Kaspersky
Security Day
2021

Что означает быть в курсе современных угроз? Threat Intelligence от лидера рынка

Александр Мазикин,
руководитель группы развития
продаж сервисов

kaspersky

Threat intelligence - это основанные на фактических данных **знания, включая контекст, механизмы, индикаторы,** последствия и действенные рекомендации, о существующей или возникающей угрозе или угрозе активам, которые могут использоваться для **принятия решений** относительно реакции субъекта на эту угрозу или опасность.

Gartner

История рынка

FireEye, a Top Cybersecurity Firm, Says It Was Hacked by a Nation-State

The Silicon Valley company said hackers — almost certainly Russian — made off with tools that could be used to mount new attacks around the world.

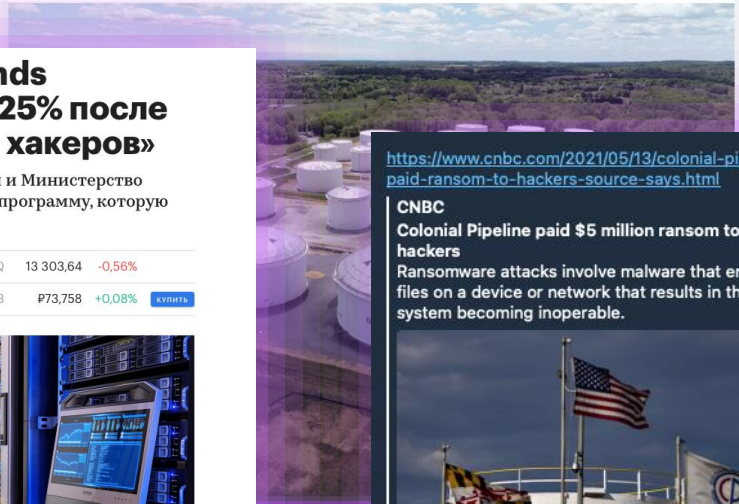
May 19, 2021
1:02 AM MSK

Technology

Ransomware hits near pre-Colonial Pipeline levels, data suggests

3 minute read

Raphael Satter



Акции SolarWinds обвалились на 25% после атаки «русских хакеров»

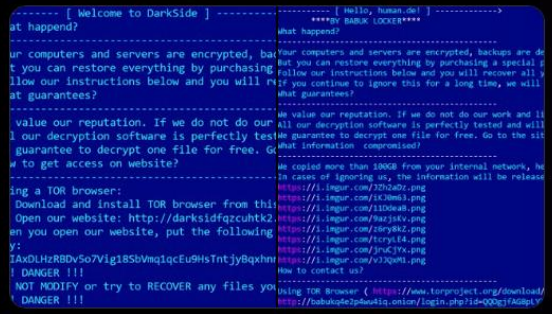
Хакеры, взломавшие Минфин и Министерство торговли США, использовали программу, которую разработала компания

NASDAQ	NASDAQ	13 303,64	-0,56%	
Доллар/Рубль	USD/RUB	₽73,758	+0,08%	купить

Фото: Sashkin / Shutterstock

Costin Raiu @craiu · May 10

Wondering what "happend" here. Did Babuk copy the DarkSide ransom text, or is it an indication of some form of cooperation between them?



8 54 157

https://www.cnbc.com/2021/05/13/colonial-pipeline-paid-ransom-to-hackers-source-says.html

