Kaspersky Industrial Cybersecurity Conference 2023

SIEM, история и сослагательное наклонение:

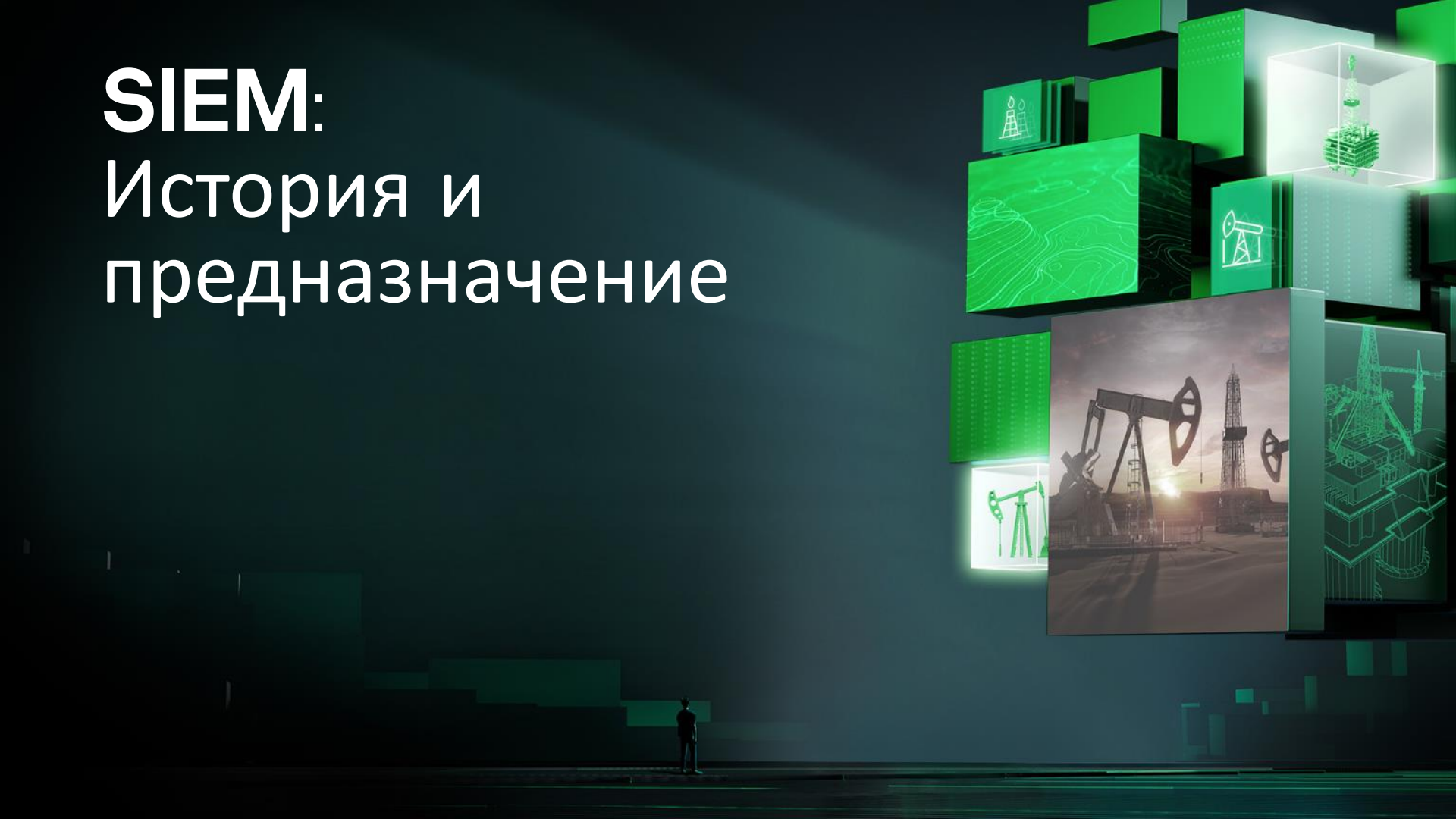
KUMA на стыке OT и IT

Евгения Лагутина

Эксперт по системам
мониторинга ИБ и SOC-сервисам

kaspersky

SIEM: История и предназначение



Функции SIEM-системы в корпоративном сегменте

Хранение

- Соответствие требованиям регуляторов
- Расширение возможностей по ретроспективному анализу

