ТИНК СМАРТ ЕООД
1729 София, ул. Анна Ахматова 9, ет. 5
www.thinksmart.bg

ЕИК: 205946661
Банка: ЮРОБАНК И ЕФ ДЖИ IBAN:
BG93BPBI79401088794701

Think Smart

Изх. № 0001269/ 23.04.2021

| | |
|---|---|
| До: | ***АЕЦ Козлодуй ЕАД*** |
| На вниманието на: | ***Христо Пачев*** |
| E-mail: | commercial@npp.bg |
| Тел.#: | **+359 973 7 6140** |

# ИНДИКАТИВНО ПРЕДЛОЖЕНИЕ

за

„Доставка и изграждане на система за наблюдение, събиране, съхранение и анализ на събития /SIEM/ и автоматизирани инструменти за защита /SOAR/ в информационната система на „АЕЦ Козлодуй“ ЕАД”

Във връзка с пазарна консултация № 46660

## Съдържание

# I. ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ

## 1. Обхват

Настоящото техническо предложение е изготвено съгласно техническо задание № 20.АЕЦ.ТЗ.126. В обхвата на проекта са включени доставка и изграждане на следните две основни системи:

- Система за анализ на потребителското поведение чрез събиране, наблюдение и анализ на лотовете в корпоративна мрежа или „Security Information and Event Management (SIEM)“ - Exabeam
- Система за реакция, управление и автоматизация на решенията за сигурност или Security Orchestration, Automation § Response (SOAR) – PaloAlto Cortex XSOAR

Подробно описание на основните характеристики и функционалности на предлаганото от компанията решение за система за наблюдение, събиране, съхранение и анализ на събития /SIEM/ и автоматизирани инструменти за защита /SOAR/, покриващо минималните изисквания на техническото задание, може да бъде намерено в приложените технически брошури.

При успешна реализация на проекта ще бъде постигнато цялостно повишаване нивото на информационна сигурност, включително:

- откриване на известни и неизвестни заплахи с помощта на откриване на известни и неизвестни заплахи с помощта на поведенчески анализи за подобряване на точността и намаляване на времето за реакция (разследване и реакция в рамките на минути вместо дни);
- автоматизиране на разследването и реакцията с помощта на предварително изградени сценарии за инциденти (SOAR);
- централизиране на работните процеси за откриване, разследване и реагиране в един потребителски интерфейс;
- постигане на съответствие с чл. 28, чл. 29, чл. 30 и чл. 31 от „Наредба за минималните изисквания за мрежова и информационна сигурност“.

Към оборудването ще се доставят нужните интерфейсни и захранващи кабели, монтажни елементи, инструменти, специализиран софтуер, драйвери и лицензи, необходими за монтаж и интегриране на компонентите в съответните информационни системи на АЕЦ Козлодуй.

## 2. Дейности за изпълнение проекта

### 2.1. Инсталация и въвеждане в експлоатация

След доставката на оборудването, ще бъде направена първоначална инсталация и конфигурация на устройствата, съгласувано с изискванията на Възложителя.

### 2.2. Обучение и квалификация на персонала на „АЕЦ Козлодуй” ЕАД

Ще бъде подсигурено обучение на най-малко двама /2/ служители на възложителя в учебен център или ще бъде организирана виртуална среда на обучение, разработена от производителя, на български език.

За провеждане на обучението ще предоставим сертификат за инженер по мрежова сигурност, издаден от производителя на предлаганото оборудване или от упълномощен от него представител и сертификат за инструктор по мрежова сигурност, издаден от производителя на предлаганото оборудване или от упълномощен от него представител.

На завършилите успешно курса се издава сертификат за преминато обучение.

При необходимост или по искане на Възложителя, в периода на гаранционната поддръжка, може да се организират полудневни или целодневни сесии за трансфер на знания по изготвена от Изпълнителя и съгласувана с Възложителя програма.

## 3. Гаранционно обслужване

Предложеното решение е с 3 години оригинална (от производителя) гаранция.

Лицензи, абонаментна поддръжка /subscriptions/ на името на „АЕЦ Козлодуй“ ЕАД, вкл. и хартиено копие са за срок от 3 години, съгласно техническото задание на АЕЦ Козлодуй ЕАД.

Гаранционното обслужване обхваща следните дейности:

- отстраняване на проблеми при функционирането, дължащи се на дефекти в оборудването, неправилни настройки и конфигурации, вкл. при инсталирането му в инфраструктурата на Възложителя;

- поддържане на лицензи и активни абонаменти за нови дефиниции версии съобразно договореното ниво.

Параметрите на качеството на обслужване на доставеното оборудване са както следва:

- режим на приемане на заявки (по телефон, e-mail или регистриране на проблем в on-line система за сервизно обслужване) - поддържащ център (help desk) 24/7;

- време за реакция (потвърждаване на получена заявка) от момента на подаването ѝ за възникнал проблем - максимално 60 минути в работно време;

- време за възстановяване на функционалностите и услугите предоставяни с отдалечен достъп (независимо от характера на проблема) - до един работен ден;

- време за разрешаване на хардуерен проблем - максимално три работни дни;

- възможност за подмяна (ако периодът за ремонт е по-дълъг от допустимото време за решаването на проблема) на дефектните части или компоненти с част или компонент със същите или по-добри характеристики.

## 4. Място за доставка

Заявените оборудване и материали ще бъдат доставени в складовете на „АЕЦ Козлодуй” ЕАД в оригиналната опаковка на производителя.