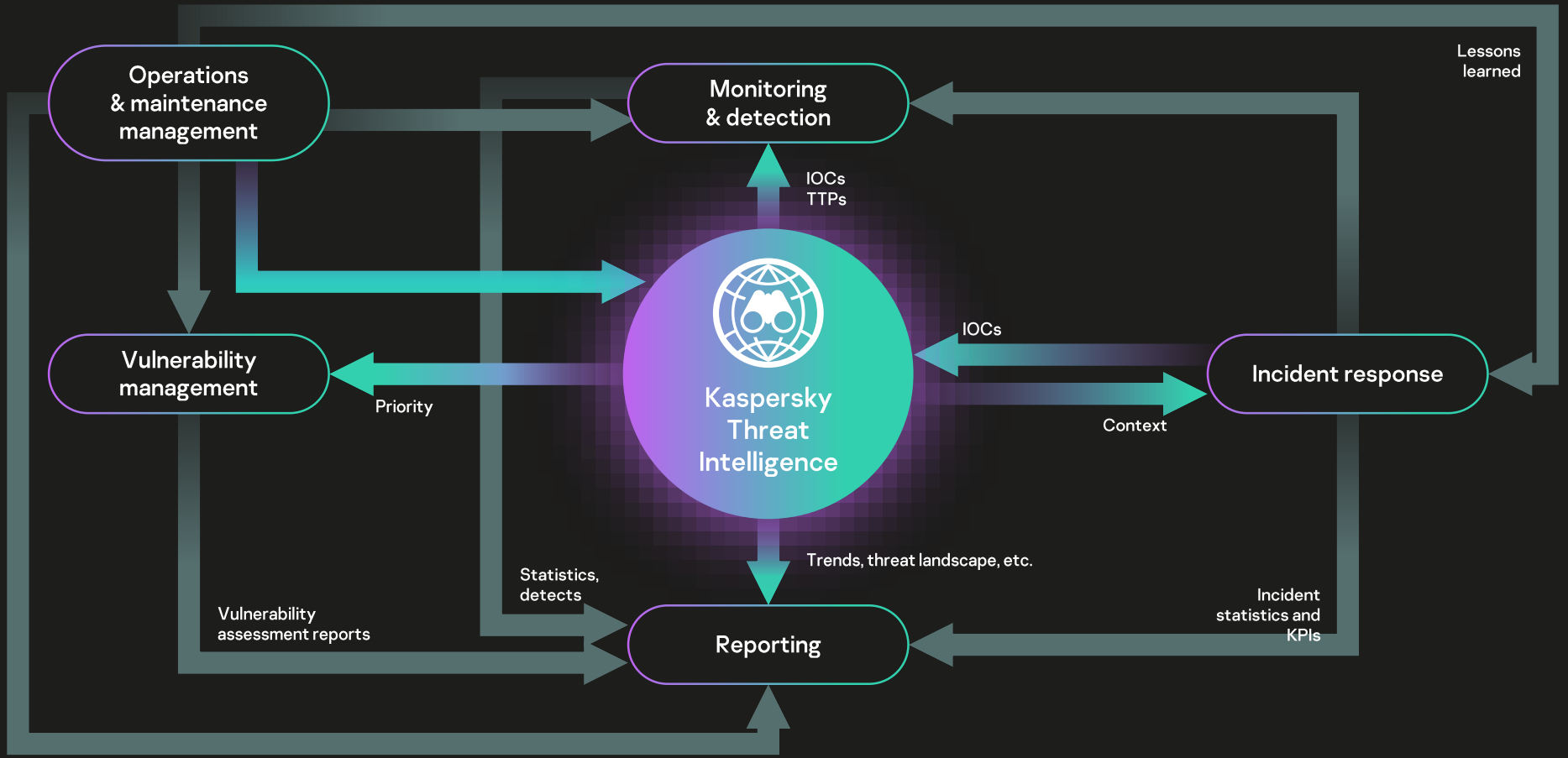
CNBC

Colonial Pipeline paid $5 million ransom to hackers

Ransomware attacks involve malware that encrypts files on a device or network that results in the system becoming inoperable.

INSTANT VIEW

Роль в security operations



Типы данных об угрозах: Threat Intelligence

Технические

#Feeds
#MRTI
#Correlation

Операционные

#Расследования
#Исследования

Тактические

#TTPs
#Actors

Стратегические

#Тренды
#Целевая информация

Почему Threat Intelligence это важно?

Принятие решений за счет понимания действий злоумышленников

Детектирование угроз, выявление техник, тактик и процедур (TTP’s)

