записью

Топ10 use case для SOC

- Аномалии аутентификации (продолжение)
  - Использование учетной записи по умолчанию
  - Использование общих (shared) учетных записей
- Сессионные аномалии
  - Типичный пользователь должен иметь сеанс работы, длительностью около 10 часов
  - Существенное изменение профиля Web-серфинга
  - Всплески в запретах исходящих соединений на МСЭ
  - Сетевые коммуникации между рабочими станциями
  - Превышение разумной длительности сессий

Топ10 use case для SOC

- Аномалии учетных записей
  - Учетная запись используется до начала рабочего дня пользователя
  - Учетная запись используется после конца рабочего дня пользователя
- Индикаторы утечек данных
  - Несоответствие HTTP(S) Send/Receive
  - Протоколы передачи файлов от пользователей или сервисов, которым эти протоколы не требуются (например, FTP с принтера)
  - Использование облачных хранилищ (Яндекс.Диск, Dropbox, OneDrive и т.п.)
- Поиск известных уязвимостей

Топ10 use case для SOC

- Любые чрезмерные отказы сервисов
  - Невозможность обновления антивируса или сбои бэкапов
- Индикаторы внутренней угрозы
  - Доступ к хакерским сайтам или «исследованиям по ИБ» для рядовых пользователей
  - Использование USB
  - Нарушение эталонного уровня аутентификации
  - Отказы аутентификации на file shares, приложениях, серверах, порталах и т.п.
- Отказы в логах безопасности

Use case для DNS-активности (пример)

1. Молодой (менее 7 дней) или недавно зарегистрированный домен
2. Имя не в списке Alexa
3. Странный или длинный домен второго уровня
4. Шестнадцатеричное имя домена
5. Энтропия символов в названии домена
6. Трафик к внешнему IP без запроса DNS
7. Запросы с длинными TXT записями
8. TXT без записи типа A
9. Запросы к динамическим DNS-провайдерам
10. Взаимодействие с вредоносными TLD

Совет 5: SOC не умеет мониторить все – выберите самое важное для вас

- Настройте SOC на обнаружение Топ10 use case – они встречаются у всех
- У вендоров серьезных SIEM есть уже готовые наборы use case – не пренебрегайте ими
- Разработайте use case, которые нужны именно вам

Вопросы?

Где вы можете узнать больше?

Пишите на security-request@cisco.com

Быть в курсе всех последних новостей вам помогут:

- http://www.facebook.com/CiscoRu
- http://twitter.com/CiscoRussia
- http://www.youtube.com/CiscoRussiaMedia
- http://www.flickr.com/photos/CiscoRussia
- http://vkontakte.ru/Cisco
- http://blogs.cisco.ru/
- http://habrahabr.ru/company/cisco
- http://linkedin.com/groups/Cisco-Russia-3798428
- http://slideshare.net/CiscoRu
- https://plus.google.com/106603907471961036146/posts
- http://www.cisco.ru/