## 5. Съпроводителна документация за различните етапи на изпълнение

Доставката на новото оборудване се придружава със следните документи, представени на български език:

### 5.1. Документи, издавани при доставка:

1) Декларация за съответствие;
2) Спецификация на доставеното оборудване и софтуер;
3) Декларация за произход;
4) Пълен комплект документация за доставения софтуер и хардуер (в електронен вид).

### 5.2. Документи, издавани след монтажа:

1) Акт за завършен монтаж,

### 5.3. Документи, издавани при въвеждане в експлоатация:

1) Протокол за входящ контрол без забележки;
2) Протокол от функционални изпитания;
3) „Ръководство на администратор”, съдържащо направените конфигурации на устройствата и начина за администриране на същите.

## 6. Осигуряване на качеството

### 6.1. Система за управление (СУ)

Тинк Смарт прилага сертифицирана система за:

- управление на качеството в съответствие с БДС EN ISO 9001:2015, с обхват покриващ дейностите по техническото задание на възложителя, което можем да удостоверим с копие на валиден сертификат при изпълнение.
- информационна сигурност в съответствие с БДС ISO/IEC 27001:2013, с обхват включващ изграждане и поддръжка на системи за защита на информацията, което можем да удостоверим с копие на валиден сертификат при изпълнение.
- ИТ услуги в съответствие с БДС ISO/IEC 20000-1:2018, с обхват включващ изграждане и поддръжка на системи за системи за защита на информацията, което можем да удостоверим с копие на валиден сертификат при изпълнение.

### 6.2. План за контрол на качеството (ПКК)

За изпълнение на дейностите в обхвата на Техническото задание компанията ще разработи План за контрол на качеството, който ще включва технологичната последователност на операциите, входящ контрол и изпитания с отбелязани точки на контрол от страна на Възложителя и Изпълнителя.

При достигане на точка за контрол изпълнението на дейностите се задържа до извършване и документиране на планирания контрол. Работата по договора продължава след положителен резултат от контрола.

ПКК се изготвя по образец, представен от „АЕЦ Козлодуй” ЕАД.

ПКК се представя за преглед и съгласуване от страна на „АЕЦ Козлодуй” ЕАД, до 20 календарни дни преди готовността за работа на компанията Изпълнител.

ПКК се предава като отчетен документ при приемане на услугата от страна на Възложителя.

### 6.3. Управление на несъответствията

Компанията изпълнител уведомява „АЕЦ Козлодуй" ЕАД за несъответствията, открити в хода на изпълнение на дейностите по договора. Несъответствия на продукти и услуги, за които се изисква преработка, се докладват на Възложителя (отговорното лице по договор/ръководителя на структурното звено Заявител на чиято територия се извършват дейностите), за да се вземе решение за разпореждане с несъответстващия продукт/услуга.

### 6.4. Квалификация на Тинк Смарт за изпълнение на поръчката, свързана със специфичните изисквани на възложителя за осигуряване на качеството

Тинк Смарт е оторизиран от Производителя за извършване на продажба, гаранционна поддръжка и сервиз на предложеното оборудване, включително за територията на Република България, за което представяме поименно оторизационно писмо. Същото ще бъде издадено и след датата на обявяване на обществената поръчка.

Тинк Смарт има успешно реализирани 3 проекта за доставка на софтуер и изграждане на системи за повишаване на нивото на информационната сигурност, доказани с писмени референции от клиентите.

## 7. Срокове за изпълнение

7.1. **Срок за доставка –** до 60 дни след сключен договор, заявка за изпълнение и осигурен достъп.

7.2. **Срок за монтаж и въвеждане в експлоатация –** до 60 дни след направена доставка и осигурен достъп за изпълнение на дейностите.

7.3. **Гаранционен срок и обслужване** – 3 години след двустранно подписан приемо-предавателен протокол за въведена в експлоатация система.

## 8. Информация за контакт

| | |
|---|---|
| Изпълнител: | "ТИНК СМАРТ" ЕООД |
| Адрес за кореспонденция: | 1729 София, ж.к. Младост 1А, ул. Анна Ахматова 9, ет. 5 |
| ЕИК | 205946661 |
| IBAN: | BG93BPBI79401088794701 |
| BIC, при банка: | BPBIBGSF, ЮРОБАНК И ЕФ ДЖИ клон София |
| МОЛ | Стефан Джурелов |
| E-mail | office@thinksmart.bg |
| Интернет адрес: | www.thinksmart.bg |

## 9. Валидност на предложението: 90 календарни дни.

## II. ЦЕНОВО ПРЕДЛОЖЕНИЕ

| № | Описание на предложеното оборудване | Мярка | Кол. | Единична цена в лева без ДДС | Обща цена в лева без ДДС |
|---|---|---|---|---|---|
| 1. | Доставка на оборудване и софтуер | бр. | 1 | 3,355,770.00 | 3,355,770.00 |
| 2. | Монтаж, инсталация и въвеждане в експлоатация, вкл. обучение | бр. | 1 | 172,000.00 | 172,000.00 |
| | | | | **Общо в лева без ДДС** | **3,527,770.00** |

## III. ПРИЛОЖЕНИЯ

Техническа брошура Exabeam EX3000

Техническа брошура Exabeam EX4003

Техническа брошура Exabeam advanced analytics

Техническа брошура Threat Hunter

Техническа брошура Exabeam data lake

Техническа брошура Cortex XSOAR

Копие на Оторизационни писма

С уважение,
**Стефан Джурелов**
Управител ТИНК СМАРТ ЕООД
+359888438195
stefan.dzhurelov@thinksmart.bg

Think Smart

www.thinksmart.bg

# Exabeam EX3000

Hardware Specifications - Gen 2

Publication date August 5, 2020

**Exabeam**
2 Waters Park Dr. Suite 200
San Mateo, CA 94403

650.209.8599

Have feedback on this guide? We'd love to hear from you!
Email us at docs@exabeam.com

Disclaimer: Please ensure you are viewing the most
up-to-date version of this guide
by visiting the Exabeam Community.

