PACIFICA
A NOVENTIQ Company

КАТАЛОГ
решений и услуг

2025

PACIFICA

A NOVENTIQ Company

ОГЛАВЛЕНИЕ

01 О КОМПАНИИ 4

02 АУДИТ И КОНСАЛТИНГ 5-7

03 СОТРУДНИЧЕСТВО С TÜV AUSTRIA 8-9

04 ПРОЕКТИРОВАНИЕ И ВНЕДРЕНИЕ СМИБ 10-13

05 УСЛУГА ПО СОЗДАНИЮ ОЦИБ 14-15

06 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА 16-17

07 ОБУЧЕНИЕ 18-19

08 КИБЕРБЕЗОПАСНОСТЬ 20-21

09 КОНТАКТЫ 22

PACIFICA
A NOVENTIQ Company

О КОМПАНИИ

Компания «ПАЦИФИКА» – это команда профессионалов, которая оказывает полный спектр услуг по информационной и кибербезопасности – от разработки стратегии ИБ, внедрения и сопровождения технических средств защиты информации до оказания консалтинговых услуг по достижению соответствия требованиям международных и отраслевых стандартов информационной безопасности.

Большой опыт

Более 15 лет на рынке ИБ. Более 30 крупных (в т.ч. государственных) клиентов из Республики Казахстан и стран СНГ в различных отраслях экономики, с различной инфраструктурой и уровнем автоматизации

Ведущие технологии

Партнерство с ведущими мировыми вендорами: IBM Security, Check Point, Trellix, Falcongaze, Tenable, CrowdStrike, FUDO Security, CyberArk, Fortinet, R-Vision, Delinea, Bitdefender и др.

Экспертная команда

20 штатных квалифицированных специалистов по системам управления информационной безопасности (СУИБ), системной архитектуре, аналитике, техническому аудиту СУИБ, этичному хакингу, реверс инженерии, администрированию и пр.

Профессиональный интегратор

Не являясь производителем программ и оборудования определенной марки, мы порекомендуем для Вас наиболее подходящие решения для построения СМИБ «с нуля» или оптимизации существующей инфраструктуры

Подтвержденное качество

Международный сертификат соответствия Системы менеджмента требованиям стандарта ISO/IEC 27001:2013, партнерство с Австрийским органом по сертификации и наличие Свидетельства TÜV AUSTRIA Standards & Compliance (№TAP 009-2020-05/25)

Учебный центр

Центр повышения квалификации профессионалов в области информационной безопасности «INTELLA» помогает максимально быстро осваивать новейшие информационные технологии и передавать накопленные знания и опыт

PACIFICA a Noventiq Company. Киберспокойствие Вашего бизнеса.

PACIFICA
A NOVENTIQ Company

АУДИТ И КОНСАЛТИНГ

1 Аудит информационной безопасности

Проводится для получения ответа на вопрос: насколько реальный уровень информационной безопасности (ИБ) в Компании соответствует декларируемому. Результатом оказания услуги является отчет об аудите (Gap-анализ), содержащий сведения о соответствии реального уровня ИБ декларируемому (заданному законодательными НПА, отраслевыми стандартами или внутренними политиками ИБ).

В случае, если Вы еще не определились с нормативным документом, мы готовы провести экспресс-аудит информационной безопасности, по результатом которого Вы получите реальную картину состояния системы менеджмента информационной безопасности и стратегию для дальнейшего развития и повышения уровня соответствия конкретным нормативным требованиям в области ИБ (Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832., ISO 27001:2022, Постановление №48 НБ РК).

2 Подготовка на соответствие Единым требованиям в области информационно-коммуникационных технологий, закона РК «Об информатизации»

В рамках услуги наша компания проводит оценку на соответствие основным «Единым требованиям в области информационно-коммуникационных технологий и обеспечения информационной безопасности» (Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832). Услуга оказывается также с учетом требований и рекомендаций комплекса стандартов ISO/IEC 2700x, СТ РК ISO/IEC 27001:2015.
Результатом работ будет являться отчет с уровнем соответствия ИС нормативной документации, а также подробные рекомендации и практическая помощь в их реализации (подготовка\актуализация внутренней документации, политик и т.д.).

3 Технический аудит информационной безопасности

Включает в себя анализ защищённости приложений, тестирование на проникновение инфраструктуры с применением контролируемых и безопасных атак, а также аудит безопасности ИТ-архитектуры.
По итогам аудита предоставляется отчет с подробной информацией, включающей объективные данные о выявленных уязвимостях и рекомендациями по их устранению.

4 Обеспечение сертификации систем менеджмента информационной безопасности согласно требованиям ISO 27001:2022 (СМИБ)

Этапы реализации проекта:

- проводим разработку документации, требуемой стандартом PCI DSS\помогаем Вам заполнить лист самооценки PCI DSS (при необходимости)
- Проведение предварительного аудита действующих процессов и определение их соответствия требованиям стандарта
- Определение и документирование области применения системы управления информационной безопасностью организации и комплекта соответствующей документации системы управления информационной безопасностью в соответствии с требованиями стандарта ISO/IEC 27001 и пр.
- Проведение оценки рисков информационной безопасности в рамках утвержденной области применения системы управления информационной безопасностью с рекомендациями по уменьшению уровня воздействия рисков на информационную безопасность
- Внедрение системы управления информационной безопасностью, включая внедрение процессов обеспечения информационной безопасности, внедрение средств и мер защиты информации, проведение обучения сотрудников, проведение внутреннего аудита на предмет готовности к сертификации
- Сопровождение в ходе сертификационного аудита, оказание консультационной поддержки
- Обеспечение сертификации СМИБ на соответствие требованиям стандарта ISO/IEC 27001:2022.

