

Решения SEL по обеспечению безопасности



Специалисты и решения SEL помогут вам защитить критически важную инфраструктуру.

- Определение ключевых элементов текущей системы операционных технологий (ОТ) и потенциальных уязвимостей.
- Устранение пробелов с помощью надежных сетевых решений и достижение соответствия стандартам с минимальным нарушением операций.
- Обеспечение соблюдения нормативных требований через централизованное управление активами, обновления программного обеспечения и встроенного ПО, журналы событий и регулярное изменение паролей.
- Обнаружение киберугроз и обеспечение эффективного реагирования и быстрого восстановления системы.



Эти вопросы помогут выявить пробелы в кибербезопасности

РЕСУРСЫ

Какова структура вашей группы кибербезопасности?

Системы ИТ и ОТ имеют разные требования к производительности. Мы можем помочь вам реализовать стратегии кибербезопасности, которые минимизируют прерывания сред ОТ.

Кто управляет вашими коммуникационными системами ОТ?

Ежедневные операции требуют специальных навыков. Мы предлагаем услуги квалифицированных специалистов и ресурсы, которые помогут вам со всеми аспектами вашей системы ОТ.

Кто следит за безопасностью вашей системы?

Правильная организация систем оповещения о событиях имеет решающее значение для ситуационной осведомленности. Мы поможем разработать и внедрить решения мониторинга «под ключ», а также предлагаем услуги мониторинга 24/7/365 через наш Центр управления безопасностью.

ФРЕЙМВОРК

У вас есть фреймворк кибербезопасности ОТ?

Безопасные решения SEL по обеспечению безопасности разработаны на основе фреймворка кибербезопасности, рекомендованного Национальным институтом стандартов и технологий США (NIST), соблюдение которого обеспечивает соответствие другим стандартам фреймворков кибербезопасности, таким как NERC CIP и IEC 62351. Мы можем помочь разработать стратегию внедрения этих решений и обеспечить постоянный мониторинг системы.

Обязаны ли вы соблюдать стандарты кибербезопасности?

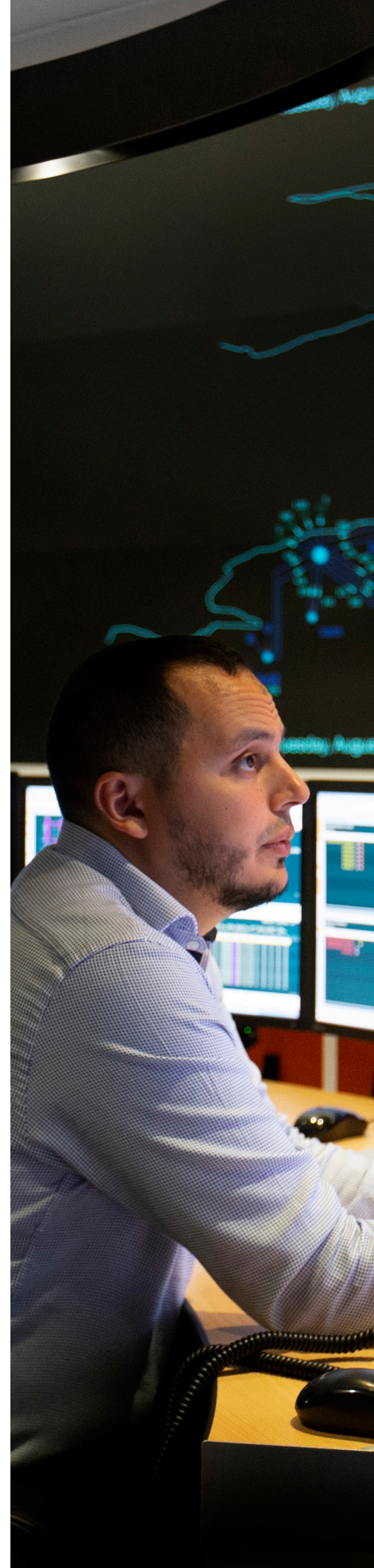
Мы предлагаем услуги анализа на соответствие стандартам кибербезопасности и можем предоставить рекомендации по повышению уровня защиты компьютеров, реле и контроллеров.