## Copyright

## Trademarks

Exabeam, the Exabeam logo, Threat Hunter, Smarter SIEM, Smart Timelines and Security Management Platform are service marks, trademarks or registered marks of Exabeam, Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. The marks and logos displayed in this document may not be used without the prior written consent of Exabeam or their respective owners.

## Patents

Exabeam owns, and reserves all rights for, patents for Exabeam products and services, which may be protected under registered patents as well as patents pending.

## Other Policies

For information regarding Exabeam’s treatment of personally identifiable information, please review Exabeam’s current privacy policy at www.exabeam.com/privacy.

## Table of Contents

# 1. EX3000 Hardware Specifications

*Gen 2*

This type of appliance is to be used for Exabeam Data Lake, for the following node types:

- Data Lake Master node
- Any Data Lake worker nodes

If you have questions about this appliance, please go to Exabeam Community for more information or create a ticket for more assistance.

| Server Configurations | |
|---|---|
| Model | Supermicro SuperChassis 826BE1C-R920LPB |
| Motherboard | Super X10SRH-CF |
| CPU | Intel Xeon processor E5-2620 v4<br>• 8 cores (16 threads) with 2.1 GHz base frequency and 20 MB cache |
| Memory | 192 GB (DDR4)<br>• DDR4-2666 MHz<br>• 6 x 32 GB |
| Chassis Configuration | 25.5" Depth 2U Rackmount Chassis<br>• 12 x 3.5 in drive bays |
| Storage | 1 x 240 GB (SSD)<br>• 1.4 DWPD, SATA3, 2.5 in<br>• Intel S4510 240 GB<br>2 x 1.92 TB (SSD)<br>• 0.8 DWPD, DATA, 2.5 in<br>• Samsumg PM883 1.92 TB<br>9 x 4 TB (HDD)<br>• 7,200 RPM, 2.5 in<br>• Seagate 7E200 EC 3.5v5 4TB SATA 512E |

| Server Configurations | |
|---|---|
| Network Controller | 2 x 1 Gbps (RJ45) LAN<br>1 x dedicated IPMI |

| Server Dimensions | |
|---|---|
| Height | 3.5" (89 mm) |
| Width | 17.2" (437 mm) |
| Depth | 25.5" (647 mm) |
| Packaging | 26.7" (H) x 11.4" (W) x 34.5" (D) |
| Gross Weight | 63.26 lbs (28.75 kg) |
| Net Weight | 55 lbs (24.95 kg) |

| Operating Environment (System) | | |
|---|---|---|
| | Operating | Non-Operating |
| Heat Output | 480.41 BTU/hr | 348.02 BTU/hr |
| Temperature Range | 5°C - 35°C (41°F - 95°F) | -40°C - 70°C (-40°F - 158°F) |
| Relative Humidity Range (non-condensing) | 8% - 90% | 5% - 95% |

| Power Supply | |
|---|---|
| Two quantity of 1U 920W Redundant Platinum Super Quiet power supply with PMbus | |
| AC Voltage | 700W: 100  140V, 50-60 Hz<br>750W: 200  240V, 50-60 Hz<br>920W: 100-240Vac, 50-60 Hz |
| +5V Standby | Max: 4A / Min: 0A |
| +12V | Max: 75A / Min: 1A (100Vac – 240Vac) |
| Cable CBL-0160L | NEMA5-15P to C13 US power cord 16AWG 6ft, PBF (default for high watt) |

| Certifications | |
|---|---|
| Power Supply Safety / EMC | • BSMI<br>• CCC<br>• CE/EMC<br>• FCC class B<br>• TUV/CB<br>• UL/CUL |

exabeam

# Exabeam EX4003

## Hardware Specifications

Publication date July 24, 2020

**Exabeam**
2 Waters Park Dr. Suite 200
San Mateo, CA 94403

650.209.8599

Have feedback on this guide? We'd love to hear from you!
Email us at docs@exabeam.com

Disclaimer: Please ensure you are viewing the most
up-to-date version of this guide
by visiting the Exabeam Community.

## Copyright

## Trademarks

## Patents

## Other Policies

For information regarding Exabeam’s treatment of personally identifiable information, please review Exabeam’s current privacy policy at www.exabeam.com/privacy.

