CYBERBIT
PROTECTING A NEW DIMENSION

# Cyberbit SOC 3D

Автоматизированная консолидация всех данных управления процессом реагирования на киберинциденты на единую панель управления и повышение эффективности SOC в целом.

## Проблема

Согласно данным Ponemon Institute ("Исследование стоимости взломов данных за 2016 г."), среднее время устранения взлома составляет 70 дней. Более того, когда устранение занимает более 30 дней, суммарная стоимость ущерба от взлома возрастает с $3.18M до $4.35M. Чем дольше длится кибератака, тем выше риск и ущерб. Поэтому является критически важным улучшать успешность и эффективность Центров управления информационной безопасностью (SOC) и минимизировать время реакции и восстановления.


Исследование стоимости ущерба от взломов данных за 2016 г., Ponemon Institute

## Борьба SOC за эффективность в условиях роста источников оповещений

По мере того, как кибератаки становятся все более частыми и изощренными, персонал SOC стремится успевать обрабатывать оповещения от многочисленных инструментов по информационной безопасности и выполнять процессы ручного реагирования на инциденты. Эта проблема еще более усложняется отсутствием средств визуализации и острой нехваткой умелых и хорошо обученных операторов и аналитиков. Менее опытные операторы не в состоянии самостоятельно разрешать тревожные ситуации и оттого переводят слишком много инцидентов на более высокий уровень, создавая тем самым непосильную нагрузку на высококвалифицированных и дефицитных аналитиков кибербезопасности. И, наконец, работа SOC не скоординирована с потребностями бизнеса и ее эффективность страдает от недостаточного объема бизнес-информации для корректной приоритизации своих действий, из-за чего уменьшается ценность SOC для владеющих ими организаций.

## SOC 3D – эффективная кибербезопасность в интересах бизнеса

SOC 3D представляет собой систему с единой панелью управления для автоматизации и координации работы SOC, сочетающуюся с передовыми средствами анализа BigData, в результате чего улучшаются эффективность и надежность SOC, возрастает эффективность персонала SOC и снижаются требования к уровню их квалификации. Система SOC 3D обеспечивает ориентацию SOC на бизнес, координацию вопросов кибербезопасности с целями бизнеса и сосредоточение деятельности SOC на наиболее важных аспектах, с точки зрения рисков для бизнеса. Разумная автоматизация ускоряет работу аналитиков по всему циклу реагирования на инциденты путем автоматизированного принятия решений, автоматизации обогащения данных и процессов реагирования, экономя в среднем по 12 минут на каждый инцидент. Анализ BigData придает тревожным оповещениям беспрецедентную видимость и контекст, обеспечивая работу SOC в упреждающем режиме.

## Преимущества SOC 3D

- **Создание эффективного SOC,** который быстрее реагирует на угрозы, снижает нагрузку на персонал центра за счет разумной автоматизации и подвергается постоянной оценке посредством четких параметров и ключевых показателей эффективности с целью ее повышения.
- **Получение SOC, оринтированного на бизнес,** который концентрирует усилия персонала кибербезопасности на критически важных для бизнеса угрозах, постоянно информирует руководство организации и вовлекает всю организацию в свою деятельность.
- **Расширение возможностей персонала SOC** и усиление влияние аналитиков благодаря упрощению сложных расследований и привлечению персонала с помощью оринтированного на пользователя интерфейса, который понижает квалификационный барьер и повышает степень удовлетворения пользователей.
- **Достижение ситуационной осведомленности обо всем киберпространстве организации** благодаря специализированным панелям и отчетам, предоставляющим критически важную для безопасности бизнеса информацию всем заинтересованным лицам.
- **Работа с упреждением** и легкость выполнения расследований с быстрым доступом к необработанным данным и историческим данным, поиском по образцу Google и визуализацией в реальном времени, что позволяет персоналу придавать тревожным оповещениям контекст и видимость и самостоятельно выполнять поиск подозрительной активности.
- **Ускорение сертификации персонала** за счет укорочения времени обучения, необходимого аналитикам – новичкам для того, чтобы начать работать без снижения профессиональных требований.

