LinkMaster KAZAKHSTAN

VIAVI Solutions

ObserverOne:

NPMD + мониторинг безопасности

Quiz

Термос ЛинкМастер Казахстан

Термос из нержавеющей стали, покрытый синим soft touch, с крышкой.

Удобно брать на учёбу, прогулку или в поход. Металл корпуса удерживает тепло минимум 12 часов

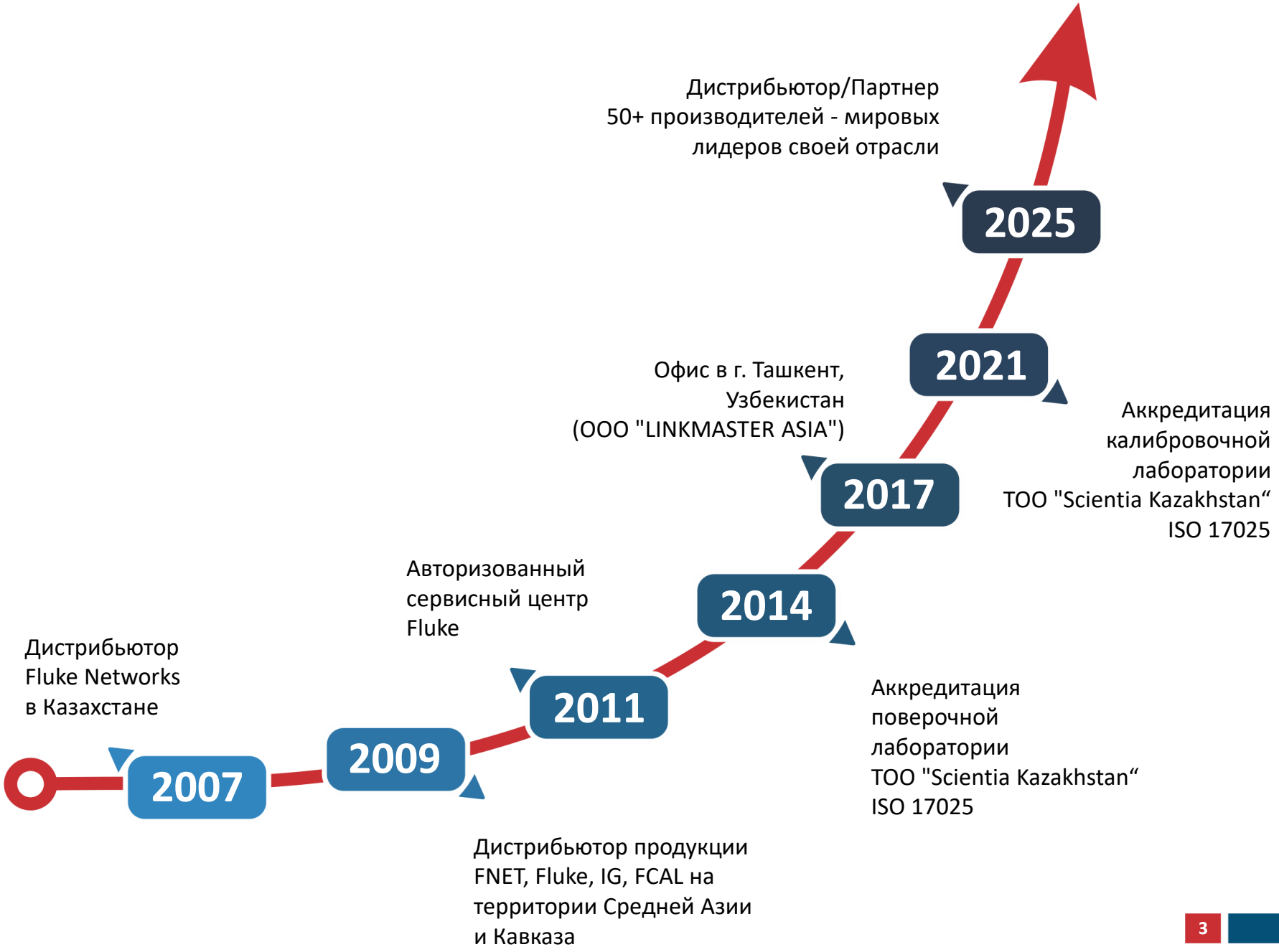
LinkMaster KAZAKHSTAN

О компании

ТОО «**ЛинкМастер Казахстан**» поставляет со склада и под заказ Клиентам в страны Средней Азии и Кавказа следующие виды оборудования: монтажное, тестовое, измерительное, а также программные продукты и комплексы для научно-исследовательской деятельности. Мы предлагаем качественные разработки метрологического обеспечения, испытаний и безопасности в области энергетики, микро- и радиоэлектроники, телекоммуникаций, информационных технологий и IP-телефонии от лидирующих мировых производителей. В нашу компетенцию также входит поверка, калибровка, ремонт всего спектра поставляемого оборудования и обучение принципам работы с ним.