## Table of Contents

# 1. EX4003 Hardware Specifications

This type of appliance is to be used for Exabeam Advanced Analytics, for the following node type:

- Master node for Advanced Analytics

If you have questions about this appliance, please go to Exabeam Community for more information or create a ticket for more assistance.

| Server Configurations | |
|---|---|
| Model | Supermicro SuperServer SYS-1019P-WTR |
| Motherboard | Super X11SPW-TF |
| CPU | Intel Xeon Gold 6230 2.1 GHz processor<br>• 20 cores/40 threads with 2.1 GHz base frequency and 27.5 MB cache |
| Memory | 256 GB (DDR4)<br>• 4 x 64 GB<br>• Micron 64 GB 2666MHz LRDIMM Z01B Dual Label |
| Storage | 2 x 240 GB (SSD)<br>• 2.0 DWPD, SATA3, 2.5 in<br>• Intel S4510 240 GB<br>2 x 3.84 TB (SSD)<br>• 3.0 DWPD, SATA, 2.5 in<br>• Samsung SM883 3.84 TB<br>6 x 2 TB (HDD)<br>• 7200 RPM, 2.5 in<br>• Seagate 7E200 EC2.5 2TB SATA 512E |
| Chassis Configuration | 23.5" Depth 1U Rackmount Chassis<br>• 10 drive bays (2.5 in) |

| **Server Configurations** | |
|---|---|
| Network Controller | 2 x 10 Gbps (RJ45) LAN<br>1 x dedicated IPMI |

| **Server Dimensions** | |
|---|---|
| Height | 1.7" (43.7 mm) |
| Width | 17.2" (437 mm) |
| Depth | 23.5" (597 mm) |
| Packaging | 8" (H) x 24" (W) x 32" (D)<br>203 mm (H) x 610 mm (W) x 813 mm (D) |
| Gross Weight | 27 lbs (12.25 kg) |
| Net Weight | 15.5 lbs (7.03 kg) |

| **Operating Environment (System)** | | |
|---|---|---|
| | Operating | Non-Operating |
| Heat Output | 599.49 BTU/hr | 281.49 BTU/hr |
| Temperature Range | 10°C - 35°C (50°F - 95°F) | -40°C - 60°C (-40°F - 140°F) |
| Relative Humidity Range (non-condensing) | 8% - 90% | 5% - 95% |

| **Power Supply** | |
|---|---|
| 500W Redundant Power Supplies with PMBus | |
| AC Voltage | 100-240Vac, 50-60Hz, 6.1-2.6A |
| +5V Standby | Max: 4A / Min: 0A |
| +12V | Max: 42A / Min: 0.5A |

| **Certifications** | |
|---|---|
| Power Supply Safety / EMC | 80 PLUS Platinum Certified |

exabeam

DATASHEET

# EXABEAM ADVANCED ANALYTICS

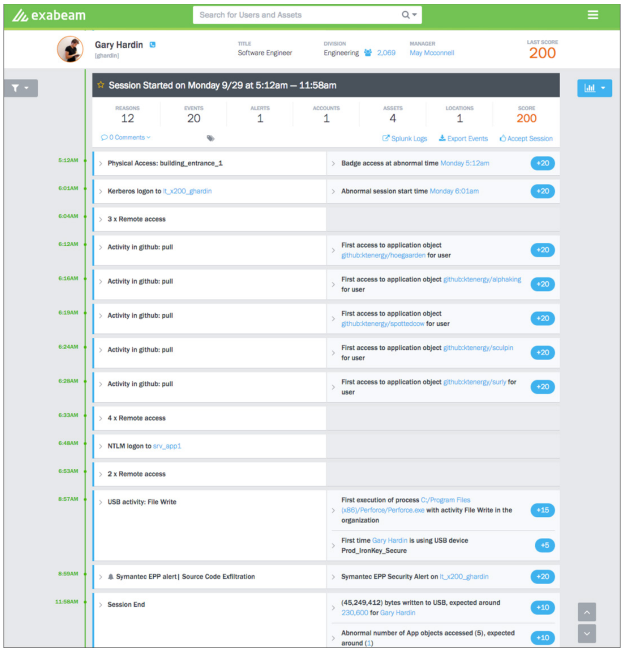
## SHINE A LIGHT ON MODERN CYBER-ATTACKS

Today's credential based threats are complex, often touching many systems, using multiple log-ins, and spanning a period of several months. These insider threats involve the legitimate credentials and access privileges of real users, making them challenging for legacy security solutions to detect. In order to tackle these insidious threats, organizations need a solution built from the ground up using modern technologies such as machine learning, behavioral analysis and data science.

### A SMARTER APPROACH TO DETECTION AND INVESTIGATION

Exabeam Advanced Analytics is the world's most deployed behavioral analytics platform. Advanced Analytics automatically links and analyzes user and entity activity to better inform security analysts about threats and corresponding remediation. Advanced Analytics provides a powerful analytics layer on top of existing SIEM and log management technologies, detecting new attacks, prioritizing incidents, and guiding a more effective response.

Exabeam Advanced Analytics combines a purpose-built architecture with an investigation-focused user experience designed to fit the way security professionals actually work. Advanced Analytics uses a proprietary Session Data model that automatically stitches together event timelines, including both normal and abnormal behavior, before flagging potential threats. This reduces the manual effort security analysts spend on investigations and increases their productivity.



Gary Hardin [ghardin]

| TITLE | DIVISION | MANAGER | LAST SCORE |
|---|---|---|---|
| Software Engineer | Engineering 2,069 | May Mcconnell | 200 |