## Как это работает?

SOC 3D интегрируется с SIEM и другими системами кибербезопасности в целях обеспечения единого интерфейса для обработки и устранения инцидентов кибербезопасности. Такие дополнительные модули системы и источники информации, как сбор предварительных данных по потенциальным угрозам, объединяются в целях автоматического обогащения информации и поддержки процесса принятия решений. Все необработанные данные и данные об инцидентах хранятся в центральном репозитории BigData, обеспечивая анализ, расследование и визуализацию в целях ускорения реагирования на инциденты.
Процедуры расследования угроз, рабочие процессы и действия по реагированию автоматизированы, скоординированы и отслеживаются, а тревожные оповещения автоматически приоритизируются в соответствии с их потенциальным воздействием на бизнес – так что персонал SOC высвобождаются для того, чтобы сосредоточиться на наиболее важных операциях и на инцидентах, представляющих наибольшую угрозу для бизнеса компании.

## Основные возможности SOC 3D

### Разумная автоматизация

SOC 3D автоматизирует три критически важных процесса SOC – принятие решений, обогащение данных и реагирование, экономя в среднем по 12 минут на каждый инцидент. SOC 3D автоматизирует сбор данных из различных источников (база данных управления конфигурации CMDB, инструментарий безопасности, данные из открытых источников, средства GRC, оценка уязвимости и др.), выдает и визуализирует дополнительную информацию персоналу SOC и автоматически выполняет действия по принятию решений – например, изменение приоритизации в соответствии со степенью критичности для бизнеса. Задачи реагирования и рабочие процессы также являются автоматизированными, экономя время и повышая эффективность процесса реагирования на инциденты.

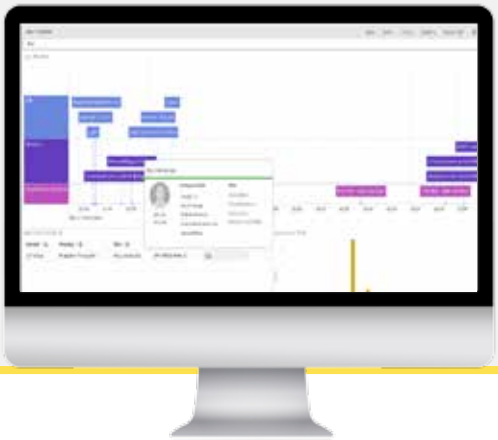
### Ориентация на бизнес

Обеспечивая безопасность организации с ориентацией на бизнес, SOC 3D предоставляет специалистам по кибербезопасности возможность выполнять более разумную обработку угроз на основе степени риска для бизнеса, гарантируя их концентрацию на том, что является наиболее важным. SOC 3D поддерживает расследования на основе бизнес – контекста, выполняет обзор всего бизнес – процесса и относящихся к нему активов и обеспечивает визуализированную ситуационную осведомленность в отношении критически важных для бизнеса областей, требующих особого внимания. Помимо того, SOC 3D предоставляет информацию руководству организации и другими заинтересованными сторонам, гарантируя информированность и осведомленность руководства относительно ситуации с кибербезопасностью и важной информации о реакции на инциденты.

### Анализ Big Data

Анализ BigData в SOC 3D обеспечивает доступ в реальном времени к необработанным и историческим данным из многочисленных информационных источников в компании и источников, относящихся к кибербезопасности, с поиском на естественном языке (“по типу Google”) и со средствами визуализации, которые приносят в тревожные оповещения видимость и контекст и поощряют упреждающий розыск. Анализ BigData ускоряет компьютерно - техническую экспертизу и реакцию на угрозы благодаря предоставлению всех данных в непосредственное распоряжение аналитика в целях более быстрого осознания и устранения угроз.
Источниками информации могут служить: устройства обеспечения безопасности, база данных управления конфигурации CMDB, данные об угрозах из открытых источников, системы антифрод и GRC, АД инструменты оценки уязвимости и др.