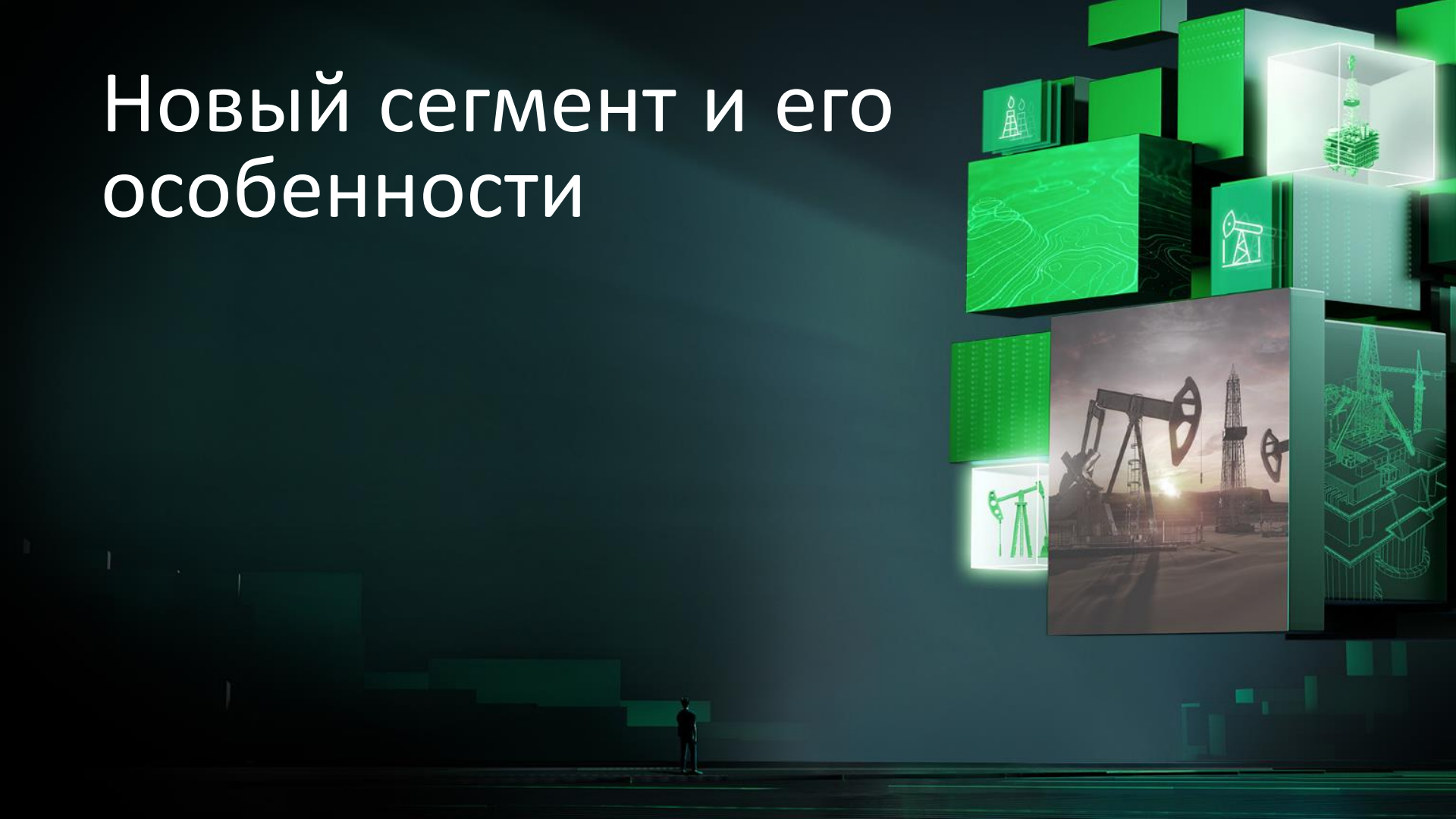
Подготовка

- Нормализация данных, обогащение
- Дополнительный анализ

Сбор

Сбор данных с различных источников

Новый сегмент и его особенности



Критичность вмешательства

Специфичность журналов

Сетевая изоляция

1/3

Уязвимостей, актуальных для технологического сегмента, относятся к системам корпоративного сегмента

Кибербезопасность
на стыке IT / OT-систем

Корпоративная безопасность

Security Information and Event Management

Промышленная безопасность

Пример 1
Black Energy

> BlackEnergy — это троянец для проведения DDoS-атак. В 2007 году создатель объявил о прекращении работы над троянцем и продал исходный код.

В 2014 году внимание привлекла группа хакеров, начавшая использовать
SCADA-модули BlackEnergy и атаковать **промышленные и энергетические секторы** по всему миру.