Session Started on Monday 9/29 at 5:12am — 11:58am

| REASONS | EVENTS | ALERTS | ACCOUNTS | ASSETS | LOCATIONS | SCORE |
|---|---|---|---|---|---|---|
| 12 | 20 | 1 | 1 | 4 | 1 | 200 |

| | | | |
|---|---|---|---|
| 5:12AM | Physical Access: building_entrance_1 | Badge access at abnormal time Monday 5:12am | +20 |
| 6:01AM | Kerberos logon to lt_x200_ghardin | Abnormal session start time Monday 6:01am | +20 |
| 6:04AM | 3 x Remote access | | |
| 6:12AM | Activity in github: pull | First access to application object github:ktenergy/hoegaarden for user | +20 |
| 6:16AM | Activity in github: pull | First access to application object github:ktenergy/alphaking for user | +20 |
| 6:19AM | Activity in github: pull | First access to application object github:ktenergy/spottedcow for user | +20 |
| 6:24AM | Activity in github: pull | First access to application object github:ktenergy/sculpin for user | +20 |
| 6:28AM | Activity in github: pull | First access to application object github:ktenergy/surly for user | +20 |
| 6:33AM | 4 x Remote access | | |
| 6:48AM | NTLM logon to srv_app1 | | |
| 6:53AM | 2 x Remote access | | |
| 8:57AM | USB activity: File Write | First execution of process C:/Program Files (x86)/Perforce/Perforce.exe with activity File Write in the organization<br>First time Gary Hardin is using USB device Prod_IronKey_Secure | +15<br>+5 |
| 8:59AM | Symantec EPP alert \| Source Code Exfiltration | Symantec EPP Security Alert on lt_x200_ghardin | +20 |
| 11:58AM | Session End | (45,249,412) bytes written to USB, expected around 230,600 for Gary Hardin<br>Abnormal number of App objects accessed (5), expected around (1) | +10<br>+10 |

### RAPID TIME TO VALUE

Regardless of the data type or source, Exabeam makes it easy for customers to make use of all of the information available to them in order to perform a truly comprehensive assessment of the threats on their network. Advanced Analytics can ingest logs from a SIEM or directly from the data sources themselves via Syslog. Customers are able to rapidly deploy and analyze historical logs for quick time to value, or analyze new log sources in Advanced Analytics which were previously cost prohibitive to send to their SIEMs. This flexible data handling delivers a fast time to value of unmatched by other behavioral analytics solutions.

### COMPOUNDING OPERATIONAL AND COST EFFICIENCIES

The benefits of the Advanced Analytics solution are compounded by Exabeam Log Manager and Incident Responder which together provide full end-to-end coverage for data storage, access, analytics, and automated response. Advanced Analytics can be deployed as a standalone solution, or as part of the larger Exabeam Security Intelligence Platform.

## KEY FEATURES

Exabeam provides world class threat detection, prioritizes analyst workloads, and greatly improves SOC productivity. Its key features include:

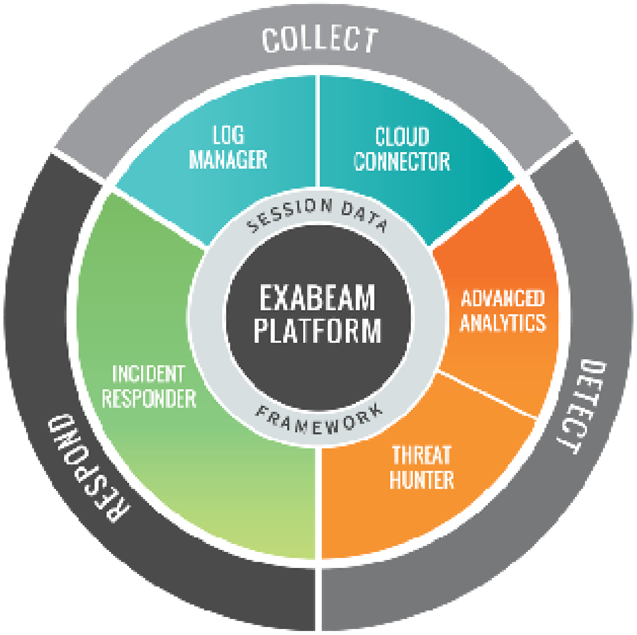
- User and Entity Behavior Analysis (UEBA) based detection for complex modern threats including credential-based attacks, insider threats, and ransomware
- Pre-constructed session timelines which automate analyst investigation, and make proactive analysis faster and easier
- Intelligent security alert prioritization to ensure analysts can easily find the alerts which require the most attention
- A unique session data model that automatically detects lateral movement including changes of credentials, IP addresses, or devices
- Interoperability with all major SIEM solutions, as well as Exabeam's Log Management and Incident Response solutions
- Ease of setup and use
- Scale-out multi-node architecture
- Supports 500+ data sources out of the box
- Ability to deploy as a pre-sized physical appliances or as a cloud-ready VM

## EXABEAM SECURITY INTELLIGENCE PLATFORM

Exabeam Log Manager is a key component in the Exabeam Security Intelligence Platform. Any of the platform components can be used together or separately with third party products. The platform includes:

- **Exabeam Log Manager**
- **Exabeam Advanced Analytics**
- **Exabeam Threat Hunter**
- **Exabeam Incident Responder**
- **Exabeam Cloud Connectors**

To learn more about these products, please visit www.exabeam.com/products to download whitepapers, datasheets, etc.



## OPERATING INFORMATION

- Deployable as a physical appliance (in multiple sizes) or as a cloud-ready virtual machine
- Includes out of the box collection agents and parsers for over 500 security data sources
- Agents operate on Windows or Linux platforms

For more information, please contact Exabeam at info@exabeam.com

exabeam

DATASHEET

# THREAT HUNTER

User and Entity Behavior Analytics (UEBA) relies on machine learning to transform millions of events into the handful of users that are performing risky behavior right now. In essence, UBA is about the machine telling the security analyst where to focus. Threat hunting is a complementary technique that enables analysts to query the event data to find users that match a specific set of criteria. Threat Hunting is about the analyst telling the machine to find the users that fit X, Y, and Z parameters.

