Sycope FlowControl: описание использования продукта для мониторинга ИТ инфраструктуры на основе сетевых данных

Клиент:	Национальный исследовательский институт онкологии имени Марии Склодовской-Кюри, Государственный научный институт (филиал в Гливице)
Требования:	Система для анализа сетевого трафика и выявления угроз с помощью протокола NetFlow. Система должна проводить комплексный анализ сетевой инфраструктуры как на общем, так и на детальном уровне. Решение должно быть масштабируемым и должно интегрироваться с продуктами других производителей.
Решение:	Sycope FlowControl
Исполнитель:	АО «Пассус» (Passus S.A)

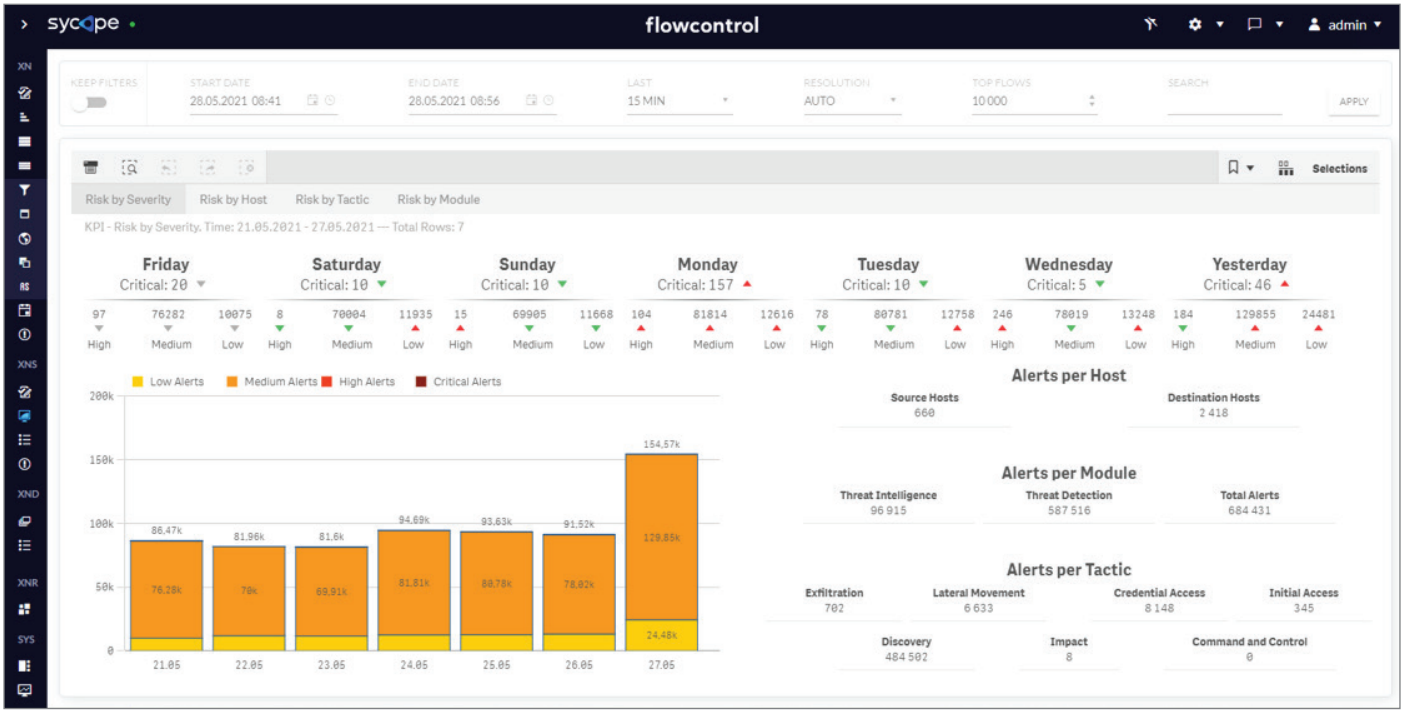
Условия

Национальный исследовательский институт онкологии имени Марии Склодовской-Кюри совместно с Государственным научным институтом (филиалом в Гливице) является одним из ведущих высококвалифицированных клинических исследовательских центров. Он оснащен современной базой оборудования и имеет опытную команду исследователей, сотрудничает со многими научными институтами в Польше и в мире. Одновременно институт известен как один из самых крупных онкологических центров в Польше и за пределами страны, в котором получает лечение огромное количество пациентов с онкологией. Центр участвует в проведении защиты магистерских и докторских диссертаций для нескольких университетов. На данный момент в филиале института в Гливице работают более 120 научных сотрудников, в том числе более 30 профессоров и защитившихся докторов, и 80 сотрудников со степенью доктора наук. Высококвалифицированные научные кадры составляют междисциплинарную команду, которая представляет различные области науки, такие как медицина в широком понимании (клиническая онкология, хирургия, ядерная медицина, медицинская радиология, эндокринологическая онкология) и биомедицина, биотехнология, медицинская физика, химия, биоинформатика и эпидемиология. ИТ-инфраструктура Национального исследовательского института онкологии — это широкая сеть LAN. Эта инфраструктура обслуживает основные приложения с многоуровневой архитектурой для работы института и обеспечивает передачу данных от медицинского и диагностического оборудования, например томографов, приборов магнитно-резонансной томографии и ПЭТ-сканеров, количество которых растет с каждым годом. Это означает, что кроме типичного для крупных организаций трафика, в сети Национального исследовательского института онкологии происходит объемная передача данных, связанная с передачей радиологических изображений, в частности КТ, МРТ, ПЭТ, УЗИ. В планах института — постоянное расширение существующих медицинских систем, требующих передачи изображений и мультимедийного контента в сети IP. Филиал Национального исследовательского института онкологии в Гливице пользуется многими ИТ-продуктами, которые повышают эффективность, отслеживая работу отдельных устройств и приложений. Учитывая характер обрабатываемой информации, безопасность и обеспечение конфиденциальности данных также имеют большое значение.