Securelist by Kaspersky (link)

1

Доставка

Документы Excel и Word с макросами
Team Viewer
Java
…

2

Сбор данных о системе

После запуска BlackEnergy позволяет проверить систему на соответствие необходимому критерию. Это позволяет определить фактическую важность зараженной системы

3

Выполнение требуемого модуля

Удаление файлов
Поиск специальных процессов, специфичных для ISC, завершение их работы и перезапись произвольными данными

Domain	ID	Name
Enterprise	T1548	Abuse Elevation Control Mechanism: Bypass User Account Control
Enterprise	T1071	Application Layer Protocol: Web Protocols
Enterprise	T1547	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
		Boot or Logon Autostart Execution: Shortcut Modification
Enterprise	T1543	Create or Modify System Process: Windows Service
Enterprise	T1555	Credentials from Password Stores: Credentials from Web Browsers
Enterprise	T1485	Data Destruction
Enterprise	T1008	Fallback Channels
Enterprise	T1083	File and Directory Discovery
Enterprise	T1574	Hijack Execution Flow: Services File Permissions Weakness
Enterprise	T1070	Indicator Removal
		Clear Windows Event Logs
Enterprise	T1056	Input Capture: Keylogging
Enterprise	T1046	Network Service Discovery
Enterprise	T1120	Peripheral Device Discovery

23

Enterprise Techniques

3

ISC Techniques

В классификации MITRE

Пример 2
Industroyer

Backdoor

CnC

Выполнение полезной нагрузки

Модуль 101

Модуль 61850

Модуль 104

Модуль OPC DA

Сетевой сканер

Модуль DoS

Стирание данных

Изменение файлов реестра

22

Enterprise Techniques

24

ISC Techniques

В классификации MITRE

Кибербезопасность
на стыке IT / OT-систем

Корпоративная безопасность

Security Information and Event Management

Промышленная безопасность

Kaspersky Unified Monitoring and Analysis Platform + KICS

Кибербезопасность
на стыке IT / OT-систем

Корпоративная безопасность

XDR

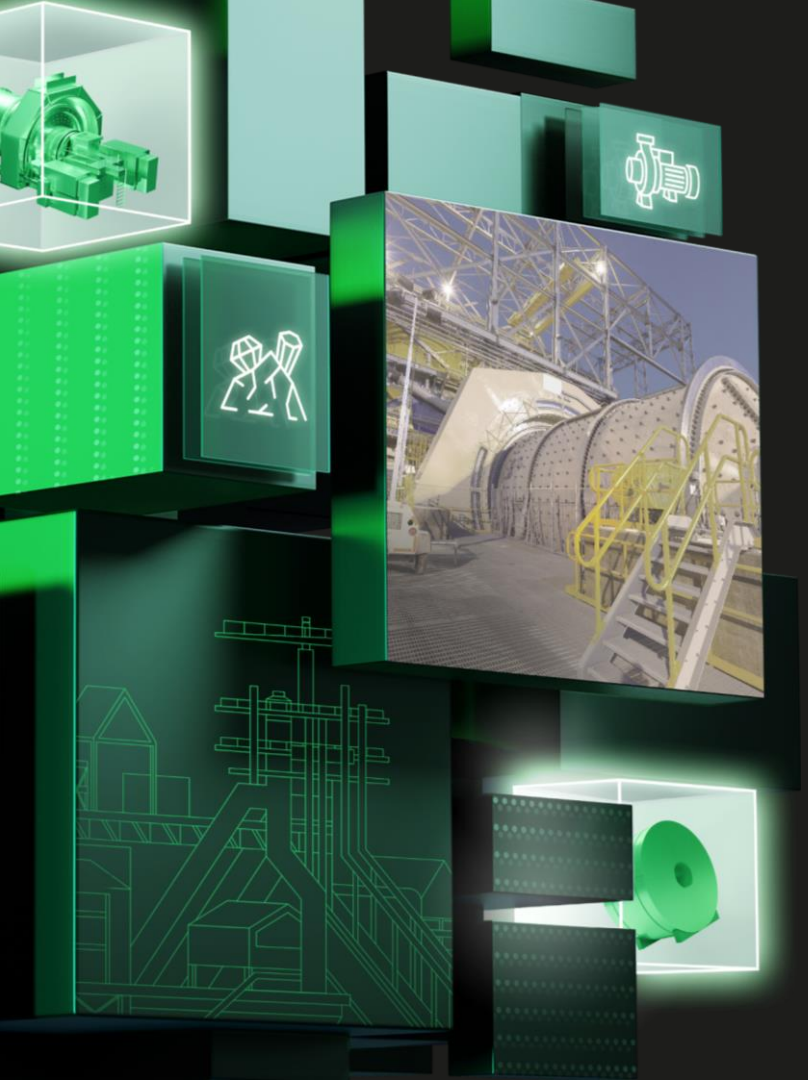
Kaspersky Symphony

Kaspersky Unified Monitoring and Analysis

Промышленная безопасность

XDR

Kaspersky Industrial CyberSecurity



Спасибо!

evgeniia.lagutina@kaspersky.com