Exabeam is the only security intelligence vendor to provide both powerful UEBA capabilities and market-leading threat hunting functionality, now available through Exabeam Threat Hunter.

## Query, Pivot, and Drill Down on Session Data

The Exabeam platform uses Stateful User Tracking™ to connect individual user activities into a session data model. Threat Hunter allows security professionals to query the platform to find all users whose sessions contain specific activities or attributes, or any combination of activities or attributes. For example, an analyst might first ask for all user sessions where the user logged into the VPN from a foreign country for the first time. The analyst can then trim the results by asking for users who then accessed a server for the first time, and then later the anti-malware software flagged a problem on that server. While each of these activities is independent of the others, the ability to combine them in a simple, point-and-click search provides significant power to even a junior analyst.

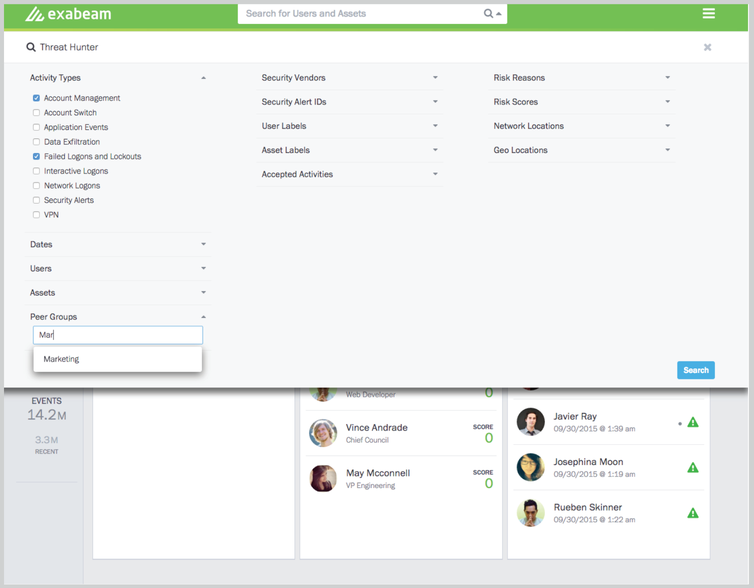
## Pull on Threads, Find Hidden Threats

While the UBA engine is designed to find users who have performed multiple activities that, together, add up to an elevated risk score, Threat Hunter gives analysts the tools to “pull on threads” to track activity that is deliberately kept under the radar. Threat hunting can be very effective after UBA is used to detect an attack. Where UBA can identify a specific attack, ThreatHunter can proactively search for groupings of activities that are similar to aspects of that attack. As a result, Threat Hunter customers are more effective at responding to all aspects of a cyber attack.

## Proactive Security Intelligence

In the example shown here, an analyst uses Threat Hunter to clean up after a malware outbreak in the marketing department that allowed hackers to penetrate the network.

The analyst begins by hunting for all sessions where any user in Marketing performed account management (i.e. new account creation or privilege escalation) and also had a failed logon. The analyst doesn’t need to understand the structure of the applicable logs, nor the search language of the un-derlying log management system. She simply clicks a few fields and hits “Search.”



Activity Types
☑ Account Management
☐ Account Switch
☐ Application Events
☐ Data Exfiltration
☑ Failed Logons and Lockouts
☐ Interactive Logons
☐ Network Logons
☐ Security Alerts
☐ VPN

Peer Groups: Mar

**Threat Hunter:** *Easily Enter Hunt Parameters*

### Filter and Drill Down

The analyst filters the result set further by adding a parameter where the event type equals "Account password was changed." Threat Hunter responds with a list of all users, within the default time period, who are in the marketing department and had credentials that were used to perform account management, had a failed logon, and then changed the account password.

Near the top of the list we see one user, Angella French, who has been flagged by Exabeam UBA as having unusual account lockout activity.

The analyst clicks on Angella, and Exabeam displays detailed information about her identity and the events associated with this lockout.

We see a very high number of failed logons across thirteen different systems. As account lockouts can be a strong signal of a compromised account and a hacker impersonating a valid internal user, this is worth further investigation.

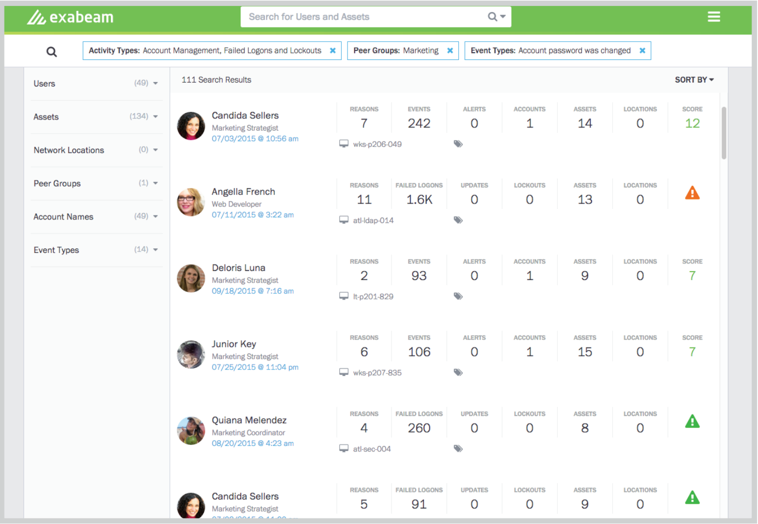
The analyst now has an additional candidate for malware infection and account takeover within the Marketing department, and can respond accordingly.