LinkMaster KAZAKHSTAN

История


2007
Дистрибьютор
Fluke Networks
в Казахстане
2009
2011
Авторизованный
сервисный центр
Fluke
Дистрибьютор продукции
FNET, Fluke, IG, FCAL на
территории Средней Азии
и Кавказа
2014
2017
Аккредитация
поверочной
лаборатории
ТОО "Scientia Kazakhstan“
ISO 17025
2021
Офис в г. Ташкент,
Узбекистан
(ООО "LINKMASTER ASIA")
Аккредитация
калибровочной
лаборатории
ТОО "Scientia Kazakhstan“
ISO 17025
2025
Дистрибьютор/Партнер
50+ производителей - мировых
лидеров своей отрасли

Заказчики

- Правительственные организации
- Учреждения образования
- Научно-исследовательские организации
- Авиационные и аэрокосмические организации
- Нефтегазовые предприятия
- Сервисные компании
- Медицинские компании
- Финансовые компании
- Военные компании
- Телекоммуникационные компании
- Подрядные организации
- Гостиничные и выставочные комплексы
- Торгово-развлекательные центры
- Строительные компании
- Энергетические компании
- Спортивные комплексы

LinkMaster KAZAKHSTAN

Структура

СТРУКТУРА ГРУППЫ

LinkMaster KAZAKHSTAN

Мы работаем в 9 регионах

LinkMaster KAZAKHSTAN

Сертификаты

ISO 9001-2015

ISO 14001-2015

OHSAS 18001-2007

ISO 27001-2015

Член СРО ОЮЛ Казахстанский Регистр

ГОСТ ИСО/МЭК 17025-2009

Авторизованный сервисный центр Furukawa Electric Co.

Hangzhou Microimage Software Co., Ltd с торговой маркой HIKMICRO

LinkMaster KAZAKHSTAN

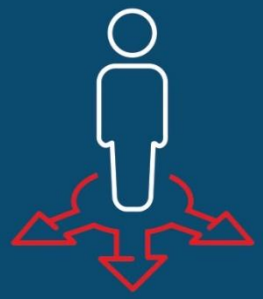
Основные направления деятельности компании

Производители*

KEYSIGHT
HIKMICRO
ETS-LINDGREN
KATMEX
BRADY
FURUKAWA ELECTRIC GROUP
ITECH
EKO
CPI Communications & Power Industries
MILLER
VIAVI Solutions
UNITESS
pendulum
SOFENO
Junkosha Enabling Technology Innovators
RIPLEY
netAlly
HEITRONICS Infrarot Messtechnik
FormFactor
SALTO inspiredaccess
Vectrawave
EMC PARTNER
AEM
IET LABS, INC
Franklin Electric GRID SOLUTIONS
Fanvil
AlbatrossProjects
ProsKit
OSCILLOQUARTZ An ADVA Company
GRAVOTECH by BRADY
Sonel
OST Omnitron Systems
SCHWARZBECK Mess-Elektronik
Cablematic
MICROCHIP
MBW calibration
SUN NUCLEAR A MIRION MEDICAL COMPANY
FLYINGVOICE
maturo
LANGER EMV-Technik
WIKA
Kambič
OHMIC INSTRUMENTS
DINSTAR
SOLAR ELECTRONICS COMPANY
JONARD TOOLS
Gigamon
Process Insights Premium Insights Into Process
HUBER+SUHNER
meatest
SONOMA INSTRUMENT
clavister

LinkMaster KAZAKHSTAN

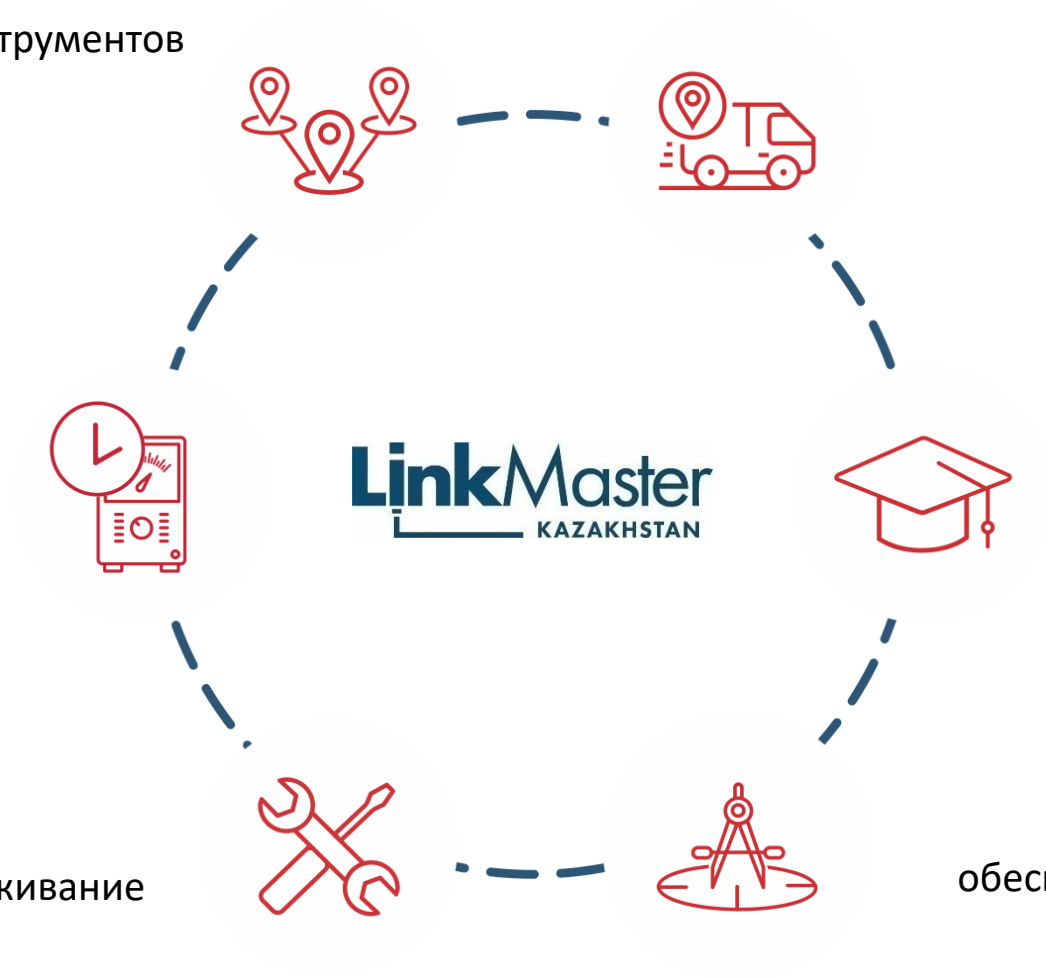
*Основные производители, представляемые ЛинкМастер Казахстан