5 Услуги по разработке и обеспечению сертификации в сфере систем менеджмента (ISO 9001, ISO 14001, ISO 45001)

Этапы работ при подготовке к сертификации требованиям стандартов ISO:

- Ознакомительная встреча с руководством и сотрудниками для разъяснения основных моментов реализации проекта
- Проведение интервьюирования ключевых сотрудников организации и анализ имеющейся внутренней документации
- Определение процессов системы менеджмента организации и правил их описания
- Разработка необходимого пакета документации, описывающего выполнение требований стандарта\стандартов
- Консультирование ответственных сотрудников организации по вопросам документированной системы менеджмента
- Проведение внутреннего аудита системы менеджмента на предмет подготовки к сертификационному аудиту
- Проведение корректирующих мероприятий, при необходимости
- Сопровождение организации при проведении сертификационного аудита

6 Обеспечение требований информационной безопасности согласно Постановлению №48 Национального Банка РК

В рамках оказания услуги наша компания выполняет:

- Анализ наличия и соблюдения требований по ИБ согласно Постановления №48
- Выработку рекомендаций по итогам обследования с целью обеспечения надлежащего уровня установленных требований
- Подготовку итоговых отчётных данных

7 Создание\оптимизация системы менеджмента информационной безопасности (СМИБ)

Построение комплексной СМИБ в Компании производится в несколько этапов:

- Анализ текущей ситуации и задач в сфере ИБ, выявление неактуальных и дублирующихся документов, формирование перечня недостающих документов
- Актуализация/проектирование процедур обеспечения информационной безопасности
- Определение иерархии и взаимосвязей документов ИБ
- Разработка требуемых документов по ИБ, актуализация положений, регламентов, инструкций в соответствии с изменениями требований законодательства, а также в целях исключения дублирований и противоречий в документах
- Обновление взаимосвязей документов ИБ
- Оформление документации в соответствии с требованиями СТ РК, отраслевыми или корпоративными стандартами
- Разработка рекомендаций и мер по совершенствованию СМИБ в дальнейшем

Результатом оказания услуги является действующая СМИБ, которая обеспечивает:

- расстановку приоритетов Компании в области ИБ
- оптимизацию управленческих процессов, повышение обоснованности расходов на обеспечение информационной безопасности
- достижение «прозрачности» процессов обеспечения и управления ИБ и снижение затрат в этой области
- повышение доверия и уровня удовлетворенности со стороны партнеров и клиентов расширение рыночных возможностей
- обеспечение эффективной защиты информации в критических ситуациях
- своевременное выявление рисков, управление ими, снижение рисков от внешних и внутренних угроз
- упрощенную процедуру сертификации отраслевым стандартам, в случае возникновения необходимости

8 Обеспечение эффективного функционирования процессов, связанных с управлением рисками ИБ (ISO 27005)

В рамки выполнения работ входит, но не ограничивается:

- Разработка нормативной документации, регулирующей процессы инвентаризации и классификации информационных и сопутствующих им активов
- Разработка нормативной документации, регулирующей процессы оценки рисков, связанных с информационными активами
- Консультационная поддержка в формировании реестра активов, подготовке реестра рисков и разработки плана по обработке рисков

PACIFICA
A NOVENTIQ Company

TÜV AUSTRIA

Внедрение систем менеджмента в соответствии с требованиями международных стандартов и последующая сертификация этих систем в TÜV AUSTRIA даёт Компании ряд значительных преимуществ, повышая при этом её капитализацию, конкурентоспособность и уровень доверия со стороны заказчиков, а также помогает привлечь новых клиентов. Однако, Компания не всегда обладает необходимыми ресурсами и опытом для самостоятельного внедрения систем менеджмента, т. к. данный процесс может быть достаточно сложным, длительным и трудоёмким. TÜV AUSTRIA является независимым сертификационным органом и не предоставляет консалтинговые услуги, связанные с подготовкой организаций к их последующей сертификации, строго соблюдая соответствующие правила Международного аккредитационного форума (IAF), поскольку, в противном случае, будет нарушен принцип независимости сертификации. Однако TÜV AUSTRIA всегда готовы оказать информационную поддержку, где и как Компания может получить необходимые консалтинговые услуги.

В этой связи TÜV AUSTRIA Standards & Compliance разработал программу регистрации консультантов, к которым можно обращаться за услугами по подготовке к сертификации. ТОО «ПАЦИФИКА» является зарегистрированным консультантом TÜV AUSTRIA (№ТАР 009-2020-05/25) и проходит регулярные тренинги по эффективному применению международных стандартов и аудиту. Мы поможем вам разработать и внедрить системы менеджмента в соответствии с требуемыми стандартами, обеспечив при этом полную поддержку вашей Компании на пути к сертификации.

Взаимодействие с TÜV AUSTRIA Standards & Compliance позволяет нам с большей эффективностью применять лучшие мировые практики и наработки TÜV AUSTRIA в различных областях при оказании услуг нашим клиентам.