Управление рисками

Сценарии использования

Расследование

- Инструменты для ускорения расследований
- Threat Hunting

Реагирование

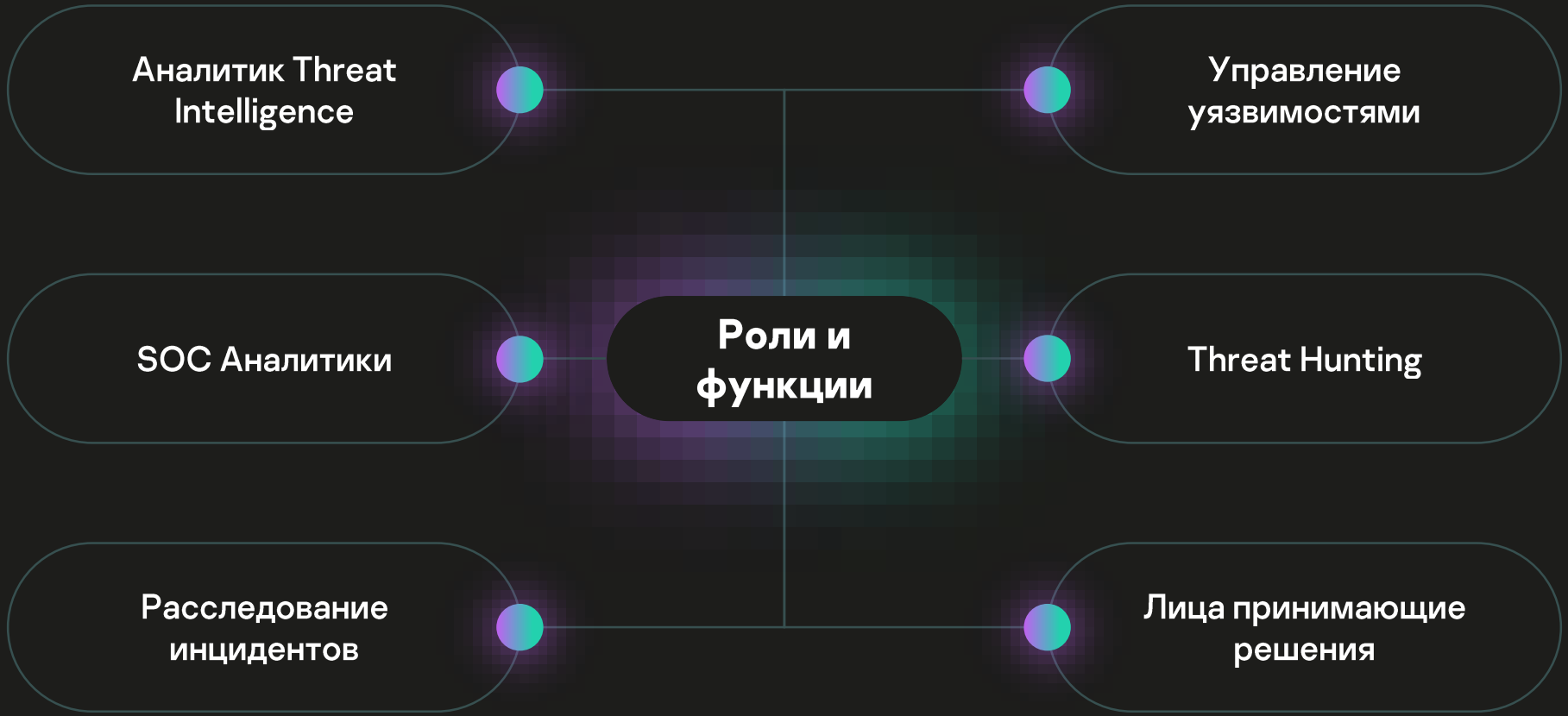
- Валидация событий и обогащение
- Приотиризация уязвимостей