Расследование, основанное на бизнес – контексте



Анализ больших массивов данных, расследование, обогащение и визуализация

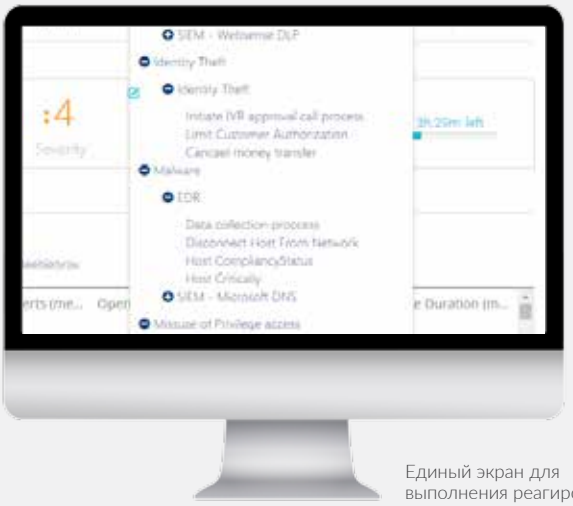
# Основные возможности SOC 3D

## Единая панель управления

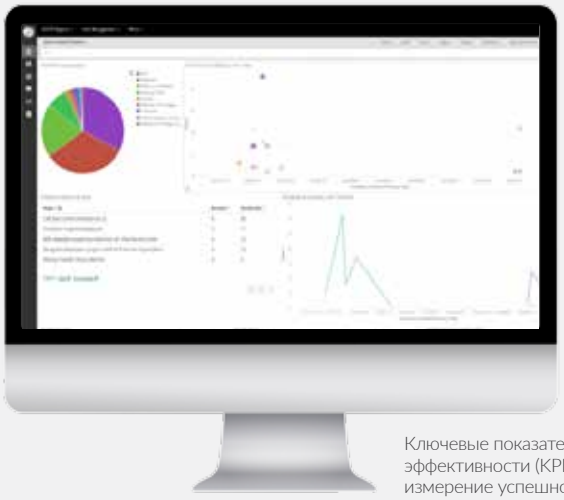
SOC 3D функционирует в качестве «узла кибербезопасности» организации, который централизует все функции SOC – обработку тревожных оповещений, расследования компьютерно - технической экспертизы и реагирование – в единой базовой системе. SOC 3D интегрируется со всеми системами выдачи тревожных оповещений, источниками обогащения данных и инструментами реагирования, осуществляя поддержку всего цикла устранения инцидента от его начала и до конца. Использование одной системы в качестве центра всех операций SOC повышает результативность операторов и аналитиков, требуя от них концентрации всего лишь на одном средстве, и уменьшает время обучения и повышения квалификации.

## Ключевые показатели эффективности (KPI) и измерение успешности

SOC 3D позволяет руководителям отделов информационной безопасности и менеджерам центров SOC осуществлять итоговое измерение и улучшение эффективности центра SOC путем контроля и визуализации показателей уровня обслуживания (SLA) и данных по сменам и по инцидентам. Специалисты могут с легкостью выявлять «узкие места», эффективные и неэффективные процедуры и осуществлять обзор тенденций в ситуации безопасности своей организации, что дает им возможность улучшать эффективность и функциональность SOC.



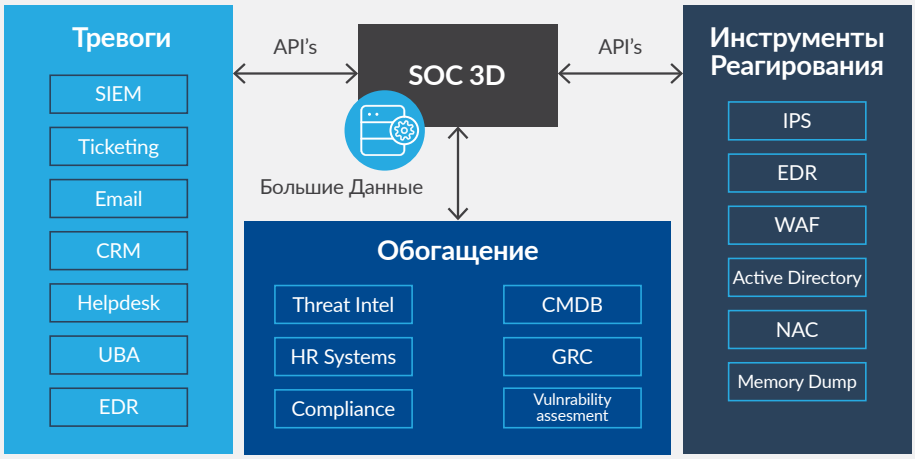
Единый экран для выполнения реагирования