Сотрудничество с TÜV AUSTRIA даёт нашей компании возможность проводить:

- Подготовку организаций к сертификации систем менеджмента по стандартам ISO
- Сертификационные курсы обучения по стандартам ISO (27001, 9001, 14001 и 45001)

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ:

Веб-сайт: www.tuv-austria.ru

УЗНАТЬ БОЛЬШЕ О TÜV

СЕРТИФИКАТ

соответствия системы менеджмента требованиям стандарта ISO/IEC 27001:2013

В соответствии с процедурами TÜV AUSTRIA CERT настоящим подтверждается, что

ТОО ПАЦИФИКА
ул. Ауэзова 60, офис 17А
050008, г. Алматы
Республика Казахстан

Применяет систему менеджмента, соответствующую вышеназванному стандарту в следующих областях:

Оказание профессиональных услуг в области обучения, внедрения, реализации оборудования и программного продукта в сфере IT и информационной безопасности.

Действующее заявление о применимости: V1.0 от 06.09.2021

Регистрационный номер сертификата: TA420213012653

Действителен до 2025-01-10
Дата первичной сертификации: 2022-01-11

Орган по сертификации
TÜV AUSTRIA CERT GMBH

г.Вена, 2022-01-11

Данная сертификация была проведена в соответствии с процедурами аудитирования и сертификации TÜV AUSTRIA CERT GMBH и подлежит регулярным надзорным аудитам.
TÜV AUSTRIA CERT GMBH Deutschstraße 10 A-1230 Wien www.tuv.at

Akkreditierung Austria A 0943 ISO/IEC 17021-1

Online Verification
www.tuv.at/certcheck

ZERTIFIKAT | CERTIFICATE | CERTIFICAT | CERTIFICADO | СЕРТИФИКАТ | شهادة | 证书 | 인증서

PACIFICA
A NOVENTIQ Company

ПРОЕКТИРОВАНИЕ И ВНЕДРЕНИЕ СМИБ

1 Комплексная система управления информационной безопасностью (СМИБ)

Комплексная СМИБ предназначена для снижения рисков реализации полного спектра угроз ИБ. Это достигается за счет совместного применения сразу нескольких технологий и средств защиты информации, развернутых под единым управлением и опирающихся на единую организационно-нормативную базу. Услуга ориентирована на защиту ИТ-инфраструктуры (сеть, ЦОД, пространство рабочих станций), а также предоставляемых на ее базе информационных и телекоммуникационных сервисов (служба каталогов, почта, удаленный доступ, файловое хранилище, сетевая печать, доступ в Интернет) и охватывает не только технологический, но и организационный уровень обеспечения ИБ.

2 Управление событиями информационной безопасности (SIEM)

Услуга необходима Компаниям в тех случаях, когда:

- необходимо обеспечить единую точку сбора, хранения и анализа информации о событиях ИБ, генерируемых ИТ-инфраструктурой и средствами защиты информации
- нужна фактура для расследования инцидентов, при этом требуется обеспечить глубокую ретроспективу «логов» (годы, месяцы)
- необходимо оперативно выявлять аварийные ситуации и инциденты ИБ по данным корреляционного анализа событий
- требуется автоматизировать процесс оценки соответствия требованиям (Compliance)
- в Компании создается оперативный центр ИБ (ОЦИБ/SOC)
- в Компании внедряются процессы управления ИТ на основе ITSM

3 Антивирусная защита (AV)

Услуга предполагает развертывание корпоративной системы, обеспечивающей централизованную антивирусную защиту для рабочих станций, серверов и прикладных шлюзов. Корпоративная антивирусная система снижает риски, связанные с активностью вредоносного ПО, а централизация управления и обновлений позволяет снизить операционные издержки (OpEx).Результатом оказания услуги является эффективно действующая комплексная система антивирусной защиты от вредоносного ПО.

4 Защита от целенаправленных атак (Anti-APT)

Услуга предоставляется в целях точной идентификации APT-атак (Advanced Persistent Threats) для эффективного предотвращения несанкционированного доступа к основным информационным ресурсам Компании. Целевые кибератаки направлены на конкретную компанию или отрасль и гарантируют злоумышленникам в случае успеха получение ценных данных или денежной прибыли. Самыми опасными из целевых атак являются APT – распределенные во времени угрозы. В ходе подобной атаки хакер получает доступ к сети компании, закрепляется в ней и может находиться внутри незамеченным в течение нескольких месяцев или даже лет.
Результатом оказания услуги является настроенный и запущенный комплекс раннего выявления сложных целенаправленных атак (мониторинг сетевого трафика, файлов и анализ исторических данных), который позволит максимально быстро обнаружить присутствие злоумышленника в сети, обеспечит своевременное реагирование и воссоздаст полную картину атаки для детального расследования.

5 Управление корпоративным доступом (IDM)

Услуга предусматривает реализацию различных механизмов идентификации, аутентификации и авторизации в информационных системах и сервисах. Управление доступом позволяет уменьшить риски НСД к важным информационным ресурсам, тем самым снижая возможные потери от разглашения информации, а также помогает оптимизировать бизнес-процессы за счет сквозной аутентификации и автоматизации процессов предоставления корпоративного доступа к ИС, повышая производительность труда.