Ситуация с клиентами

Национальный исследовательский институт онкологии использовал системы мониторинга сетей с помощью анализа пакетов и логов с активных устройств. Огромное количество данных, приходящих из различных систем, приводило к тому, что анализировать их стало сложно и трудоемко. В частности, было трудно предсказать, каково будет влияние запланированного развития медицинской инфраструктуры на эффективность ИТ-инфраструктуры, а впоследствии — и на обслуживание как пациентов института онкологии, так и сотрудников, занимающихся научной работой.

Для филиала Национального исследовательского института онкологии в Гливице важной задачей было знать об источниках нагрузки на сетевую инфраструктуру и понимать, откуда и куда идет увеличенный трафик. В частности, некоторые пользователи сообщали о проблемах с доступностью и эффективностью отдельных услуг. Дополнительным критерием была возможность быстрого обнаружения проблем с производительно-



Ключевое для компании – это быстрый доступ к критичной информации, способной обеспечить защиту. Интерактивный ежедневного обновляемый дашборд отображает события информационной безопасности, разделенные по критичности, хостам, применяемой тактике и модулям.

стью, а также инцидентов и аномалий безопасности. Кроме того, сотрудники института ожидали, что новое решение позволит отслеживать несанкционированную связь, вредоносные программы и хакерские атаки типа брутфорс. Необходимо было найти эффективную и рентабельную систему для мониторинга, с помощью которой можно было бы проводить анализ всего сетевого трафика с точки зрения производительности и безопасности. Также очень важными критериями были интуитивность решения и простота его внедрения: в связи с многочисленными обязанностями сотрудники института не могли бы уделить достаточно времени, необходимого для параметризации и изучения новой системы.

Порядок работ

В соответствии с четкими критериями отбора был объявлен тендер на создание системы для анализа сетевого трафика и отслеживания угроз с помощью протокола NetFlow. Среди компаний, участвующих в тендере, АО «Пассус» с продуктом FlowControl сделало самое выгодное предложение, которое соответствовало функциональным критериям, и выиграло тендер. Внедрение и запуск системы Sycope FlowControl заняли один рабочий день. Это произошло в декабре 2019 года. ИТ-команда института оценила быструю и эффективную установку системы FlowControl, которой можно было пользоваться уже на следующий день после запуска, а простой интерфейс позволил избежать долгого обучения и помог начать сразу использовать полный функционал. Внедрение решения FlowControl не потребовало от Национального исследовательского института онкологии расширения инфраструктуры, что определенно снизило затраты, связанные с запуском системы. Решение анализирует практически весь возможный трафик.

