Навигация в бурном море событий

Как компания Esri уменьшила шквал оповещений с помощью Cortex XSOAR

ИСТОРИЯ ПРОЕКТА: ПО

Отрасль

- ПО/ГИС

Использованные решения

- Платформа Cortex XSOAR для локального развертывания
- SIEM
- Сетевой мониторинг

Проблемы

- Слишком много оповещений (свыше 10 тысяч в неделю)
- Нехватка квалифицированных аналитиков (всего 5 аналитиков в SOC)
- Обнаружение дубликатов и связанных инцидентов
- Сложное и разрозненное управление индикаторами угроз

Решение

- Автоматизированные сценарии для ускорения закрытия инцидентов и обнаружения ложных срабатываний
- Перекрестная корреляция данных прошлых периодов для обнаружения дубликатов
- Окно коллективной работы для проведения совместных расследований с привлечением накопленных аналитиками знаний

Результаты

- На 95% меньше еженедельных оповещений
- Более эффективная работа аналитиков
- Уменьшение организационных рисков

Заказчик

Esri – глобальная организация, помогающая более чем 350 тыс. заказчиков по всему миру решать сложные проблемы с помощью передовой геопространственной технологии. Учитывая, что свыше 75% компаний из Fortune 500 развертывают решения Esri для достижения своих бизнес-целей, ей было крайне важно обеспечить уровень безопасности, достаточный для защиты разнообразных цифровых активов – как ее собственных, так и тех, что принадлежат ее заказчикам.

Проблема

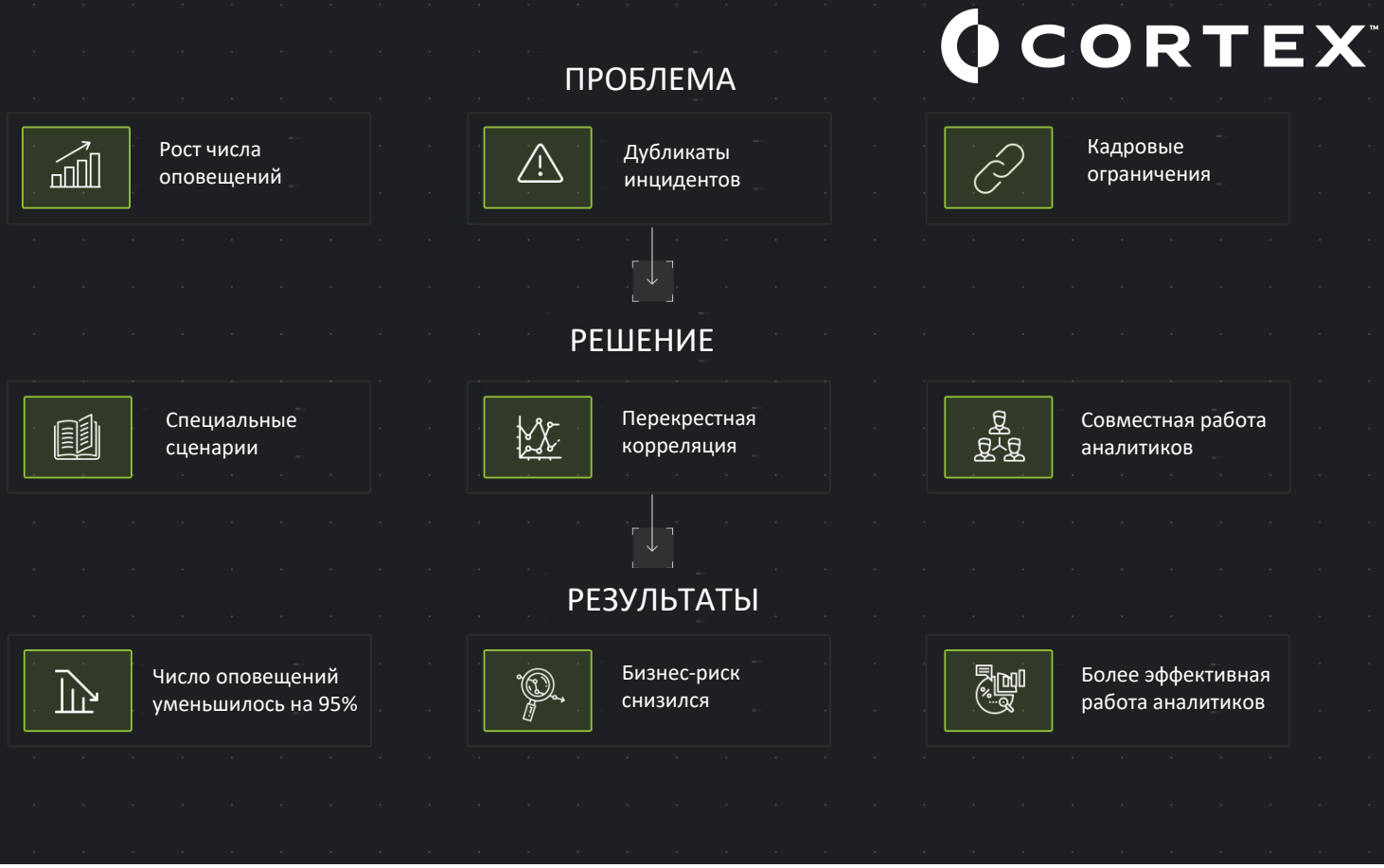
Обширная база заказчиков Esri и активное использование цифровых технологий породили множество проблем безопасности. Из-за лавины оповещений (свыше 10 тысяч в неделю) команда, состоящая из 5 аналитиков SOC, оказалась сильно перегружена. На обнаружение ложных срабатываний и дубликатов инцидентов в этой лавине атак уже не хватало сил. Esri также стремилась упорядочить управление индикаторами угроз, так как текущие сложные и разрозненные процессы не позволяли оптимизировать упреждающий поиск угроз.