Интегрированы ли средства физической защиты в вашу систему кибербезопасности?

Физическая безопасность является частью концепции глубокоэшелонированного подхода к кибербезопасности. Решения SEL формируют целостную систему оценки рисков кибербезопасности с учетом средств физической защиты, а также стихийных и экологических бедствий.

Является ли безопасность цепочки поставок одним из актуальных для вас вопросов?

SEL понимает важность обеспечения безопасности нашей цепочки поставок и следует строгим внутренним и внешним процедурам для поддержания качества наших продукции на должном уровне. Мы - владельцы каждой строки кода нашего программного обеспечения и встроенного программного обеспечения. Этот код имеет цифровую подпись, никогда не передается за пределы SEL и постоянно отслеживается на предмет уязвимостей к новым угрозам. Выбирая решение SEL, вы можете быть уверены, что оно абсолютно надежно.





СЕТЕВОЕ ПРОЕКТИРОВАНИЕ

Когда вы в последний раз проводили сторонний аудит своей сети?

Мы можем провести анализ и аудиты на соответствие нормативным требованиям непосредственно на вашем объекте.

Как вы защищаете сетевые каналы для удаленного доступа?

Среди наших услуг: проектирование сети, консультации и внедрение безопасных криптографических решений для удаленного доступа.

Увеличена ли степень защиты ваших устройств ОТ?

Мы предлагаем сетевые решения, в которых используются программно-определяемые сети (SDN) для внесения в белый список утвержденных сетевых потоков, отключения неиспользуемых портов и служб и устранения нескольких векторов атак, присущих традиционным локальным сетям (LAN).

ПРОЦЕДУРЫ БЕЗОПАСНОСТИ

Каков процесс управления активами ваших систем ОТ?

Управление ресурсами больших систем может являться сложной задачей. Программное обеспечение SEL для управления активами может помочь снизить эксплуатационные расходы и упростить процессы установки обновлений и исправлений.

Как осуществляется управление учетными записями пользователей для доступа к вашим устройствам ОТ?

В сетях ОТ имеется большое количество устройств с несколькими уровнями разрешений доступа. Пароли должны безопасно изменяться на регулярной основе, а права пользователей должны назначаться надлежащим образом. Мы предлагаем централизованное управление учетными записями пользователей, что упрощает работу и контроль учетных записей пользователей.

Как вы управляете версиями системных настроек?

Создание и поддержание базовых настроек системы является ключевым компонентом эффективной владения системой. Мы предлагаем программное обеспечение для управления активами, которое упрощает определение базовой конфигурации системы и контроль версий.

Какой подход вы используете для управления программными обновлениями?

Определение того, какие исправления требуются, и безопасное развертывание обновлений могут быть сложной задачей. В наши услуги управления программными обновлениями входит отслеживание уведомлений об уязвимостях и составление эффективного плана их устранения.

Можете ли вы обнаруживать присутствие киберугроз в своей системе?

Имеется много индикаторов компрометации, указывающих на потенциально вредоносную активность и на известные тактики, используемые злоумышленниками. Решения SEL по обеспечению безопасности обнаруживают вторжения, и мы предоставляем инструкции по процедурам реагирования.

Вы используете закрепляющие тренинги для рассмотрения процессов восстановления системы?

Внедрение политик и процедур имеет наибольший эффект, когда персонал должным образом обучен. Мы предлагаем закрепляющие тренинги для проверки знаний персонала и определения эффективности процедур реагирования. Такие службы, как автоматическое резервное копирование настроек, могут облегчить процесс восстановления системы.

Почему SEL?

Обладая большим опытом в области ОТ и кибербезопасности, мы создаем эффективные решения под ключ, которые повышают уровень кибербезопасности, оптимизируют управление активами и обеспечивают соответствие нормативам. Решение SEL по обеспечению безопасности будет готово защищать от и предотвращать уязвимости без отрицательного влияния на системные показатели ОТ. SEL предлагает широкий спектр решений и услуги высококвалифицированных специалистов для их эффективной реализации.

Следующие шаги

Со специалистами SEL по кибербезопасности ОТ можно связаться электронной почтой secure@selinc.com.