Решения и преимущества

Благодаря системе FlowControl для клиентов стал доступным анализ сетевого трафика с использованием протокола типа NetFlow. Национальный исследовательский институт онкологии начал сбор и анализ данных из сетевых потоков для диагностики причин проблем с сетевыми подключениями и идентификации так называемых трудных участков. Система получила детальную информацию о трафике пользователей, связи между серверами и используемых в организации приложениях.

Преобразуемые дашборды, содержащие статистические данные о том, насколько загружены интерфейсы, доступные сети и сетевые ресурсы, облегчили понимание движения сетевого трафика и управление ими. Благодаря информации, содержащейся в Netflow, были идентифицированы источники и места назначения, а также классы услуг, что позволило быстро определять приложения, ответственные за задержку и снижение производительности. Обнаружение неиспользуемых ресурсов дало возможность увеличить производительность инфраструктуры и сократить расходы на покупку новых мощностей. Система FlowControl также используется для проверки влияния

нововведенных приложений на производительность.

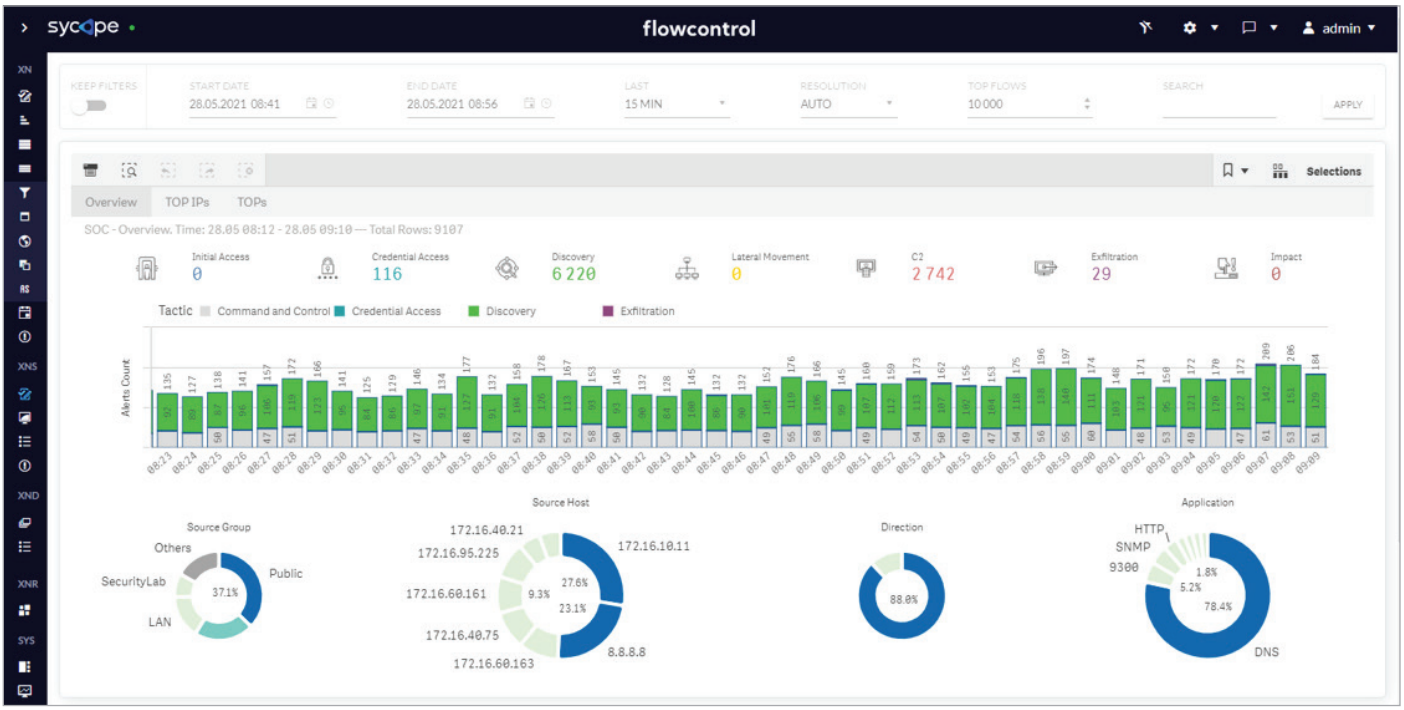
Сейчас система FlowControl в Национальном исследовательском институте онкологии выполняет для ИТ-отдела функцию «врача первой помощи», выявляя участки, требующие дальнейшего анализа. Диаграммы соединений, дополненные соответствующей информацией позволяют определить те области в инфраструктуре, на которые нужно обратить внимание. Большим подспорьем в повседневной работе являются передовые системы поиска, например понятный механизм поиска, как в Google. Более глубокую проверку облегчают инструменты drill-down, которые с помощью одного клика позволяют перейти от общих показателей к детальным анализам статистик и индексов для конкретного порта, интерфейса или IP-адреса.