6 Обеспечение безопасности привилегированного доступа (PAM)

Привилегированный доступ предоставляется ИТ-администраторам, контролирующим значительную часть технологий организации, и другим пользователям, имеющим доступ к критически важным для бизнеса активам.
Злоумышленники часто используют слабые места в системе безопасности привилегированного доступа во время проведения атак с помощью программ-шантажистов, осуществляемых человеком, и целенаправленной кражи данных. Поэтому организации должны сделать защиту привилегированного доступа одним из главных приоритетов безопасности из-за значительного потенциального влияния на бизнес злоумышленников, компрометирующих этот уровень доступа.

7 Контроль защищенности и соответствия стандартам (VM)

Услуга нацелена на создание и запуск в Компании процесса контроля и анализа защищенности в целях подтверждения соответствия мер защиты требованиям руководящих и методических документов, политики ИБ и техническим решениям по защите информации.
В результате внедрения процесса обеспечивается должный контроль за уровнем информационной безопасности, что позволяет подтверждать соответствие требованиям по обеспечению заданного уровня ИБ и оперативно выявлять недостатки в обеспечении ИБ и уязвимости ИТ-систем и сервисов. Тем самым, существенно снижаются риски нарушения ИБ и связанные с ними издержки.

8 Обнаружение и предотвращение вторжений (IDS/IPS)

Целью предоставления услуги является обеспечение ИБ при подключении к внешним информационно-вычислительным сетям (сеть Интернет, сети сторонних организаций, сеть оператора связи) и внутри корпоративной сети за счет обнаружения в сетевом трафике признаков попыток реализации атак.
Установленная и настроенная система предотвращения вторжений позволяет обеспечить раннее обнаружение атак и своевременную реакцию на них до наступления неблагоприятных последствий. Повышается уровень доступности информационных ресурсов и сервисов, за счет чего обеспечивается снижение потерь, связанных с простоями вследствие реализации угроз ИБ.

9 Межсетевое экранирование: защита периметра сети (NGFW)

Целью предоставления услуги является обеспечение ИБ при подключении к внешним информационно-вычислительным сетям за счет управления прохождением сетевого трафика через границу (периметр безопасности) сети.
Услуга удовлетворяет широкий спектр потребностей в обеспечении сетевой безопасности информационно-вычислительных ресурсов.
Кроме того, межсетевое экранирование является обязательным условием выполнения требований по защите персональных данных, применяется при реализации положений законодательства об охране конфиденциальной информации и при реализации требований СТ РК ISO/IEC 27001 и PCI DSS.

10 Предотвращение утечек и шифрование данных (DLP & Encryption)

Услуга предназначена для создания условий по выявлению и блокированию попыток несанкционированного распространения (копирования, передачи) конфиденциальной информации, представляющей для ее владельца коммерческую или иную ценность. Тем самым, на технологическом уровне осуществляется противодействие инсайду, а также профилактика негативных последствий халатного обращения с информацией ограниченного доступа и нарушения правил ее обработки. Ключевая ценность развернутого DLP-решения заключается в минимизации потерь, связанных с утечками данных к конкурентам, в СМИ и в другие нежелательные места.
Результатом оказания услуги является комплекс решений DLP и СКЗИ, который на основе документированных процедур обеспечивает конфиденциальность информации. За счет этого снижаются потери и издержки, связанные с неправомерным доступом к важным данным в случае потери носителей информации, при случайном доступе со стороны неавторизованного персонала вследствие нарушения или халатности, при попытках доступа к данным со стороны лиц, ознакомление которых с защищаемой информацией нежелательно.

11 Защита почтового трафика (SEG)

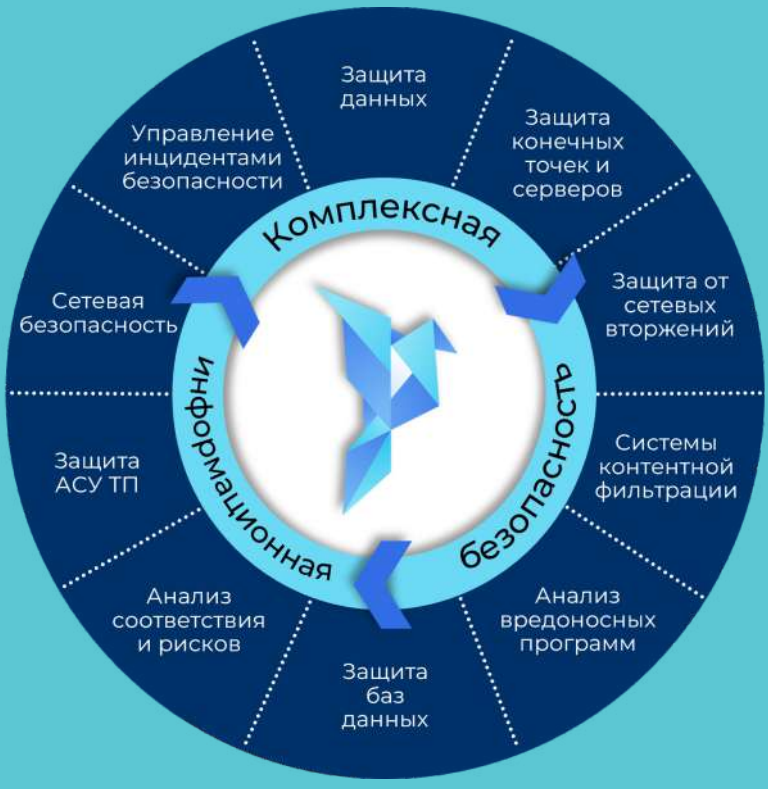
Услуга предоставляется в целях противодействия распространению нежелательной электронной почты и вредоносных вложений.
Результатом оказания услуги является настроенный и запущенный сервис информационной безопасности с проверкой почтового трафика на предмет наличия в нем вирусов и спам-сообщений. Его применение обеспечивает снижение общих издержек и повышение производительности Компании за счет устранения комплекса негативных факторов, связанных с распространением спама и вредоносных вложений.

