Solar LightHouse

Платформа управления
безопасностью инфраструктуры



Проблематика/ зачем это всё

Безопасность инфраструктуры – фундамент защищённости организации

01

Знание инфраструктуры

Компании не знают свою инфраструктуру, в каком она состоянии и кто за что отвечает, серые зоны, теневое ИТ

02

ИТ гигиена

Без ИТ гигиены растер общая уязвимость инфраструктуры. Защита становится дорогой и неэффективной – все уходит на латание дыр

03

Процессный подход

Без процессного подхода защита разовая и нестабильная. Чтобы она работала, нужны повторяемые действия, контроль и метрики

SOLAR



ЛОГИЧЕСКИЙ РАДАР

SOLAR

Защита данных
- DLP
- Database Activity Monitor and Database Firewall
- Data Access Governance
- Secure Collaboration
- Information Leaks Detection
- Data encryption
- Data Discovery and Classification

Защита приложений
Защита веб-приложений
- WAF
- DDoS Protection L7
- AntiBot
- CDN

Безопасная разработка
- AST
- Runtime Application Self-Protection (RASP)
- Software Composition Analysis (SCA)
- Application Security Education and Awareness
- Mobile application security
- IAST (interactive application security testing)
- API Security

Управление доступом
- SSO
- MFA
- Identity Management
- Access Governance
- Identity and Access monitoring & analytics
- PAM
- PKI
- ITDR

Security Operations
- SIEM
- UEBA
- EDR
- NTA/NDR
- XDR
- Application\Network performance monitoring
- Fraud prevention
- Deception
- Digital Risk Protection
- Advanced malware detection
- IRP
- Orchestration and Automation (SOAR, RPA, DevOps Automation)
- Cyber range
- Digital Forensics an Incident Response
- Threat Intelligence Platform

Security Management
- Security Asset Management & Configuration Management Database (CMDB)
- Network Configuration Control
- Patch Management
- Configuration Management
- Change Management
- Security Governance, Risk, Compliance (SGRC)
- Security Awareness Platform
- Vulnerability Management
- Breach and Attack Simulation
- Vulnerability Prioritization Technology
- External Attack Surface Management
- CPT

Cloud Security
- Cloud Access Security Broker
- Cloud Security Posture Management
- Secure Access Service Edge

Безопасность ИТ инфраструктуры
Endpoint & Storage Security
- Endpoint Protection Platforms
- Remote Browser Isolation
- Модуль доверенной загрузки
- Unified Endpoint Management (UEM)

Безопасность виртуализации
- Container security
- Virtualization security

Сетевая безопасность
- Network Firewall + IDS/IPS
- Data Diode
- VPN
- DDoS Protection L3/4
- Wireless Security
- SEG
- SWG
- Network AV
- SandBox
- NAC
- SD-WAN
- Industrial Network Security
- Firewall management



SOLAR

Контрольные вопросы

Инфраструктура

- Вы знаете состав своей инфраструктуры? Есть серые зоны?
- Назовёте время, необходимое для обнаружения нового хоста в сети?
- Знаете сколько интерфейсов надо посмотреть, чтобы понять что за хост?
- Всегда известно к чему относится сервер, виртуальная машина, учётка?
- Знаете процент инфраструктуры, где определены ответственные за ассет?

Управление процессами ИБ

- Известно количество процессов поддержки ИБ инфраструктуры?
- Процессы как-либо документированы? Соответствуют документации?
- Процессы вообще функционируют? Знаете как проверить?
- Проводится проверка исполнения задач? Много сил отнимает?

Политики безопасности

- А какой процент инфраструктуры покрыт политиками безопасности?
- Как составляете политики безопасности? Много источников экспертизы?
- Везде ли работают СЗИ?

Приоритизация и критичность

- Определена критичность ассетов? Понятно какие ассеты в приоритете?

Контроль, обзор и зрелость

- Есть helicopter view? Связан ли он с реальным состоянием инфраструктуры?