Кто мы?

Дистрибьюция инструментов и оборудования

Проектирование и поставка систем



Аренда оборудования

Технические тренинги

Сервисное обслуживание (Авторизованный сервисный центр)

Метрологическое обеспечение, поверка и калибровка

LinkMaster KAZAKHSTAN

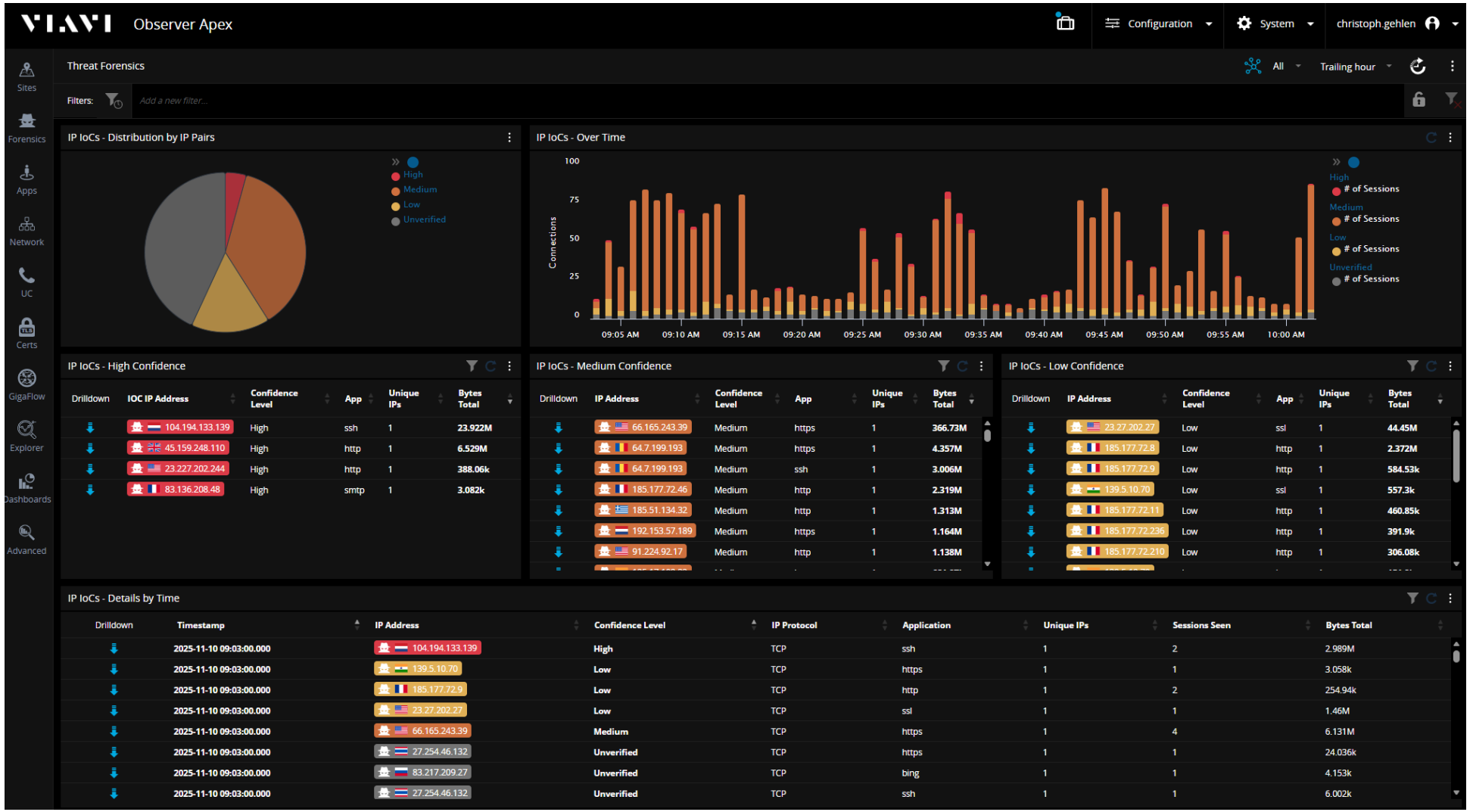
LinkMaster KAZAKHSTAN

VIAVI Solutions

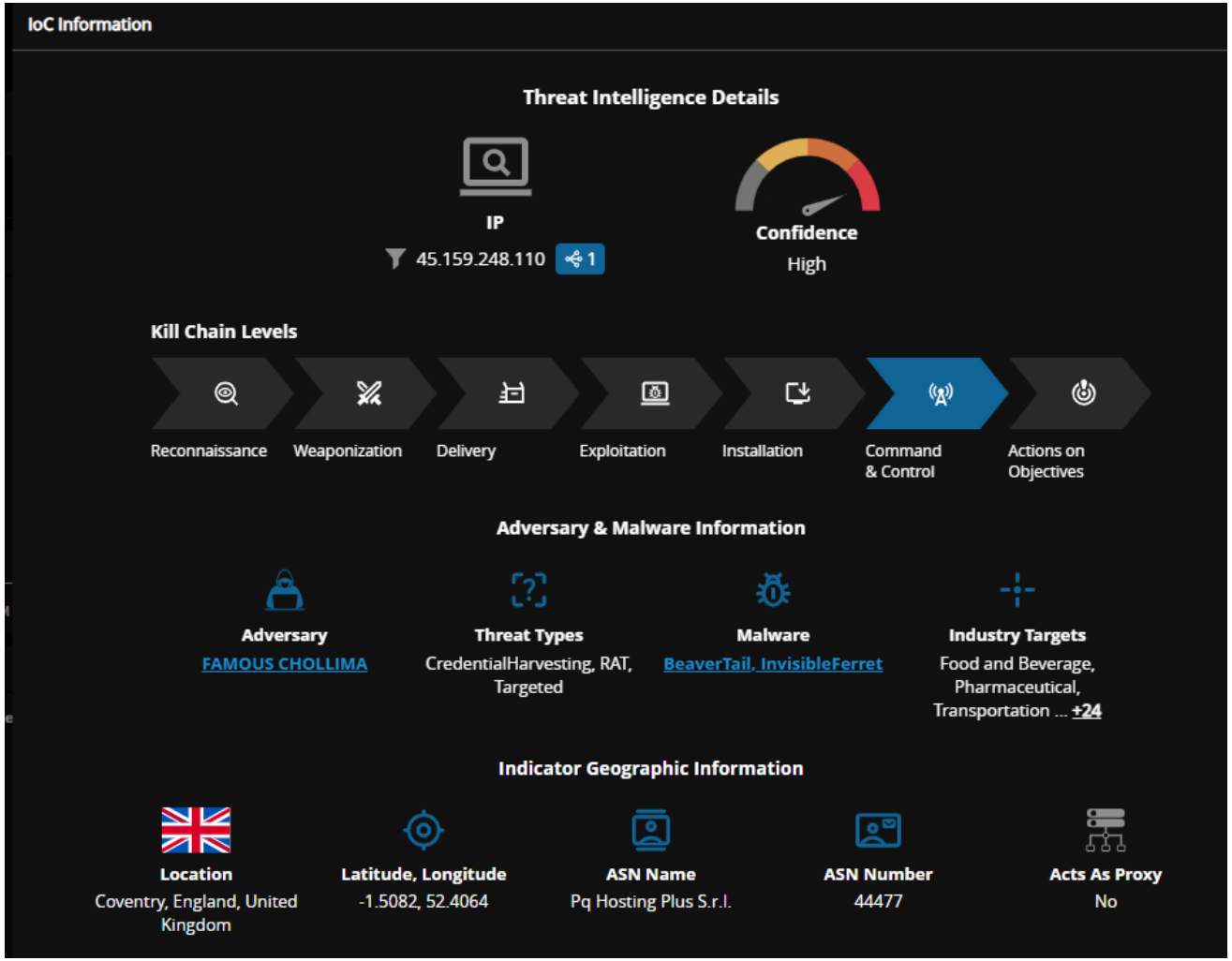
ObserverOne:

NPMD + мониторинг безопасности

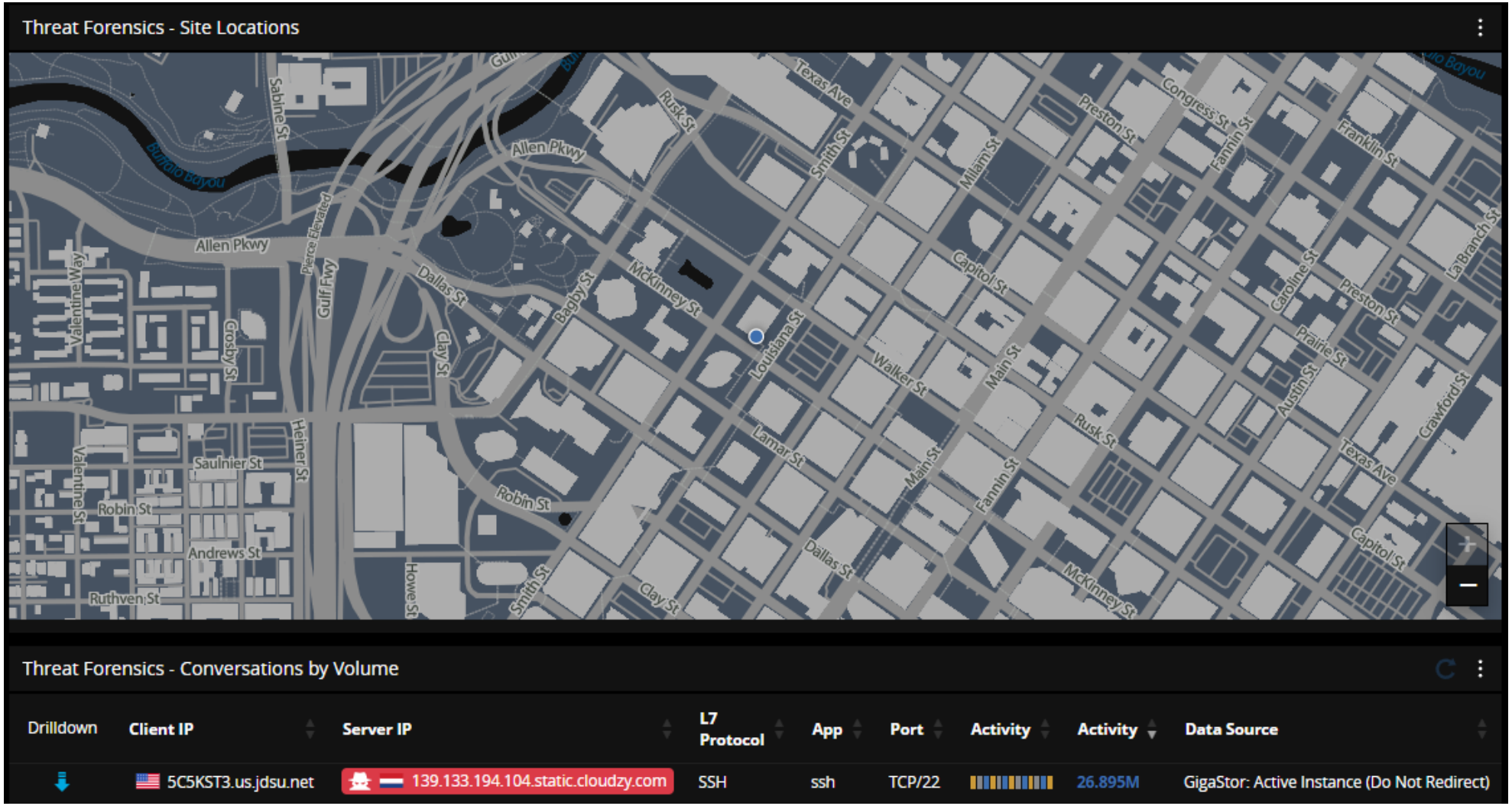
NetSecOps: Мониторинг. Обнаружение. Приоритезация. Исправление



NetSecOps: детальная информация по инциденту нарушения безопасности – что происходит, кто атакует…



NetSecOps: выявление кто в коннекте с атакующим IP



Интегрируется в сторонние системы Apex

- ServiceNow
  - Автоматическое создание инцидентов
    - Apex теперь может создавать инциденты в ServiceNow
    - Автоматическое удаление шума
- Splunk
  - Централизованное оповещение сетевой и ИБ команд
    - Apex пересылает как сетевые, ИБ оповещения в Splunk
    - Данные Apex полностью доступны в любой панели управления Splunk
- CrowdStrike
  - 1-й инструмент для наблюдения за сетью, интегрированный с CrowdStrike Next-Gen SIEM
    - Apex пересылает как сетевые, ИБ оповещения в Next-Gen SIEM
    - Включает настраиваемые панели мониторинга для визуализации событий NetSecOps.
- OKTA (Скоро появится)
  - IAM через OKTA на всей платформе Observer обеспечивает работу MFA и SSO

Пять главных вызовов в области кибербезопасности сегодня

ПЯТЬ ОСНОВНЫХ ВЫЗОВОВ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ НА СЕГОДНЯ

ПО МНЕНИЮ УЧАСТНИКОВ ДАННОГО ИССЛЕДОВАНИЯ

26% Решение проблем истощает ресурсы кибербезопасности, препятствуя улучшению безопасности

24% Увеличение площади атаки из-за роста числа мультиоблачных сервисов и удаленных работников

23% Управление объемом предупреждений о безопасности является сложной задачей

22% Соблюдение нормативных требований часто превосходит лучшие практики в области безопасности

21% Трудности с наймом/удержанием сотрудников по кибербезопасности, обладающих необходимыми навыками

Пять основных проблем в области безопасности, актуальных на сегодня

ПЯТЬ ОСНОВНЫХ ТЕКУЩИХ ПРОБЛЕМ В ОБЛАСТИ БЕЗОПАСНОСТИ (ОБЩИХ/СТРАТЕГИЧЕСКИХ)

ПО МНЕНИЮ УЧАСТНИКОВ ДАННОГО ИССЛЕДОВАНИЯ

28% Увеличение объема и сложности предупреждений о безопасности.

28% Растущее использование публичных облачных сервисов.