Устранение

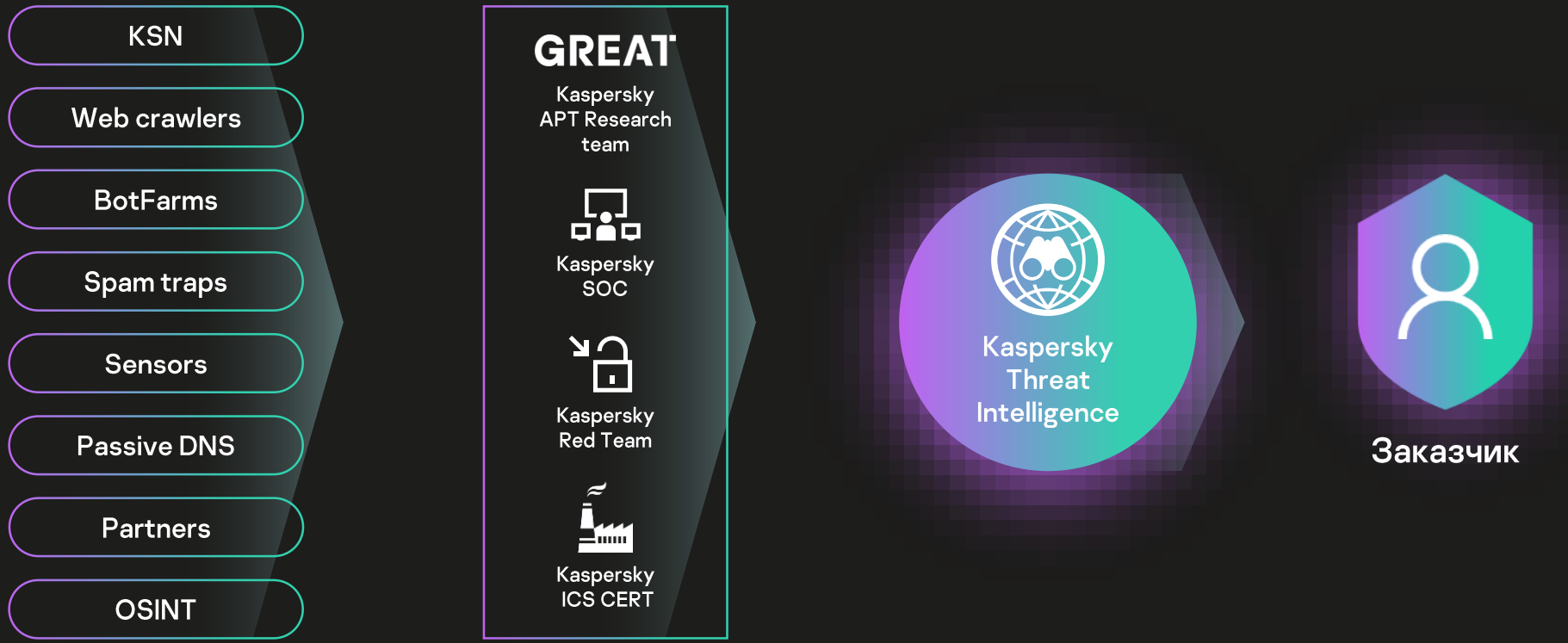
- Мониторинг бренда
- Takedown и блокировка ресурсов

Детектирование

- Обнаружение инцидентов
- Отслеживание источников
- Security Enrichment


Аналитик Threat Intelligence
Управление уязвимостями
SOC Аналитики
Роли и функции
Threat Hunting
Расследование инцидентов
Лица принимающие решения

Threat intelligence - источники



Исследования – публичные анонсы ЛК

2016

- Metel
- Saguaro
- Adwind
- StrongPity
- Lazarus
- Ghoul
- Lurk
- Fruity Armor
- GCMan
- ScarCruft
- Poseidon
- Danti
- Dropping Elephant
- ProjectSauron

2017

- StoneDrill
- WhiteBear
- BlueNoroff
- Silence
- ExPetr/ NotPetya
- ATMitch
- ShadowPad
- BlackOasis
- Shamoon 2.0
- WannaCry
- Moonlight Maze

2018

- Zebrocy
- DarkTequila
- MuddyWater
- Skygofree
- Olympic Destroyer
- ZooPark
- Hades
- Octopus
- AppleJeus

