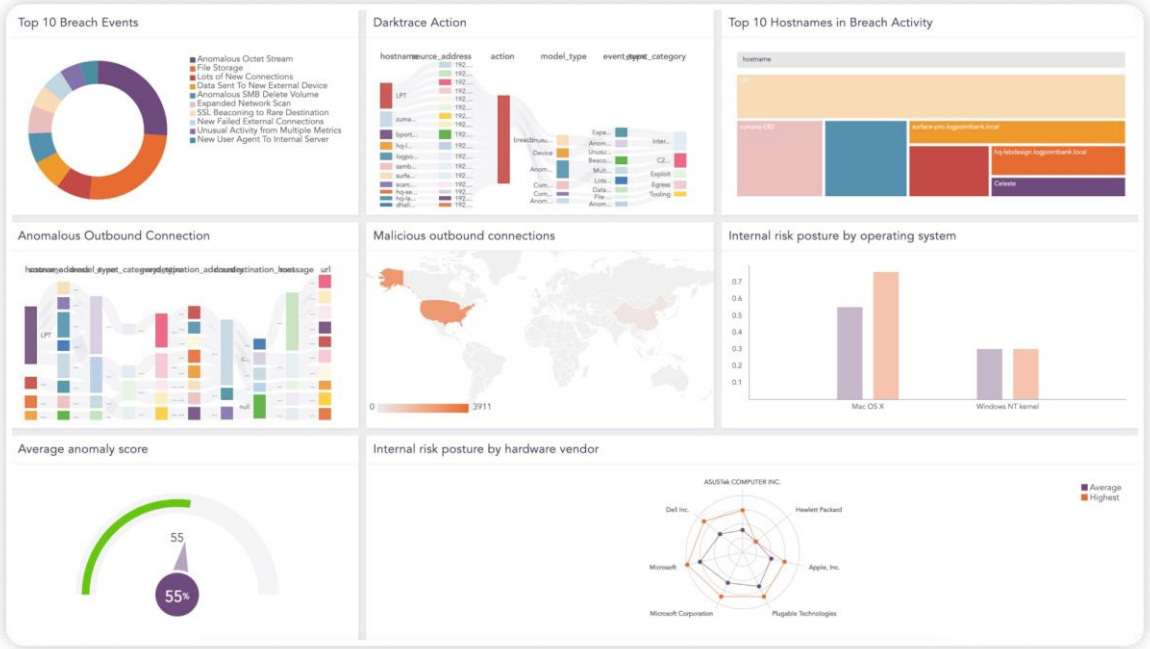
LOGPOINT

LOGPOINT CONVERGED SIEM

Logpoint Converged SIEM помогает командам SOC объединять данные из различных источников. Вместо использования нескольких отдельных продуктов, они теперь имеют единственный источник достоверной информации. Converged SIEM — это единственная унифицированная платформа, которая предоставляет возможности SIEM+SOAR, UEBA, защиты конечных точек и контроля бизнес-корреляций (BCS) для предприятий из единой консоли управления.

ПОВЫСЬТЕ ЭФФЕКТИВНОСТЬ БЛАГОДАРЯ ЕДИНОМУ РЕШЕНИЮ ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ



Logpoint Converged SIEM позволит вам:

- Собирать и централизовать журналы данных.
- Легко соответствовать самым строгим требованиям по соблюдению нормативных требований.
- Обнаруживать самые сложные угрозы с использованием методов машинного обучения.
- Повышать продуктивность SOC с помощью автоматизированной сортировки оповещений.
- Автоматизировать весь процесс обнаружения, расследования и реагирования с помощью готовых плейбуков, нацеленных на самые распространенные случаи использования в области безопасности.

Converged SIEM собирает журналы данных с устройств и приложений по всей ИТ-инфраструктуре. Журналы затем преобразуются в качественные данные через нормализацию и корреляцию. Решение автоматически определяет и отправляет оповещения о инцидентах и аномалиях с использованием алгоритмов машинного обучения. Кроме того, Converged SIEM сопоставляет оповещения с фреймворком MITRE ATT&CK, подключает информацию о киберугрозах и собирает контекстные данные для определения степени серьезности угроз. На основе собранной информации автоматически запускаются необходимые плейбуки для реагирования, что позволяет быстро и безопасно нейтрализовать атаки за считанные секунды.

САМЫЙ ЭФФЕКТИВНЫЙ И ДЕЙСТВЕННЫЙ СПОСОБ ЗАЩИТЫ ВАШЕГО БИЗНЕСА

Командам по безопасности не хватает сотрудников. Этот дефицит кадров означает, что они сталкиваются с трудностями при расследовании инцидентов и оперативном реагировании на угрозы.
Logpoint Converged SIEM автоматизирует трудоемкие и повторяющиеся, но критически важные действия, что позволяет вашей команде более эффективно взаимодействовать и реагировать на инциденты.

Ключевые преимущества

Эффективность масштабирования: Единая платформа, обеспечивающая полную интеграцию данных с конечных точек, SIEM, UEBA и SAP в SOAR.

Комплексная платформа: Благодаря добавлению информации об угрозах, бизнес-контексте и рисках организации слабые сигналы превращаются в значимые расследования.

Постоянное совершенствование продукта: Специальная команда исследователей в области безопасности регулярно обновляет возможности продукта по обнаружению и реагированию, повышая вашу гибкость в противодействии новым угрозам.

Единый инструмент для всех аспектов безопасности вашего бизнеса: Converged SIEM объединяет и автоматизирует процессы обнаружения, расследования и реагирования на инциденты, значительно повышая эффективность и минимизируя риски.

АВТОМАТИЗИРУЙТЕ РАБОТУ СВОЕЙ КОМАНДЫ

Основные характеристики

Оптимизируйте вашу техническую инфраструктуру: Благодаря нашему конвергентному подходу, SIEM, SOAR и UEBA полностью интегрированы в одной платформе для ускорения процессов обнаружения, расследования и реагирования на угрозы (TDIR).

Конфиденциальность данных: Converged SIEM гарантирует полную изоляцию и защиту данных клиентов, соответствуя самым строгим требованиям по защите данных, включая Screms II, Общий регламент по защите данных (GDPR) и Закон о конфиденциальности данных Калифорнии (CCPA).

Поддержка 1.000+ источников данных: Converged SIEM собирает данные с конечных точек, облачных платформ и критически важных бизнес-приложений, обеспечивая защиту всей инфраструктуры с помощью единого инструмента.

Нормализация данных: Converged SIEM нормализует журналы данных в едином стандартизированном формате, что упрощает их корреляцию между приложениями и позволяет выявлять закономерности.

80+ детекторов, использующих машинное обучение: Converged SIEM использует машинное обучение для анализа поведения пользователей с целью выявления известных неизвестных, что позволяет вам быстро реагировать, расследовать и устранять угрозы.

800+ интеграций из коробки: Converged SIEM объединяет разрозненные инструменты и автоматизирует действия.

75+ готовых к использованию плейбуков: Converged SIEM автоматизирует процессы расследования и реагирования, сокращая время реакции с нескольких часов до секунд.

Защита конечных точек: На базе SIEM, SOAR и UEBA наш встроенный агент конечных точек, AgentX, оснащен возможностями обнаружения и реагирования на угрозы на конечных устройствах.