12 Контроль и защита веб-трафика (SWG)

Услуга предоставляется в целях противодействия распространению нежелательных веб-элементов и устранения комплекса негативных факторов, связанных с веб-трафиком.
Результатом оказания услуги является настроенный и запущенный сервис информационной безопасности ПРОКСИ сервер (WEB GATEWAY). Его применение обеспечивает снижение общих издержек и повышение производительности Компании за счет устранения комплекса негативных факторов, связанных с распространением нежелательных веб-элементов и

13 Защита мобильных устройств (MDM)

Управление мобильными устройствами (Mobile device management, MDM) – набор сервисов и технологий, обеспечивающих контроль и защиту мобильных устройств, используемых организацией и её сотрудниками. Понятие «мобильные устройства» в данном случае подразумевает смартфоны, планшеты и специализированные компьютеры, такие как терминалы сбора данных или мобильные платежные системы.
Услуга предоставляется в целях решения двух основных задач: обеспечение безопасности корпоративных данных на устройствах, находящихся вне сетевой инфраструктуры, а также контроль состояния самих устройств.



НАШИ ПАРТНЕРЫ:

- Check Point
- Trellix
- IBM Security
- Fortinet
- CrowdStrike
- R-Vision
- Radware
- Trend Micro
- Symantec
- ESET
- Forcepoint
- CyberArk
- FUDO Security
- Delinea
- Rapid7
- Falcongaze
- Imperva
- Fidelis
- tLab Technologies
- Phishman
- Claroty
- iBatyr
- HCL
- Senhasegura
- Bitdefender
- Tenable Network Security

PACIFICA
A NOVENTIQ Company

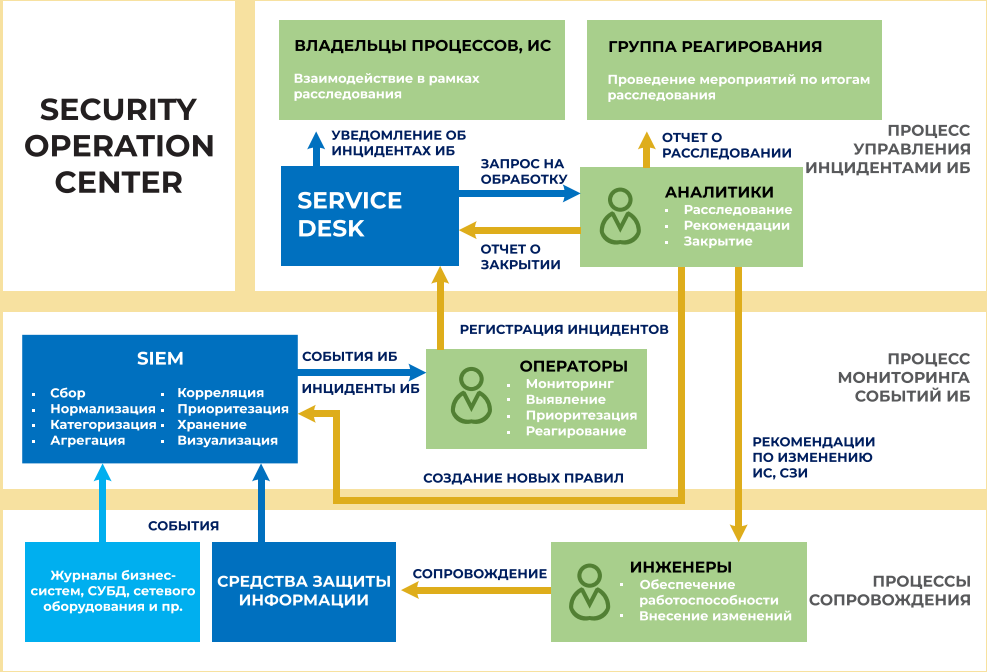
УСЛУГА ПО СОЗДАНИЮ ОЦИБ

Компания «ПАЦИФИКА» оказывает профессиональные услуги в формировании стратегии и построении оперативных центов информационной безопасности в организациях любого уровня, а также, учитывая отраслевую специфику и особенности деятельности организации, действующую политику безопасности и используемые средства защиты, подбирает минимальный набор поисковых средств.

Оперативный центр ИБ (ОЦИБ) или SOC – это центр мониторинга и реагирования на критические инциденты информационной безопасности (ИБ), который позволяет осуществлять постоянный мониторинг и предотвращение атак, включая полный контроль на всех уровнях ИТ: сетевых пакетов, сетевых потоков, активности ОС, контента и поведения пользователей.

