CTI COMMUNICATIONS TECHNOLOGY INNOVATIONS

ВНЕДРЕНИЕ CISCO SECURE NETWORK ANALYTICS В ИНФРАСТРУКТУРУ АВИАКОМПАНИИ

ЗАДАЧА

Для повышения уровня информационной безопасности авиакомпания AirBridgeCargo (ABC), входящая в группу «Волга-Днепр», приняла решение о внедрении Cisco Secure Network Analytics. Интеграцию в инфраструктуру реализовала компания CTI, золотой партнер Cisco Systems.

«В целом, мы остались довольны решением Cisco Secure Network Analytics, специалисты золотого партнера Cisco компания CTI в сжатые сроки реализовали проект и выполнили необходимые настройки, чтобы мы могли использовать все возможности системы».

Александр Юфаркин, руководитель отдела информационной безопасности авиакомпании AirBridgeCargo

РЕШЕНИЕ

Cisco Secure Network Analytics, являясь решением класса Network Behavior Analysis, обеспечивает непрерывный мониторинг всего сетевого трафика по всем направлениям в реальном времени, значительно повышает прозрачность сети и ускоряет реагирование на вызывающие подозрение инциденты. Создается эталон нормальной веб- и сетевой активности для узла сети, далее применяется анализ на основе контекста для автоматического обнаружения аномального поведения.

Для выявления аномального поведения при использовании встроенных поведенческих сигнатур решению Cisco Secure Network Analytics не требуется «слушать» копию всего трафика и сравнивать его с известными паттернами атак, как это происходит в классических IPS (Intrusion Prevention System), что при распределенной филиальной сети компании AirBridgeCargo является важным преимуществом. Также в современных реалиях удаленной работы и размытого периметра организации оказалась полезной возможность собирать телеметрическую информацию непосредственно с оконечных устройств пользователей. Дополнительное преимущество – выявление вредоносного поведения в зашифрованных по протоколу TLS соединениях, криптомайнинг.

В качестве SOAR-системы было выбрано решение Cisco Secure X, право на использование которого заказчик получает с приобретением лицензий на любой продукт Cisco по ИБ. Cisco Secure X позволяет связать между собой несколько решений Cisco по кибербезопасности, ускорить процедуру расследования и автоматизировать реагирование на инцидент. В дальнейшем AirBridgeCargo планирует интегрировать решение с SIEM-системой для большей детализации и полноты картины происходящего в ИТ-инфраструктуре компании.

«Проект, реализованный нашим Золотым партнером компанией CTI для компании AirBridgeCargo, является хорошим примером того, что информационная безопасность на предприятии может быть не только реально эффективной, но и удобной в повседневном управлении ею».

Михаил Кадер,
заслуженный системный инженер Cisco

РЕЗУЛЬТАТЫ

В результате реализации проекта система позволила выявлять зараженные ПК, скрытые сканирования и предотвратить распространение шифровальщиков, тем самым снизив риски для организации. Помимо решения задач информационной безопасности, система позволяет обнаруживать аномалии в работе сети, осуществлять непрерывный мониторинг производительности сети, выявлять ошибки и/или нарушения сетевой сегментации, обеспечить полноценную видимость и осведомленность о происходящих в сети процессах, коммуникациях. Решение полезно и подразделению ИТ для планирования развития сети, аудитов, выявления некорректно работающего ПО.

т.: +7.495.784.73.13
WWW.CTI.RU, INFO@CTI.RU