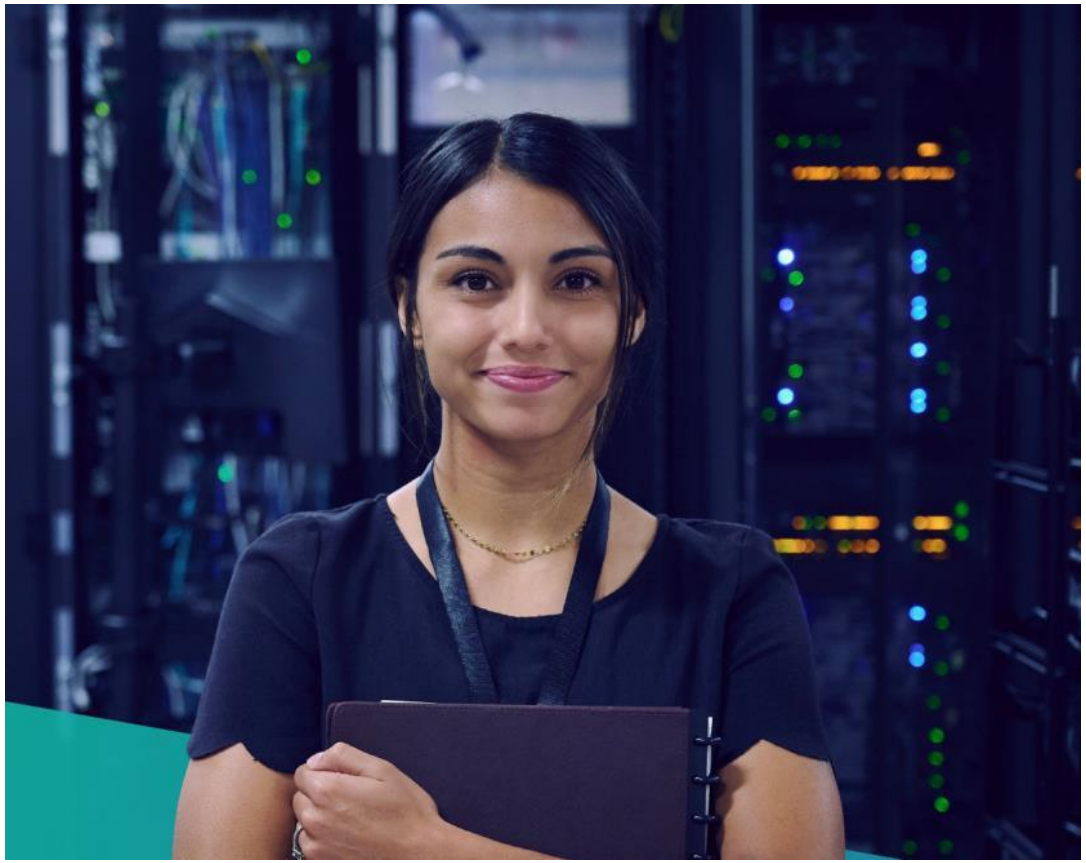
27% Рост объема данных, связанных с безопасностью.

26% Найм, обучение и удержание достаточного количества квалифицированного персонала службы безопасности.

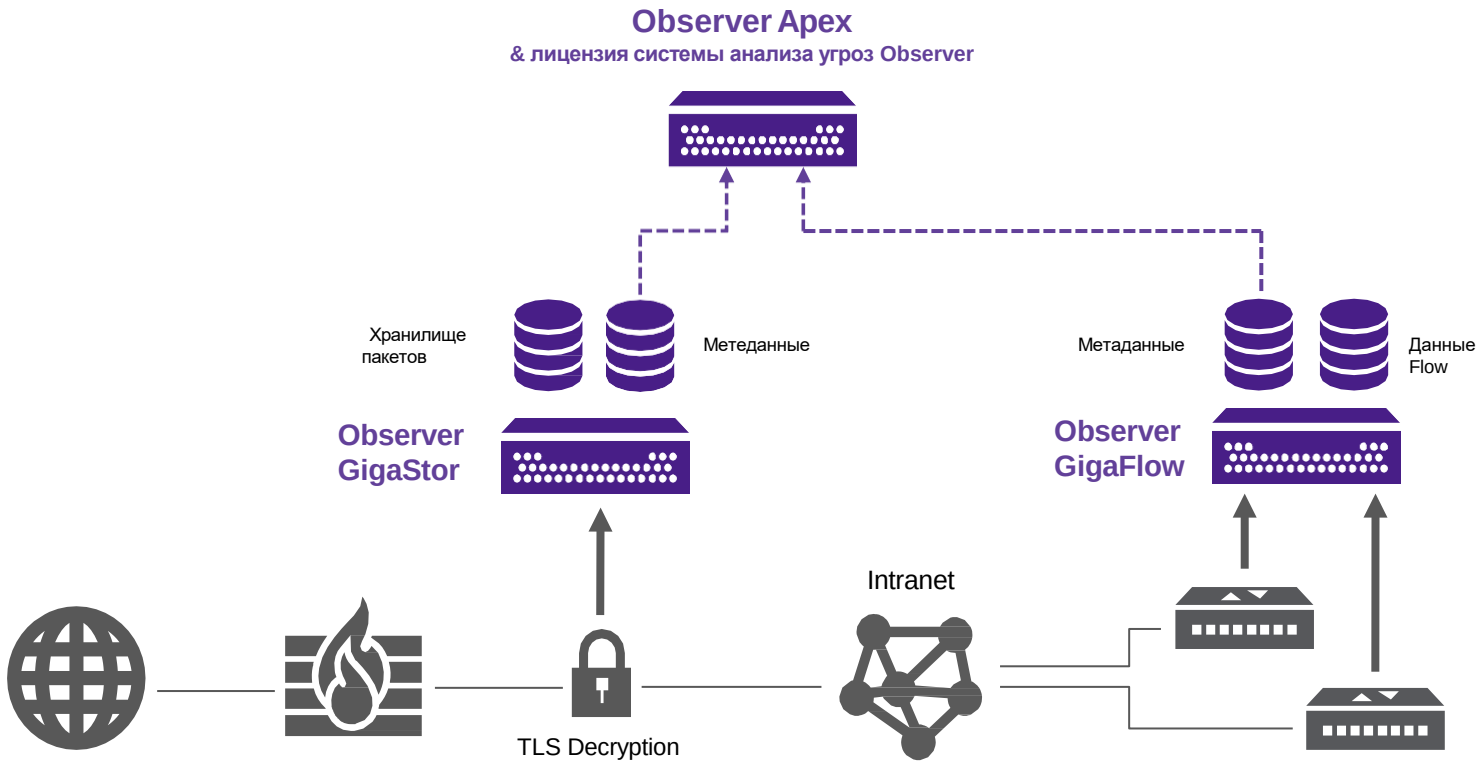
25% Масштабирование операций по обеспечению безопасности для удовлетворения растущих потребностей.