> *«До внедрения продукта Sycope мы использовали системы, которые хорошо функционировали, но были намного дороже и имели ограниченную эффективность, — сказал Артур Вуйчик (Artur Wójcik), ИТ-специалист, реализующий продукт FlowControl в филиале Национального исследовательского института онкологии в Гливице. — Прежде всего нам было необходимо устройство, которое позволило бы иметь быстрый доступ к данным и хранить их несколько месяцев без построения дополнительной сетевой инфраструктуры. Мы также учитывали то, что в настоящее время мы ищем доступное в ценовом плане решение».*

ИТ-отдел Национального исследовательского института онкологии все больше использует систему FlowControl для обеспечения безопасности. В модуле XNS большую роль выполняет применение методики MITRE, позволяющей оценить риски, которые несет данный конкретный инцидент и сосредоточиться на тех атаках, которые представляют реальную угрозу для критически важных данных и приложений.

В ближайшие месяцы команда планирует адаптировать настройки и алерты с учетом своих требований, что в конечном итоге повысит производительность и эффективность использования системы.

> *«Система, за один день подготовленная к работе, — это непривычно. Мы были очень удивлены легкостью установки и интеграции FlowControl с другими системами», — подчеркнул Артур Вуйчик.*



Диаграммы, индикаторы и таблицы, адаптированные для работы SoC команды и основанные на анализе Netflow позволили заказчику анализировать изменения и тип подозрительных событий ежеминутно.

Компания Sycope специализируется на разработке и внедрении узкоспециализированных ИТ-решений в области мониторинга и улучшения производительности сети и приложений, а также ИТ-безопасности. Создаются локальные решения on-premise в архитектуре и в гибридных средах, а также решения в частных и общедоступных облачных сервисах.

Наши продукты были созданы и разработаны инженерами с более чем 18-летним опытом работы в вопросах производительности сети, эффективности приложений и ИТ-безопасности.

Благодаря решениям по мониторингу производительности приложений APM / NPM и мониторингу производительности сети SIEM мировых поставщиков мы реализовали 400 проектов для таких клиентов, как «Франклин Теплтон Инвестмент» (Franklin Templeton Investment), Национальный банк Польши (Narodowy Bank Polski), «Т-Мобайл» (T-Mobile), «Икея» (Ikea), «Группа ИНГ» (Grupa ING), «Оранж» (Orange) и «Алиор Банк» (Alior Bank). Помимо множества успешных внедрений, компетенции команды были подтверждены многими индивидуальными достижениями, в том числе сертификатами CISA, CISSP, «Ведущий аудитор ISO 27001», IBM Certified Deployment Professional Security QRadar SIEM, ArcSight Certificate AS Data, Platform Technical, Certified Ethical Hacker, Offensive Security Certified Professional.

Инженеры, работающие с крупными сетями и множеством оборудования не нуждаются в отображении всех возможных данных об этих устройствах. Для успешного выполнения своих обязанностей им нужен удобный инструмент, демонстрирующий только то, что важно в данный момент времени.

Адрес: 108811 г. Москва, п. Московский, Киевское шоссе 22-й км., домовл. 4, стр. 2, этаж 9 (девятый), блок В, офис № 925В
web: www.komsvenergy.ru, email: sales@komsvenergy.ru, телефон: +7 (495) 240-55-00
Павел Иванов менеджер продукта +7 (905) 713-72-56, ip@komsvenergy.ru

КОМ СвязьЭнерджи