Ключевые показатели эффективности (KPI) и измерение успешности

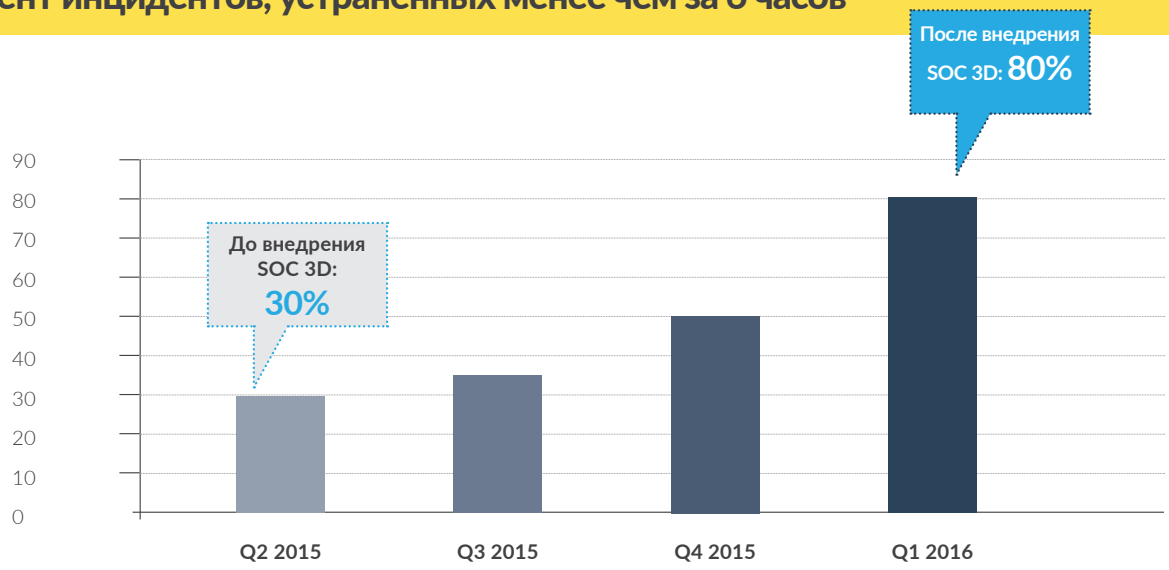
## Обогащенная интеграция со сторонними системами

SOC 3D может интегрироваться с любыми инструментами сторонних поставщиков через свой общий интерфейс API, который включает скрипты, REST и веб-сервисы. Таким образом любой источник тревожных оповещений и обогащения или инструмент реагирования с легкостью интегрируется с платформой для создания «узла безопасности» организации.




Типичные интерфейсы SOC 3D

## Процент инцидентов, устраненных менее чем за 6 часов




Постоянное улучшение в результате внедрения SOC 3D в большой организации, представленной на бирже NASDAQ

# О КОМПАНИИ CYBERBIT™

Cyberbit предлагает передовые решения в области кибербезопасности для финансовых организаций, предприятий критической инфраструктуры, военных и правительственных организаций. Портфолио компании предоставляет полный набор продуктов для обнаружения и митигации кибератак, а также помогает нашим Заказчикам решать оперативные задачи управления кибербезопасностью. Портфолио Cyberbit включает в себя решения по обнаружению и реагированию для конечных устройств (EDR), по кибербезопасности и контроля бесперебойной работы SCADA (SCADAShield), по автоматизации процессов управления SOC (SOC 3D), а также по подготовке персонала для обеспечения кибербезопасности на базе полнофункционального симулятора (Range). Продукты компании Cyberbit были выбраны крупными международными корпорациями по всему миру для обеспечения кибербезопасности своих сетей.

Cyberbit является стопроцентной дочерней компанией Elbit Systems Ltd. (NASDAQ и TASE: ESLT)

**sales@cyberbit.net | www.cyberbit.net**

**Офис в Израиле:**

CYBERBIT Commercial Solutions Ltd.
22 Zarhin St. Ra'anana
Israel 4310602
Тел.: +972-9-7799800 | E-mail: sales@cyberbit.net



CYBERBIT
PROTECTING A NEW DIMENSION