80%

рынка **не ответит утвердительно** даже на половину вопросов

SOLAR

Solar LightHouse наведёт порядок в инфраструктуре и выстроит устойчивую систему ИБ

Порядок в инфраструктуре – это меньше инцидентов, проще защита и меньше затрат

Безопасность начинается с прозрачности и контроля

Что получает клиент

Единую архитектуру безопасности: единые политики и контроль их исполнения

Централизованную и масштабируемую ИБ-архитектуру

Инфраструктуру, готовую к росту и требованиям регуляторов

Solar LightHouse – это **on-premise продукт с уникальным целеполаганием**, сочетает в себе функции сразу нескольких классов решений

Как было раньше



Как это будет



Ключевая польза	Методы реализации	Традиционные классы продуктов
Полная картина инфраструктуры	Активное сканирование, аудит, интеграционное получение информации, сбор событий	• Asset Management/CMDB/ITAM • Vulnerability Management
Снижение уязвимостей	Patch-менеджмент, безопасные конфигурации	• Vulnerability Management • Compliance Management
Снижение рисков атак	Hardening, best practice, безопасные конфигурации	Compliance Management
Безопасность сетевой инфраструктуры	Управление доступом, сегментация, контроль конфигураций	• Firewall Management • Compliance Management
Устойчивость ИБ-процессов	Автоматизация, централизация процессов, контроль задач и рекомендации по решению проблем	• (Business) Process Management • sGRC
Оценка зрелости и план развития	Анализ и описание мер защиты по требованиям и по регуляторным и best practice документам	sGRC

* Exposure Assessment Platform

Примеры решаемых задач с LightHouse

Знания об инфраструктуре

- Сбор перечня ассетов со всех возможных систем
- Выявление новых ассетов в инфраструктуре
- Определение владельцев для всех ассетов в инфраструктуре
- Определение критичности ассетов
- Определение вхождения ассета в ИТ системы

Практики безопасности

- Контроль установленного ПО согласно белому/черному списку
- Запуск и контроль корректности работы патч-менеджмента
- Контроль параметров и версий СЗИ
- Проверка корректности сетевой сегментации
- Обеспечение «чистого» периметра

Смежные задачи

- Контроль сроков действий лицензий
- Менеджер задач для упрощения взаимодействия
- Оценка соответствия по реальному состоянии инфраструктуры и процессов
- Переводчик с ИБшного
- Учёт и экономия используемых ИТ ресурсов

SOLAR

Решаемые бизнес задачи

Рациональное использование наложенных средств ИБ за счёт реализации базовых мер

Систематизация деятельности по безопасному управлению инфраструктурой

Снижение требований к количеству и компетенциям экспертных кадров

Возможность «измерения» состояния инфраструктуры для обоснования бюджетов или защиты результатов труда

Контроль процессов (всё ли работает, есть ли отклонения или проблемы с функционированием процессов)

Создание прозрачности и понятности ИБ для ИТ и бизнеса

SecFlow

Security Flow

Это методология по внедрению мер, процессов и контролей для безопасности инфраструктуры

Включает следующие компоненты:

- Описание (что, зачем, какой результат)
- Пошаговая инструкция (от документации до контролей)
- Шаблоны документов/регламентов
- Интеграционные модули
- Скрипты, инструкции по настройке
- Шаблоны автоправил для запуска процессов

SecFlow

как это выглядит



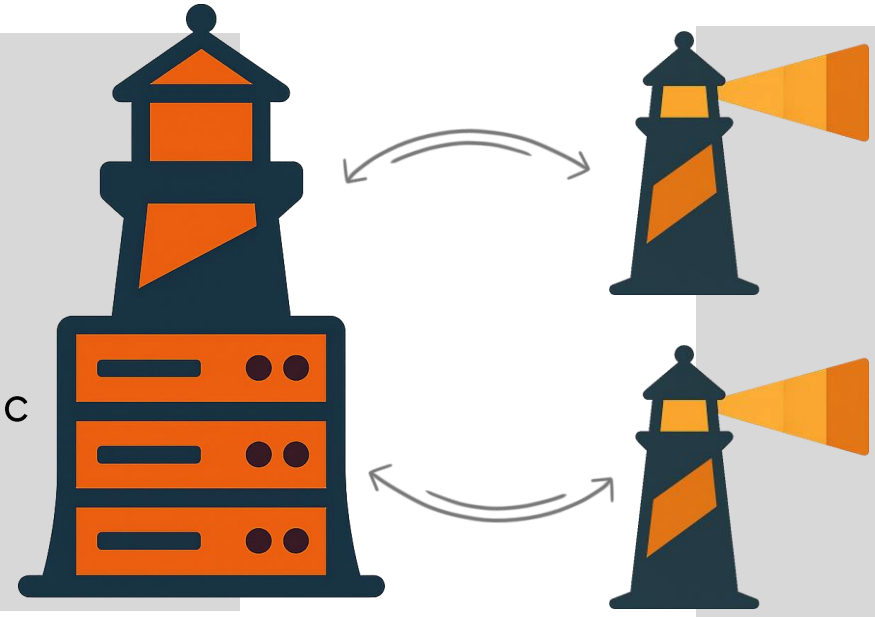
SOLAR

Главное о продукте Solar LightHouse

Архитектура продукта

LightHouse сервер

- База ассетов
- Управление задачами
- Пользовательский интерфейс
- Бизнес логика