Платформа SOC обычно базируется на отказоустойчивой конфигурации SIEM, к которой дополнительно подключены источники данных об актуальных угрозах информационной безопасности (не вызывающих доверия IP, URL и бот-сетях), получаемые от ведущих лабораторий, которые занимаются обнаружением атак и противодействием киберпреступности. Это дает возможность агрегировать информацию об угрозах, выявлять больше инцидентов и обнаруживать атаки нулевого дня (zero-day) в кратчайшие сроки.

Взаимодействие технологий (средств защиты информации и сбора и обработки событий ИБ), людей (квалифицированных специалистов) и процессов представлено на рисунке ниже:



Построение оперативного центра информационной безопасности (ОЦИБ) – непростая комплексная задача. Его невозможно просто купить, его нужно органично встроить в уже работающую экосистему бизнеса, не навредив основным процессам.

Внедряя SOC, организация одновременно должна реализовать часть процессов системы менеджмента ИБ (СМИБ) в соответствии со стандартом ISO 27001 (процесс управления инцидентами ИБ, управление уязвимостями, управление изменениями, контроль соответствия законодательным и отраслевым требованиям), а также соответствовать единым требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности (Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832).

ТИП СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

СРЕДСТВА ЗАЩИТЫ КЛИЕНТОВ ОТ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

01 Решение класса Next-Generation Firewall или Unified Threat Management

02 Система обнаружения угроз на рабочих станциях и реагирования на них (Endpoint Threat Detection and Response)

03 Средство проактивного поиска и обнаружения угроз (Threat Hunting) посредством анализа событий информационной безопасности

04 Средство предотвращения утечки информации (DLP) по техническим каналам

СРЕДСТВА МОНИТОРИНГА И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

05 Система управления событиями информационной безопасности (SIEM)

06 Платформа реагирования на инциденты (IRP)
Повышение эффективности управления, реагирования и расследования на инциденты информационной безопасности

07 Платформа управления информацией об угрозах (Threat Intelligence Platform)
Повышение эффективности обнаружения нетипичных инцидентов информационной безопасности

08 Средство динамического анализа вредоносных программ типа «песочница»

СРЕДСТВА АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ В ИНФОРМАЦИОННЫЕ СИСТЕМЫ И РЕСУРСЫ

09 Сетевой сканер для поиска и классификации сетевых ресурсов

10 Сканер уязвимостей для поиска технических каналов утечки информации

11 Сканер уязвимостей веб-приложений для поиска технических каналов утечки информации в веб-приложениях

12 Средство эксплуатации уязвимостей

PACIFICA
A NOVENTIQ Company

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

1 Поддержка и сопровождение систем менеджмента информационной безопасности (СМИБ)

Заинтересованность в услуге обусловлена необходимостью привлечения узкоспециализированных специалистов ИБ.

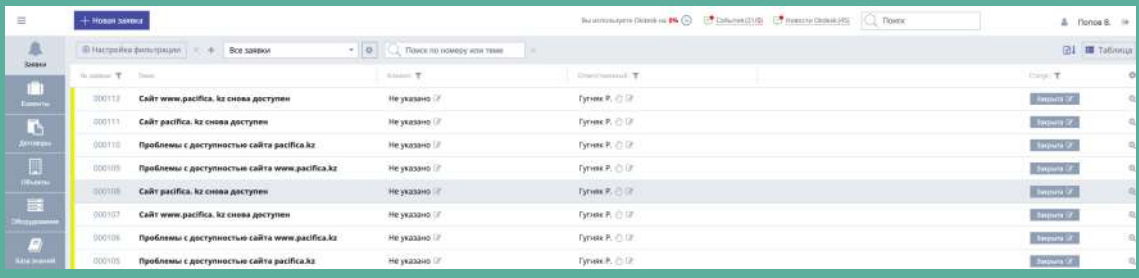
Целевыми установками Заказчика в этом случае являются:

- предотвращение возникновения аварийных ситуаций и инцидентов ИБ
- оптимизация затрат на подготовку кадров
- оптимизация ИБ-инфраструктуры. Решение проблем на стыке производителей, привлекая при необходимости инженеров Trellix, Symantec, IBM Security, Fortinet, Check Point, и др.

Описание услуги

Оптимальная техническая поддержка

- предоставление технических консультаций – письменный (по электронной почте, через веб-ресурс **https://helpdesk.pacifica.kz/** и т. п.) или устный (по телефону) ответ на вопрос по установке, настройке, функционированию или особенностям работы оборудования и программного обеспечения
- предоставление консультаций при диагностике неисправностей, выработке решений по их устранению
- выезды технических специалистов на объекты Заказчика
- прямой доступ к специалистам производителя по всем имеющимся у Заказчика продуктам



Ресурсная техническая поддержка

Предоставляется определенный набор часов и компетенций технических специалистов ТОО «ПАЦИФИКА», которые Заказчик может использовать для:

- выполнения проектных работ
- проведения обследования ИБ-инфраструктуры
- выездов специалистов Исполнителя для штатной технической и консультационной поддержки
- установки (переноса), модернизации ПО, смены версий ПО, установки и настройки нового ПО, первичного администрирования или деинсталляции, и пр.

Инцидентная поддержка

Разовое исполнение услуг по устранению инцидентов на площадке Заказчика.