Основные выводы из отчета ESG

- **На 44% быстрее анализ инцидентов:**
  - Организации, обладающие **возможностями захвата пакетов**, анализируют источники и причины инцидентов на **44% быстрее**, чем организации, не обладающие такими возможностями.
- **Междоменный мониторинг:**
  - Решения, предназначенные для устранения различных типов инцидентов (безопасность, сети), сокращают время обучения и улучшают совместную работу.
- **Вызовы**
  - Инструменты мониторинга сети остаются фрагментированными, несмотря на стремление к консолидации.
- **NetSecOps Конвергенция Ожидаемое время прибытия: Сейчас!**
  - В условиях разнообразия и сложности проблем безопасности одним из наиболее эффективных подходов является объединение NetOps и SecOps в NetSecOps. Какова выгода? Явное улучшение общей безопасности.

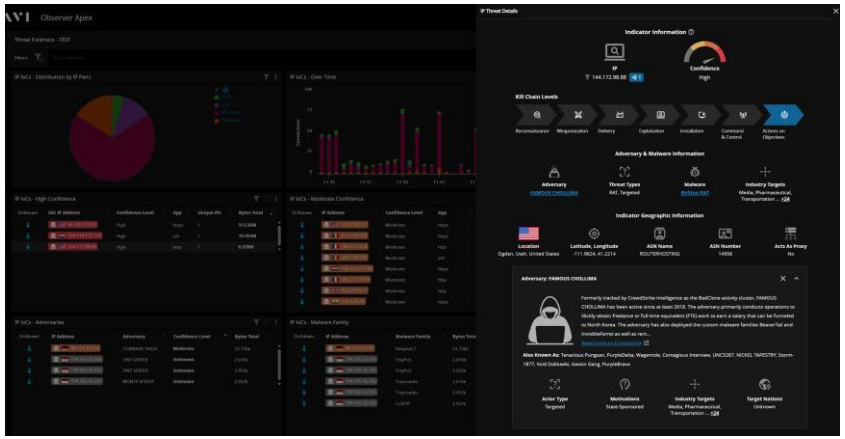


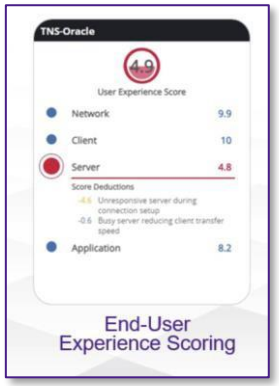
Архитектура системы анализа угроз Observer



Платформа NetSecOps Observer

- VIAVI Observer объединяет сеть и безопасность в одной платформе.
  - Сетевые операции могут рассматривать контекст безопасности как часть оценки проблем производительности.
  - Служба безопасности может видеть влияние событий безопасности на критически важные ресурсы.
- Система анализа угроз Observer интегрирует информацию об угрозах, предоставляя краткие данные об угрозах для NetSecOps.
  - Обширная информация о угрозах
  - Простые в использовании рабочие процессы
  - Гибкие параметры фильтрации
- Показатели производительности с использованием запатентованного машинного обучения
  - Сеть, клиент, сервер или приложение?
  - Доступно для каждого разговора
- Система анализа захваченных пакетов и богатых долгосрочных метаданных

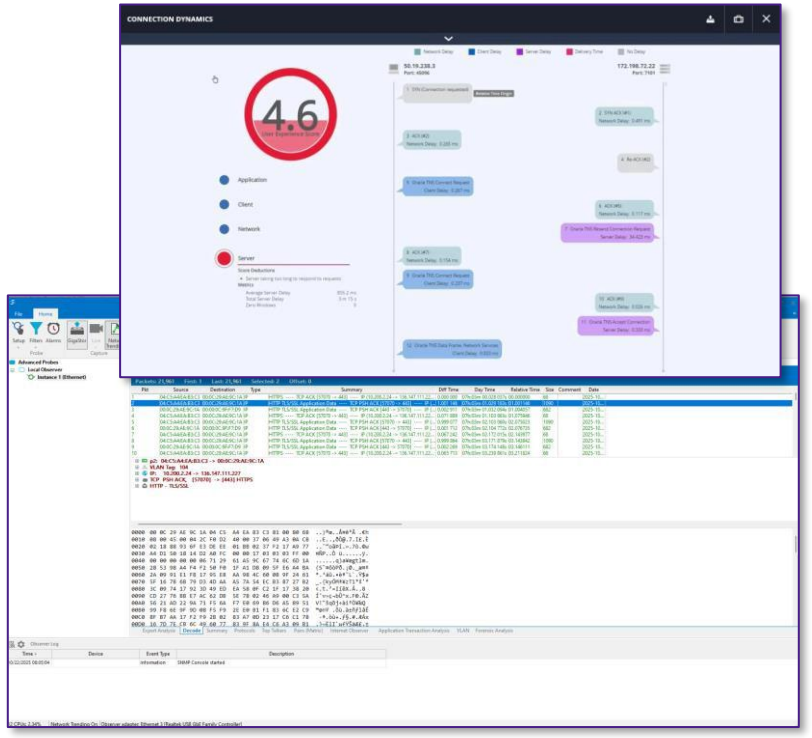




Роль захвата пакетов и интеграции

Критически важно для анализа инцидентов:

- Система анализа захваченных пакетов автоматически создает богатые метаданные, которые используются для мониторинга производительности сети и выявления угроз безопасности.
- Захват пакетов позволяет **тщательно анализировать** источники и происхождение инцидентов.
- Connection Dynamics — это простая кнопка для анализа пакетов.
- Благодаря удобному интерфейсу VIAVI Observer упрощает доступ к пакетам (при необходимости).