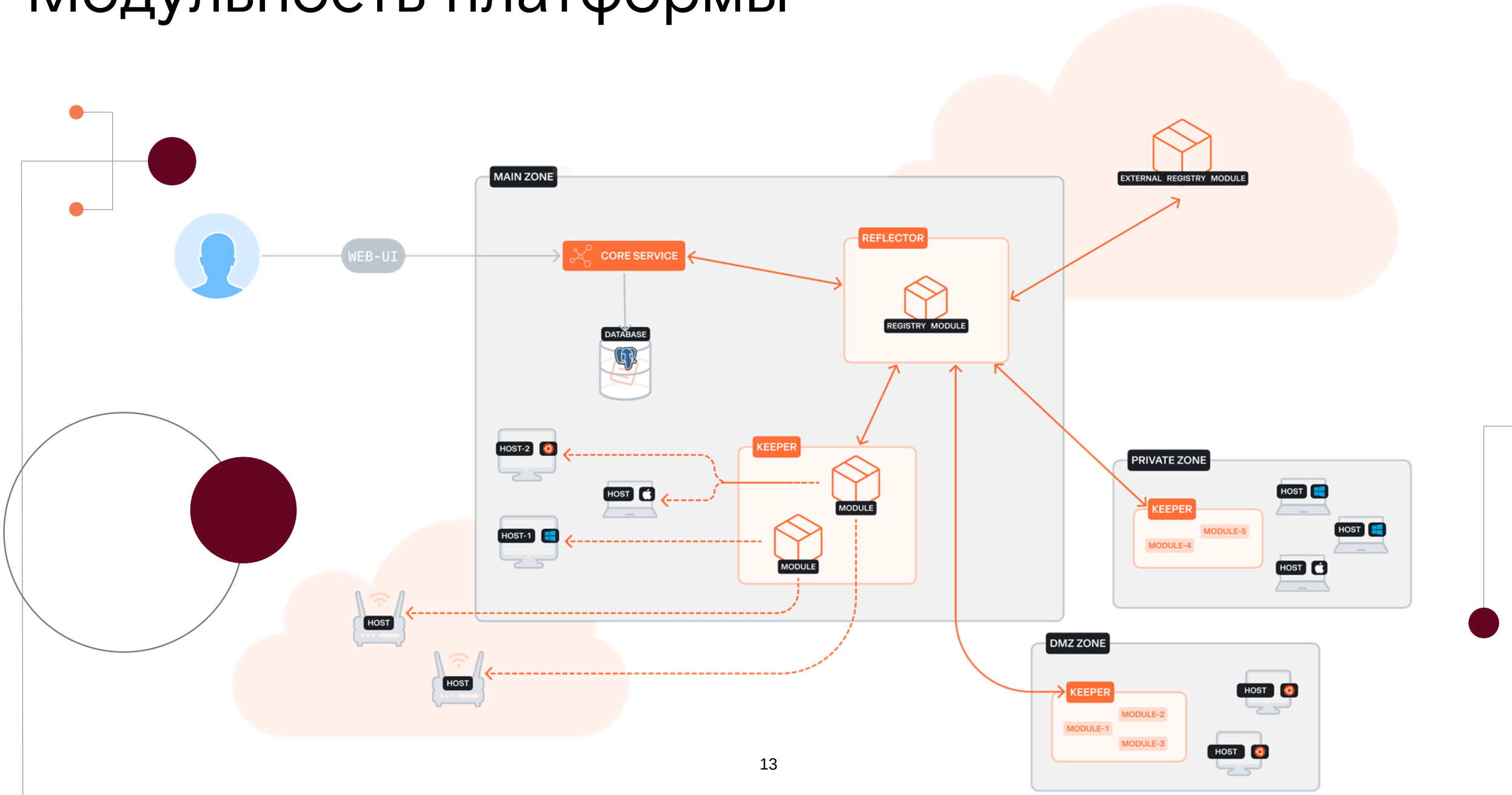


LightHouse Keeper (коллекторы)

- Запуск модулей
- Взаимодействие с хостами
- Реализация интеграций
- Локальная работа с данными

Модульность платформы

SOLAR



Тенантная* структура

Тенанты могут быть реализованы как в рамках одной инсталляции, так и в схеме с несколькими инсталляциями

Типовое применение:

Холдинговая структура

Использование «мастер» тената для агрегации информации по холдингу и задания централизованных политик. Подчиненные тенаты имеют видимость только своей части инфраструктуры и возможность настройки политик, не противоречащих централизованным.

