



THREAT INTELLIGENCE

От реакция към предвидимост

Вижте сигналите за киберзаплахи по-рано.
Разберете риска. Действайте навреме.

КАКВО ПРЕДЛАГАМЕ

Вижте заплахата, преди да се превърне в инцидент

Threat Intelligence събира, анализира и интерпретира информация за киберзаплахи, за да покаже кои рискове могат реално да засегнат организацията и как да се действа навреме.

За разлика от решенията, фокусирани върху вътрешната инфраструктура, Threat Intelligence наблюдава външната среда – там, където се появяват ранните сигнали за бъдещи атаки.



ДВА НАЧИНА НА ИЗПОЛЗВАНЕ



САМОСТОЯТЕЛНА THREAT INTELLIGENCE УСЛУГА

ВЪНШНА ВИДИМОСТ И РАННО ПРЕДУПРЕЖДЕНИЕ

За организации без собствен SOC или за компании, които искат да разширят видимостта си извън вътрешната инфраструктура.

- ✓ Ранно предупреждение за потенциални заплахи
- ✓ Видимост върху външни дигитални рискове
- ✓ Мониторинг на изтекли данни и кредитеншали
- ✓ Контекст и препоръки за действие



THREAT INTELLIGENCE + SOC

КОНТЕКСТ, ПРИОРИТИЗАЦИЯ И ПО-БЪРЗА РЕАКЦИЯ

За организации, които искат да обогатят съществуващото наблюдение и да ускорят реакцията при заплахи.

- ✓ Повече контекст към SOC алармите
- ✓ По-точна приоритизация на рисковете
- ✓ По-бързо разследване на инциденти
- ✓ По-ефективна реакция и ограничаване на заплахите



Двата подхода се допълват: външната видимост показва риска по-рано, а интеграцията със SOC превръща тази информация в по-бърза и по-ефективна реакция.

КАК LIREX ПРЕДОСТАВЯ THREAT INTELLIGENCE

От информация към действие.

LIREX комбинира платформата Cyberint с експертен анализ, който добавя контекст, оценка на риска, приоритизация и конкретни препоръки за действие.



01 СЪБИРАНЕ

Публични източници, специализирани бази данни, threat канали и Deep/Dark Web.



02 АНАЛИЗ

Модели, тенденции и поведение на атакуващите.



03 КОНТЕКСТ

Сигналите се свързват с активите, служителите, сектора и бизнес критичността.



04 ПРИОРИТИЗАЦИЯ

Вероятност, потенциално въздействие и бизнес значение.



05 ДЕЙСТВИЕ

Конкретни препоръки за предотвратяване, ограничаване на риска и реакция.

ОСНОВНИ НАПРАВЛЕНИЯ



DIGITAL RISK PROTECTION

Видимост върху външни дигитални рискове, изтичане на данни и phishing кампании.



PERSONAL PROTECTION

Защита на ключови служители и ръководители от целенасочени дигитални заплахи.



BRAND PROTECTION

Откриване на фалшиви домейни, злоупотреба с име, лого и идентичност.



ATTACK SURFACE MANAGEMENT

Пълна видимост върху публичните дигитални активи и тяхната експозиция.



THREAT EXPOSURE ANALYSIS

Оценка кои експонирани активи представляват реален риск спрямо актуалните заплахи.



Комбиниране технологии и експертиза, за да ви дадем цялостна видимост върху външните рискове и да ви помогнем да действате навреме и с увереност.

БИЗНЕС ПОЛЗИ

По-ранен сигнал. По-ясен риск. По-уверено действие.



Threat Intelligence от LIREX превръща
външните сигнали за риск в ясни приоритети
и конкретни действия за бизнеса.



ПРОАКТИВНО ОТКРИВАНЕ

Откривайте заплахи и
уязвимости, преди да се
превърнат в реални инциденти.



ПРИОРИТИЗАЦИЯ

Фокусирайте се върху
сигналите с реално
въздействие върху бизнеса.



ПЪЛЕН КОНТЕКСТ

Разберете участниците,
техниките и целите зад
атаките.



ПО-НИСКИ MTTD / MTTR

Съкращавайте времето за
откриване и реакция (MTTD /
MTTR) чрез Threat Intelligence и
24/7 SOC експертиза.



DARK WEB МОНИТОРИНГ

Следете за изтекли данни,
креденшъли и ранни
индикатори за
компрометиране.



СТРАТЕГИЧЕСКО УПРАВЛЕНИЕ

Управлявайте киберриска с
ясни приоритети и измерими
резултати.

Не чакайте заплахата да се превърне в инцидент.

Вижте сигналите по-рано. Разберете риска. Действайте навреме.

Готови да видите риска по-рано?

office@lirex.com

lirex.com