### Works With Any Log or SIEM System

Exabeam UBA and Threat Hunter include prebuilt integrations with all leading log management products, including:

- IBM QRadar
- Splunk
- HP ArcSight
- McAfee ESM
- RSA Security Analytics

**In addition, Threat Hunter** and UBA can integrate with any log system via syslog forwarding. Additional feeds from products such as Data Loss Prevention, endpoint security, cloud security, and others can be easily integrated and used in threat hunting.



Activity Types: Account Management, Failed Logons and Lockouts ✖ | Peer Groups: Marketing ✖ | Event Types: Account password was changed ✖

| | |
|---|---|
| Users | (49) |
| Assets | (134) |
| Network Locations | (0) |
| Peer Groups | (1) |
| Account Names | (49) |
| Event Types | (14) |

111 Search Results — SORT BY

Candida Sellers
Marketing Strategist
07/03/2015 @ 10:56 am
REASONS 7 · EVENTS 242 · ALERTS 0 · ACCOUNTS 1 · ASSETS 14 · LOCATIONS 0 · SCORE 12
wks-p206-049

Angella French
Web Developer
07/11/2015 @ 3:22 am
REASONS 11 · FAILED LOGONS 1.6K · UPDATES 0 · LOCKOUTS 0 · ASSETS 13 · LOCATIONS 0 · ⚠
atl-ldap-014

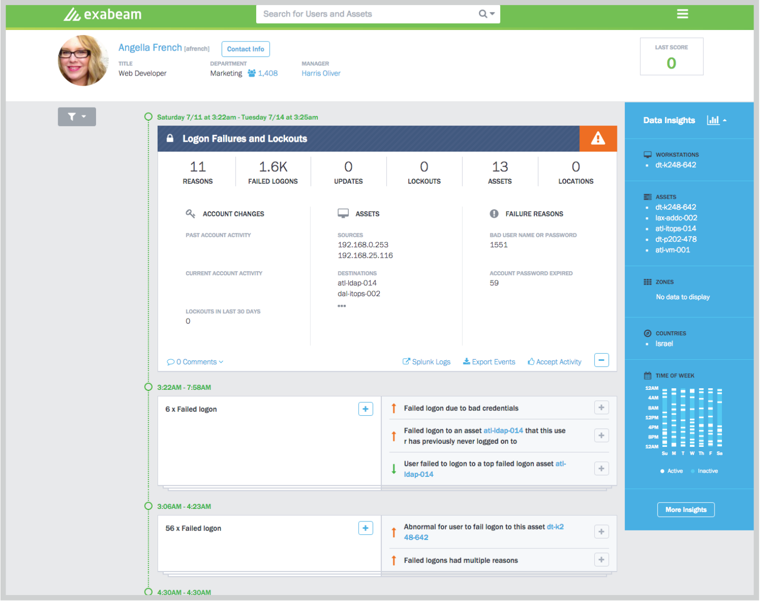
Deloris Luna
Marketing Strategist
09/18/2015 @ 7:16 am
REASONS 2 · EVENTS 93 · ALERTS 0 · ACCOUNTS 1 · ASSETS 9 · LOCATIONS 0 · SCORE 7
lt-p201-829

Junior Key
Marketing Strategist
07/25/2015 @ 11:04 pm
REASONS 6 · EVENTS 106 · ALERTS 0 · ACCOUNTS 1 · ASSETS 15 · LOCATIONS 0 · SCORE 7
wks-p207-835

Quiana Melendez
Marketing Coordinator
08/20/2015 @ 4:23 am
REASONS 4 · FAILED LOGONS 260 · UPDATES 0 · LOCKOUTS 0 · ASSETS 8 · LOCATIONS 0 · ⚠
atl-sec-004

Candida Sellers
Marketing Strategist
REASONS 5 · FAILED LOGONS 91 · UPDATES 0 · LOCKOUTS 0 · ASSETS 9 · LOCATIONS 0 · ⚠

**Threat Hunter:** *Session Results List*



Angella French [afrench]
TITLE: Web Developer
DEPARTMENT: Marketing 1,408
MANAGER: Harris Oliver
LAST SCORE: 0

Saturday 7/11 at 3:22am - Tuesday 7/14 at 3:25am

Logon Failures and Lockouts ⚠

11 REASONS · 1.6K FAILED LOGONS · 0 UPDATES · 0 LOCKOUTS · 13 ASSETS · 0 LOCATIONS

ACCOUNT CHANGES
PAST ACCOUNT ACTIVITY
CURRENT ACCOUNT ACTIVITY
LOCKOUTS IN LAST 30 DAYS: 0

ASSETS
SOURCES: 192.168.0.253, 192.168.25.116
DESTINATIONS: atl-ldap-014, dal-itops-002 ...

