

ArcSight Enterprise Security Manager (ESM)

Комплексная SIEM-платформа ArcSight ESM призвана стать основой центра мониторинга информационной безопасности (SOC). Обладая расширенными возможностями обогащения данных, она сочетает в себе функции обнаружения и анализа угроз в реальном времени, управления процессами безопасности и обеспечения требований регулирующих органов. ArcSight ESM выявляет признаки возникновения инцидентов в реальном времени, позволяя быстрее на них реагировать.



Что нового?

- Информационная панель SOC позволяет администраторам увидеть источники и распределение событий.
- Современная среда SOC оснащена инновационным пользовательским интерфейсом и удобными настройками, в частности, появились темы с контрастным отображением событий.
- Информационная панель управления глобальным **Security Operation Center Manager (SOC)** предоставляет возможность просмотра деталей с использованием разных метрик.

- Поддержка **корпоративного IPv6** способна удовлетворить потребности самых крупных и самых современных предприятий, в том числе владельцев сред с двойным стекком.

Это интересно!

- Теперь ESM поддерживает режим **распределенной корреляции**, в котором можно развернуть несколько экземпляров корреляторов и агрегаторов — это повышает производительность обработки событий безопасности и отказоустойчивость систем защиты.

«Ни один ИТ-директор не хотел бы краснеть и оправдываться перед своим руководством в случае взлома сети компании».

ЭРИК ОГРЕН
Аналитик компании 451 Research

«Ежедневно мы регистрируем 110 миллионов событий безопасности, обеспечивая соблюдение требований банковского законодательства».

Крупный поставщик финансовых услуг

«Нам удалось ускорить поиск нарушений в системе контроля доступа: теперь вместо четырех дней этот процесс выполняется за два часа».

Руководитель медицинской компании