Показатель ESG:

Организации с надежными возможностями захвата пакетов достигают **44% более быстрого решения инцидентов**.

Директивы ЕС по кибербезопасности NIS2 и DORA

Директива NIS2 — это регламент Европейского союза в области кибербезопасности, который ужесточает требования к безопасности, расширяет сферу применения в отношении критически важных секторов и вводит более строгие требования к уведомлению об инцидентах с целью повышения устойчивости важнейших служб и цифровой инфраструктуры.

Закон о цифровой операционной устойчивости (DORA) ориентирован конкретно на *финансовые организации* и направлен на повышение их устойчивости к сбоям, связанным с ИКТ. Директива определяет требования к широкому кругу финансовых организаций по созданию комплексных систем обеспечения цифровой операционной устойчивости.

Несколько систем безопасности могут помочь в определении и установке технических областей.

Концепция кибербезопасности NIST

- Национальный институт стандартов и технологий (NIST) разработал рамочную концепцию кибербезопасности (NIST CSF), которая представляет собой добровольный, признанный в отрасли набор руководящих принципов и передовых методов, призванных помочь организациям эффективно управлять рисками кибербезопасности.

- CSF разделен на шесть (6) функций
  - Управление, Идентификация, Защита, Обнаружение, Реагирование, Восстановление
  - Каждая из функций имеет категории и подкатегории для управления рисками.
  - CSF охватывает примерно 150 подкатегорий..

- Системы анализа угроз Observer поможет компаниям решить **более 73%** технических задач в области CSF.

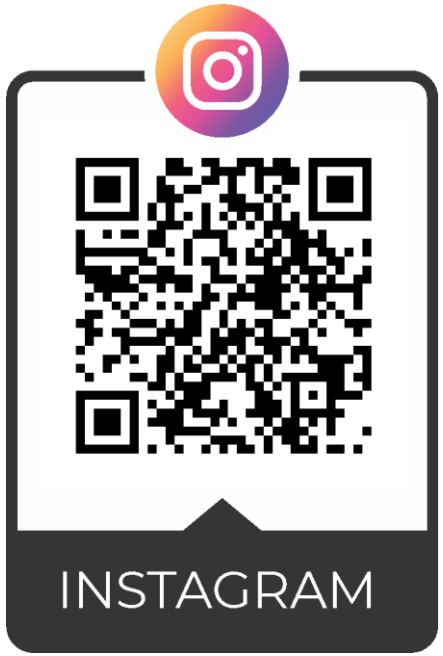
- Основная функциональность системы анализа угроз предназначена для решения критически важных задач по обнаружению и реагированию, определенных в рамках концепции кибербезопасности Национального института стандартов и технологий (NIST).

LinkMaster KAZAKHSTAN

Категории структуры кибербезопасности NIST

Функция	Категория	VIAVI системы анализа угроз
Управление **(GV)**	Сосредоточенность на обеспечении организационной структуры	Нет
Идентификация **(ID)**	Управление активами(7 подкатегорий)	5 из 7 (71%)
	Оценка рисков(10 подкатегорий)	7 из 10 (70%)
	Улучшение (4 подкатегории)	4 из 4 (100%)
Защита **(PR)**	Управление идентификацией, аутентификацией и контролем доступа (6 подкатегорий)	1 из 6 (17%)
	Осведомленность и обучение (2 подкатегории)	Нет
	Безопасность данных(4 подкатегории)	1 из 4 (25%)
	Безопасность платформы (6 подкатегорий)	4 из 6 (67%)
	Устойчивость технологической инфраструктуры (4 подкатегории)	2 из 4 (50%)
Обнаружение **(DE)**	Непрерывный мониторинг(5 подкатегорий)	4 из 5 (80%)
	Анализ нежелательных явлений (6 подкатегорий)	6 из 6 (100%)
Реагирование **(RS)**	Управление инцидентами(5 подкатегорий)	5 из 5 (100%)
	Анализ инцидентов(4 Subcategories)	4 из 4 (100%)
	Отчетность и коммуникация по реагированию на инциденты(2 подкатегории)	2 из 2 (100%)
	Смягчение последствий инцидентов (2 подкатегории)	2 из 2 (100%)
Восстановление **(RC)**	Выполнение плана восстановления после инцидента (6 подкатегорий)	5 из 6 (83%)
	Связь при восстановлении после инцидента (2 подкатегории)	Нет

LinkMaster KAZAKHSTAN



ПОДПИСЫВАЙТЕСЬ НА НАС

LinkMaster
KAZAKHSTAN

ТОО «ЛинкМастер Казахстан»

Республика Казахстан, 050036, г. Алматы, мкр. Мамыр-4, дом 117/6

+7 (727) 390-18-70 +7 707 998 4944 info@linkmaster.kz www.linkmaster.kz