Результат и его бизнес-ценность

- четкое определение ролей между Заказчиком и Исполнителем (технологическая, финансовая, юридическая)
- снижение затрат на техническую поддержку по сравнению с поддержкой от производителя
- закрепленный за Заказчиком аналитик может помочь разобраться в том, какой вред конкретная вредоносная программа может нанести его бизнесу. Аналитик также может создать специальные сигнатуры для защиты уникальной инфраструктуры Заказчика

2 Расследование инцидентов

Заинтересованность в услуге обусловлена наиболее неблагоприятными обстоятельствами, а именно – обнаружением факта нарушения ИБ или наличием существенных подозрений.

Целевыми установками Заказчика в этом случае являются:

- остановка негативного воздействия, если нарушение продолжается или развивается
- определение обстоятельств и идентификация уязвимостей, способствовавших наступлению события
- определение сценария развития инцидента (реализации атаки)
- поиск виновных должностных лиц, определение источника атаки (идентификация злоумышленника в целях возмещения ущерба)
- сбор доказательств для передачи в правоохранительные органы
- предотвращение возникновения подобных инцидентов в будущем

Описание услуги

Методики расследования инцидентов ИБ варьируются в зависимости от особенностей объекта и условий нарушения. Они ориентированы на получение полной и достоверной (насколько это возможно при данных конкретных условиях) информации о факторах и обстоятельствах, предшествовавших событию и сопровождавших инцидент. Источниками информации служат регистрационные файлы, данные о статистике сетевого трафика, записи в журналах событий средств защиты, операционных систем, СУБД. В некоторых случаях необходимая информация может быть предоставлена сервис-провайдером телекоммуникационных услуг. Кроме того, при расследовании инцидентов проводятся опросы персонала, прямо или косвенно имеющего отношения к обстоятельствам возникновения инцидента. Применяются специализированные технологии восстановления удаленной информации. Полученные данные анализируются, позволяя воссоздать сценарий нарушения. Сформулированные на основе такого анализа выводы докладываются руководству пострадавшей организации.

Результат и его бизнес-ценность

Отчет о расследовании инцидента ИБ (с приложением доказательной информации), содержащий сведения о сценарии нарушения и его причинах, а также рекомендации по улучшению мер защиты информации. Принятие указанных мер обеспечивает снижение возможных потерь от инцидентов ИБ. Кроме того, материалы расследования предоставляют возможность возмещения нанесенного ущерба.

PACIFICA
A NOVENTIQ Company

ОБУЧЕНИЕ

Центр повышения квалификации «INTELLA» создан благодаря накопленному опыту ведущего интегратора по информационной безопасности ТОО «ПАЦИФИКА».
Вектор специализации Центра обучения – подготовка квалифицированных специалистов по информационной безопасности и информационным технологиям (ИБ/ИТ).

1 Тренинги по основам информационной безопасности

- Комплексное обеспечение информационной безопасности в организации
- Основы криптографии
- Практические аспекты защиты АСУ ТП и промышленных сетей
- Подготовка к аудиту по требованиям PCI DSS

2 Тренинги по подготовке к аудиту информационной безопасности и систем менеджмента

- ISO 27001:2022 Системы управления информационной безопасностью.
  Требования. Внедрение. Внутренний аудит
- ISO 27001:2022 Системы управления информационной безопасностью.
  Курс ведущего аудитора
- ISO 27001:2022 Системы управления информационной безопасностью.
  Курс ведущего специалиста по внедрению
- ISO 27005:2022 Информационная безопасность, кибербезопасность и защита конфиденциальности.
  Руководство по управлению рисками информационной безопасности
- ISO 22301:2019 Система менеджмента непрерывности бизнеса.
  Введение, внедрение, внутренний аудит
- ISO 22301:2019 Система менеджмента непрерывности бизнеса.
  Курс ведущего аудитора
- ISO 22301:2019 Система менеджмента непрерывности бизнеса.
  Курс ведущего специалиста по внедрению
- ISO 20000-1:2018 Система управления IT сервисами.
  Введение, внедрение, внутренний аудит
- ISO 20000-1:2018 Система управления IT сервисами.
  Курс ведущего аудитора
- ISO 20000-1:2018 Система управления IT сервисами.
  Курс ведущего специалиста по внедрению
- ISO 31000:2018 Управление рисками.
  Введение, внедрение
- Внутренний аудитор интегрированной системы менеджмента
  (ISO 9001, ISO 14001, ISO 45001)

3 Тренинги по подготовке к сдаче экзаменов по ИБ и ИТ

- CEH. Этичный хакинг и тестирование на проникновение v.13 (с ваучером на сдачу экзамена)
- Подготовительный тренинг к экзаменам CISSP (Exam Prep Course)
- Подготовительный тренинг к экзамену CISM (Exam Prep Course)
- Подготовительный тренинг к экзамену CISA (Exam Prep Course)
- Подготовительный тренинг к экзамену CompTIA (Exam Prep Course)
- Подготовительный тренинг – основы COBIT 2019 (Exam Prep Course)

4 Тренинги по продуктам ведущих производителей ИБ

- Администрирование Trellix (McAfee) Data Loss Prevention
- Администрирование системы контентной фильтрации Trellix (McAfee) Web Gateway
- Администрирование Trellix (McAfee) Network Security Platform
- Администрирование Trellix (McAfee) ATD
- Защита баз данных – Trellix (McAfee) Database Security
- Администрирование системы мониторинга ИБ Trellix (McAfee) SIEM
- Развертывание и администрирование MaxPatrol Enterprise Edition
- Администрирование сетевых экранов Check Point
- Аналитика угроз безопасности Check Point
- Администрирование IBM Security QRadar SIEM
- Основы IBM Security QRadar SIEM
- Разработка контента для IBM Security QRadar SIEM
- Развертывание и администрирование CyberArk Privileged Account Security

5 Результат и его бизнес-ценность

В Центре повышения квалификации «INTELLA» проводятся тренинги по международной сертификации, а также разрабатываются специальные программы обучения, в которых учитывается отраслевая специфика и особенности деятельности организации, принятая политика безопасности и используемые средства защиты, функциональные обязанности и степень ответственности различных категорий специалистов, а также стоящие перед ними задачи.