Логическое разделение

Можно использовать если в рамках общей инфраструктуры требуется сузить видимость для разных функций, например для разных блоков ИТ (сеть, БД, Windows, Linux).

*логическая единица, используемая для разделения информации об инфраструктуре

Технологии и окружение

Технологический стек

- Собственная разработка с нуля
- Ядро системы написано на Go
- Микросервисная архитектура
- Модульный подход к функционалу
- Живём практиками AppSec/ DevSecOps

Функции безопасности

- Vault для хранения секретов
- RBAC для пользователей
- ACL для объектов платформы
- Журналирование действий пользователей
- Хранение истории состояний объектов

Для установки продукта поддерживаются:

Отечественные ОС:
- Astra
- RedOS

Linux с Docker, например:
- Ubuntu
- Debian
- CentOS

SOLAR

Интеграции и окружение

В ИТ ландшафте работаем с:

Операционные системы
(Windows, Linux, иные с CLI)

Среды виртуализации

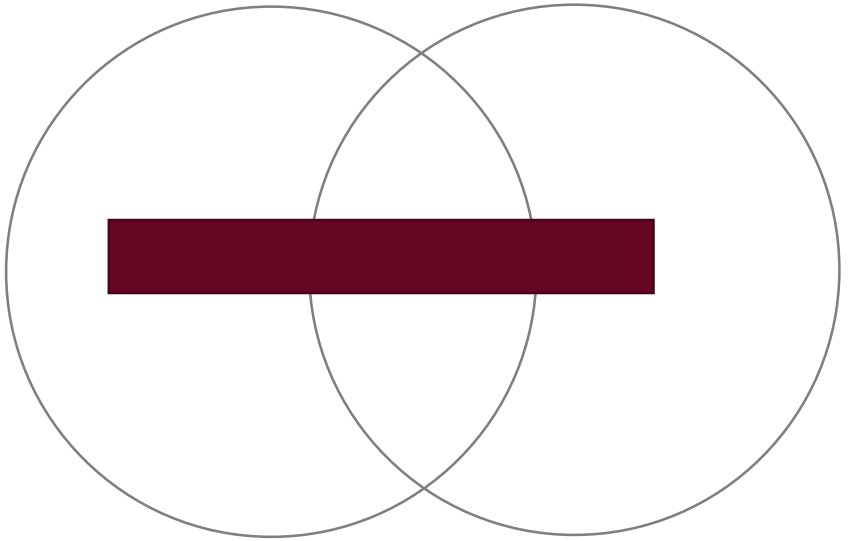
Базы данных

Средства защиты информации

Интерфейсы управления
(iLo, iDRAC, IPMI, ...)

Сетевое оборудование
(роутеры, межсетевые экраны, коммутаторы, ...)

Инфраструктурные системы
(каталоги пользователей, DNS, DHCP, почтовые сервисы, ...)



Ключевые особенности продукта

01	*Data Driven*	ИБ строится на фактах: отталкиваемся от реальной инфраструктуры, а не гипотез. Видим, что есть, и уже от этого выстраиваем защиту
02	*Shift Left всей безопасности*	Продукт даёт общий язык, помогает синхронизировать задачи (ИБ и ИТ) и сфокусироваться на том, что важно для бизнеса
03	*Проводник, помощник*	Слишком много СЗИ, стандартов, требований. Продукт помогает выбрать нужное — по приоритету, по риску, по готовности
04	*Автоматизация рутины*	Платформа берёт на себя контроль за выполнением мер и политик. Уходит ручная работа, остаётся осмысленный ИБ-менеджмент
05	*Комьюнити и контент из коробки*	Поделись своей практикой, возьми чужую. Встроенная экспертиза, шаблоны, процессы — всё доступно и запускается в 2 клика

SOLAR

Давайте начнём путешествие к защищенной инфраструктуре

SOLAR

Product Owner – Бачевский Артем a.bachevskii@rt-solar.ru

BDM – Болтунов Кирилл k.boltunov@rt-solar.ru

PM – Захарченко Иван i.zakharchenko@rt-solar.ru