Принимаемые полумеры не решали этих проблем. В результате не только повысился бизнес-риск, но и управление текущими ресурсами и SOC было трансформировано неправильно.

Решение

Полная решимости справиться с этими трудностями, компания Esri развернула Cortex XSOAR в дополнение к имеющимся системам сетевого мониторинга и SIEM. Чтобы быстрее сортировать и реагировать на большой объем инцидентов, она запустила специальные сценарии, в которых тесно переплетались как автоматизированные, так и выполняемые вручную задачи. В сценариях также систематизировалась база знаний аналитиков, чтобы можно было единообразно реагировать на те или иные типы атак.

Для обнаружения ложных срабатываний и дубликатов Esri воспользовалась перекрестной корреляцией данных прошлых периодов, доступной в Cortex XSOAR. Оперативно выделяя общие для инцидентов артефакты и индикаторы, аналитики Esri смогли обнаружить и закрыть дубликаты атак, не тратя слишком много времени на повторные расследования.



Для более эффективной работы и обучения аналитиков Esri также использовала Командный центр Cortex XSOAR, где они могут улучшать навыки друг друга и вести совместные расследования. Теперь, вместе работая над сложными инцидентами, аналитики комбинируют разные инструменты защиты и документируют результаты в одном и том же окне, концентрируясь на нетривиальных задачах, требующих интеллектуального подхода.

Результаты

Оркестрация, автоматизация и совместная работа в компании Esri привели к различным улучшениям как объективного, так и субъективного характера. Количество оповещений в неделю снизилось с 10 тыс. до примерно 500 – на целых 95%! Во многом это произошло потому, что на закрытие ложных срабатываний и дублирующихся инцидентов стало уходить гораздо меньше времени благодаря автоматизированным сценариям и перекрестной корреляции данных прошлых периодов.
Более того, все оповещения сейчас поступают прямо в Cortex XSOAR, и аналитикам Esri не нужно самим извлекать информацию из множества систем. Помимо автоматизации и оркестрации, к ИБ-платформе Esri добавился функционал управления заявками, а это значит, что больше НИ ОДНО оповещение не останется незамеченным и не приведет к бизнес-риску.

Автоматизация также помогла разгрузить аналитиков – вместо того, чтобы погрязнуть в ежедневном тушении пожаров, они смогли сфокусироваться на стратегических задачах и непрерывном совершенствовании процессов. Сценарии помогают эффективно соизмерять усилия с задачами, позволяя Esri по максимуму использовать свой самый дефицитный ресурс – квалифицированных аналитиков.

Командный центр Cortex XSOAR повысил удовлетворенность аналитиков. Автоматическое документирование всех действий аналитиков, реализованное в Командном центре, помогает им улучшать навыки друг друга и использовать наработки машинного обучения. Вместо того, чтобы увязнуть в документации и рутинных задачах, аналитики могут больше времени уделять любимому делу – решению действительно сложных проблем.

«Автоматизация, привнесенная платформой Cortex XSOAR в нашу инфраструктуру безопасности, дополняет имеющуюся у нас систему SIEM, позволяя команде SOC действовать эффективнее. Автоматизация этих рутинных задач позволяет нашим аналитикам сосредоточиться на принятии решений»

Шон Колмайер

Руководитель команды реагирования на инциденты, Esri