По итогам обучения выдаются:

- Фирменные свидетельства Центра повышения квалификации «INTELLA»
- Сертификаты компаний-партнеров

КОНТАКТЫ ТОО «INTELLA»

Адрес: г. Алматы, ул. Ауэзова 60, офис 17А
Телефон: +7 (727) 355 02 34
Веб-сайт: www.intella.kz

ПЕРЕЙДИТЕ НА САЙТ

PACIFICA
A NOVENTIQ Company

КИБЕРБЕЗОПАСНОСТЬ

Кибербезопасность представляет собой набор средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые используются для защиты киберсреды, ресурсов организаций и пользователей.
Кибербезопасность подразумевает достижение и сохранение свойств безопасности у ресурсов организации или пользователей, направленных против соответствующих киберугроз.
Основными задачами обеспечения безопасности считаются: доступность, целостность, включающая аутентичность, а также конфиденциальность. Кибербезопасность является необходимым условием развития информационного общества.

Описание услуги

Предупреждение кибератак:

- формирование и поддержание в актуальном состоянии сведений об информационных системах
- формирование и поддерживание в актуальном состоянии моделей угроз и моделей нарушителей для информационных систем
- контроль защищенности информационных систем
- контроль устранения уязвимостей информационных систем
- осуществление мероприятий по повышению квалификации обслуживающего персонала и пользователей информационных систем в части, относящейся к предупреждению, обнаружению и ликвидации последствий кибератак

Обнаружение кибератак:

- сбор и анализ данных журналов аудита, генерируемых программным обеспечением и средствами защиты информационных систем
- обнаружение кибератак на информационные системы, осуществляемых на сетевом и прикладном уровнях
- обнаружение нетипичных кибератак на информационные системы, в том числе – анализ вирусной активности в информационных системах, выявление сложных целенаправленных атак

Реагирование на кибератаки:

- сбор и фиксация сведений об инциденте
- определение границ инцидента и влияния на инфраструктуру
- координация действий ответственных лиц, направленных на устранение и расследование причин кибер-инцидентов

Ликвидация последствий кибератак:

- координация действий ответственных лиц, направленных на противодействие выявленным кибератакам, минимизации возможного ущерба и ликвидации их последствий
- анализ действий нарушителя, определение недостатков в обеспечении информационной безопасности, использовавшихся при проведении атаки
- разработка рекомендаций по предупреждению подобных кибератак и типовым действиям по реагированию на них

При оказании услуги с целью защиты организации от современных угроз в сфере кибербезопасности и утечек данных, при этом также достигая соответствия с законодательными нормативами по защите данных и безопасности, наша компания использует модель «нулевого доверия» (Zero Trust), согласно которой каждый пользователь или устройство должны подтверждать свои данные каждый раз, когда они запрашивают доступ к какому-либо ресурсу внутри или за пределами корпоративной сети.
Стратегия «нулевого доверия» предоставляет существенный уровень защиты против утечек данных и различных современных киберугроз.

МОДЕЛЬ БЕЗОПАСНОСТИ ZERO TRUST БАЗИРУЕТСЯ НА 3 ОСНОВНЫХ ПРИНЦИПАХ:

При внедрении модели безопасности «нулевого доверия» организация должна придерживаться следующих рекомендаций:

- Необходимо обновить каждый элемент стратегии ИБ на соответствие принципам Zero Trust: все ли части текущей стратегии соответствуют вышеописанным принципам «нулевого доверия»? При необходимости их нужно скорректировать.
- Необходимо провести анализ используемого стека технологий и проверить, требуют ли он обновления или замены для достижения Zero Trust: все ли используемые технологии компаний-производителей соответствуют принципам «нулевого доверия»? При необходимости нужно рассмотреть дополнительные решения, которые могут потребоваться для внедрения стратегии Zero Trust.
- Необходимо следовать принципу методичного и осознанного подхода при внедрении Zero Trust: нужно убедиться, что новые поставщики решений также соответствуют выбранной стратегии.

PACIFICA
A NOVENTIQ Company

КОНТАКТЫ

АЛМАТЫ

Адрес: ул. Ауэзова 60, бизнес-центр «Almaty Residence», офис 17А

Телефон: +7 (727) 355 00 11

АСТАНА

Адрес: ул. Алматы 7, бизнес-центр «Seven», офис 903

Телефон: +7 (7172) 64 20 00

Веб-сайт: www.pacifica.kz

ПЕРЕЙДИТЕ НА САЙТ

PACIFICA

A NOVENTIQ Company

www.pacifica.kz