2019

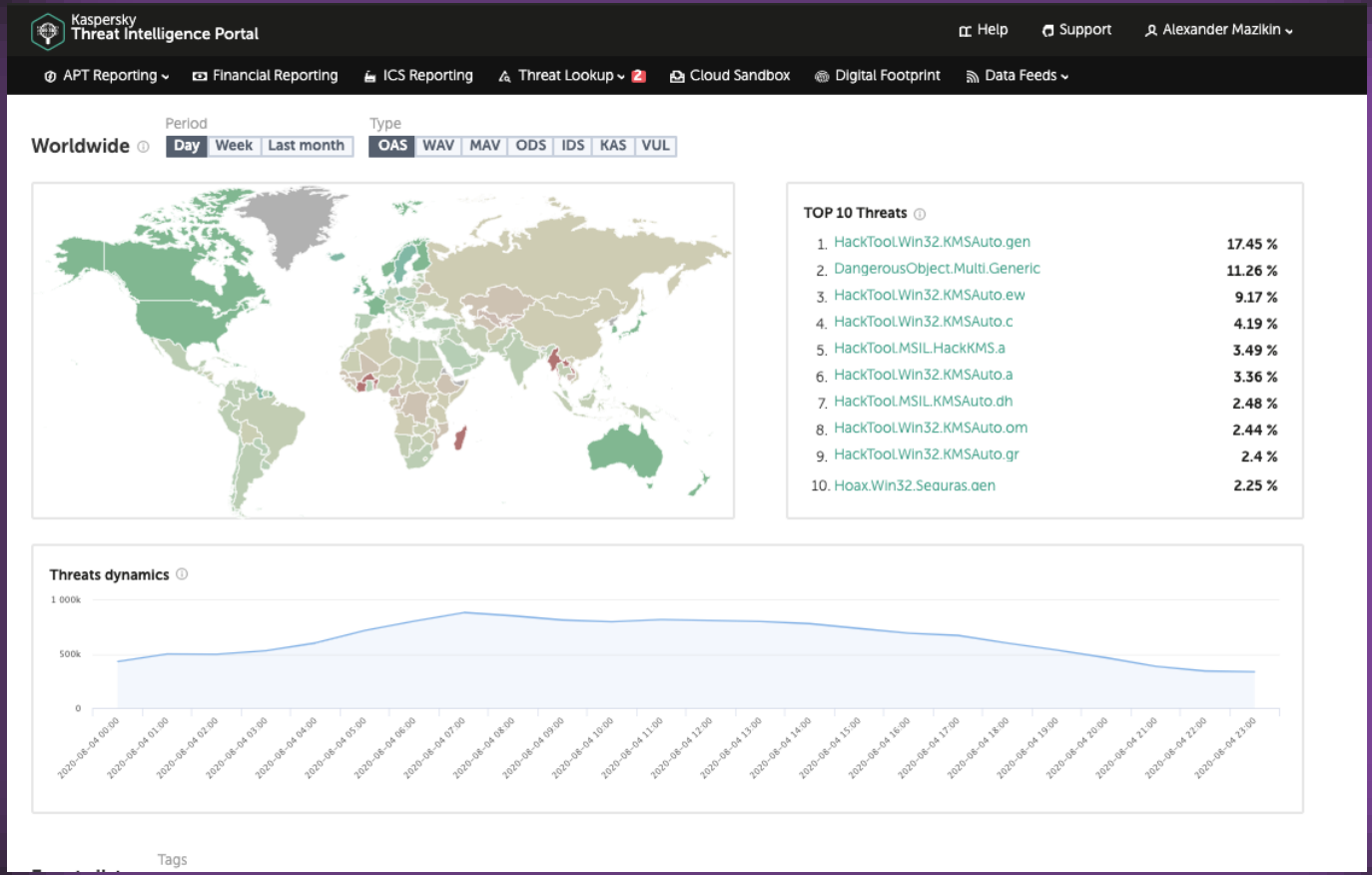
- Topinambour
- ShadowHammer
- SneakyPastes
- FinSpy
- DarkUniverse
- COMpfun
- Titanium

2020

- Cyclodek
- MosaicRegressor
- SixLittle Monkeys (aka Microcin)
- VHD Ransomware
- CactusPete
- WildPressure
- DeathStalker
- PhantomLance
- MATA
- TransparentTribe
- WellMess
- TwoSail Junk
- MontysThree

Портфолио Kaspersky Threat Intelligence

Threat Intelligence Portal



Дорожная карта

Объединение технологий

- Threat Analysis Lab

Унификация

- Эволюция экосистемы, единая строка поиска

Развитие решений

- Новые продукты и развитие текущих

Защита бренда

- Усиление позиций Digital Risk Management

FORRESTER®

The Forrester Wave™: External Threat Intelligence Services Q1, 2021.

«Лаборатория Касперского» признана лидером в области сервисов оперативного информирования о киберугрозах.

> The biggest intelligence bodies in the cyberworld are private entities – FireEye and Kaspersky have more information than any state intelligence body.

Dr. Mohamed al-Kuwaiti, Head of Cyber Security, UAE Government

Спасибо!

kaspersky