FAILURE REASONS
BAD USER NAME OR PASSWORD: 1551
ACCOUNT PASSWORD EXPIRED: 59

3:22AM - 7:58AM
6 x Failed logon
- Failed logon due to bad credentials
- Failed logon to an asset atl-ldap-014 that this use r has previously never logged on to
- User failed to logon to a top failed logon asset atl-ldap-014

3:06AM - 4:23AM
56 x Failed logon
- Abnormal for user to fail logon to this asset dt-k2 48-642
- Failed logons had multiple reasons

4:30AM - 4:30AM

Data Insights
WORKSTATIONS
- dt-k248-642

ASSETS
- dt-k248-642
- lax-addc-002
- atl-itops-014
- dt-p202-478
- atl-vm-001

ZONES
No data to display

COUNTRIES
- Israel

TIME OF WEEK

**Threat Hunter:** *Drill Down Into a Specific User Session*

## For more information, please contact Exabeam at info@exabeam.com

exabeam

DATASHEET

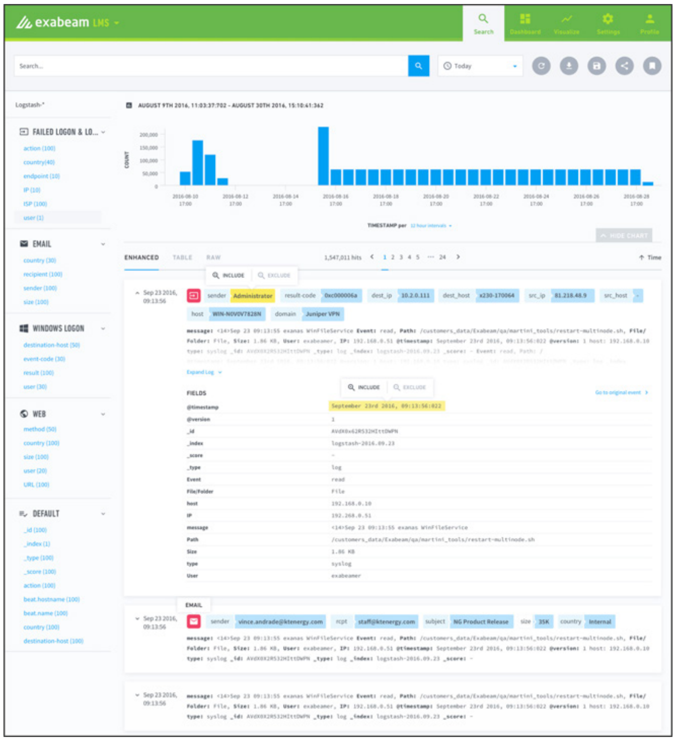
# EXABEAM DATA LAKE

## LEGACY LOG MANAGEMENT IS RIPE FOR DISRUPTION

Log management is a fundamental component of a strong enterprise security architecture. It supports security intelligence and analytics, as well as compliance and forensics reporting. The good news is that the log management process is mature and well-understood. The bad news is that log management vendors have not kept pace with rapid changes in data growth, cloud architectures, and open source big data management. Log management systems are now measured in petabytes, with data streaming in from internal networks and the cloud. Legacy log management systems simply weren't designed for such an environment. Even worse, these systems are licensed "by the byte," becoming more expensive every year as data grows and requiring CISOs to plunk down more of their budget for no associated gain.

Exabeam Data Lake is different. It's designed for the modern world, with a scale-out architecture that can support any volume of data, and for a predictable price.

### LOG SEARCH SHOULDN'T BE PAINFUL



Sep 23 2016, 09:13:56

sender Administrator · result-code 0xc000006a · dest_ip 10.2.0.111 · dest_host x230-170064 · src_ip 81.218.48.9 · src_host -
host WIN-N0V0V7828N · domain Juniper VPN

```
message: <14>Sep 23 09:13:55 exanas WinFileService Event: read, Path: /customers_data/Exabeam/qa/martini_tools/restart-multinode.sh, File/
Folder: File, Size: 1.86 KB, User: exabeamer, IP: 192.168.0.51 @timestamp: September 23rd 2016, 09:13:56:022 @version: 1 host: 192.168.0.10
type: syslog _id: AVdX0X2R532HIttDWPN _type: log _index: logstash-2016.09.23 _score: - Event: read, Path: /
```

FIELDS

| | |
|---|---|
| @timestamp | September 23rd 2016, 09:13:56:022 |
| @version | 1 |
| _id | AVdX0x62R532HIttDWPN |
| _index | logstash-2016.09.23 |
| _score | - |
| _type | log |
| Event | read |
| File/Folder | File |
| host | 192.168.0.10 |
| IP | 192.268.0.51 |
| message | <14>Sep 23 09:13:55 exanas WinFileService |
| Path | /customers_data/Exabeam/qa/martini_tools/restart-multinode.sh |
| Size | 1.86 KB |
| type | syslog |
| User | exabeamer |

Sep 23 2016, 09:13:56

sender vince.andrade@ktenergy.com · rcpt staff@ktenergy.com · subject NG Product Release · size 35K · country Internal

```
message: <14>Sep 23 09:13:55 exanas WinFileService Event: read, Path: /customers_data/Exabeam/qa/martini_tools/restart-multinode.sh, File/
Folder: File, Size: 1.86 KB, User: exabeamer, IP: 192.168.0.51 @timestamp: September 23rd 2016, 09:13:56:022 @version: 1 host: 192.168.0.10
type: syslog _id: AVdX0X2R532HIttDWPN _type: log _index: logstash-2016.09.23 _score: -
```

Sep 23 2016, 09:13:56

```
message: <14>Sep 23 09:13:55 exanas WinFileService Event: read, Path: /customers_data/Exabeam/qa/martini_tools/restart-multinode.sh, File/
Folder: File, Size: 1.86 KB, User: exabeamer, IP: 192.168.0.51 @timestamp: September 23rd 2016, 09:13:56:022 @version: 1 host: 192.168.0.10
type: syslog _id: AVdX0X2R532HIttDWPN _type: log _index: logstash-2016.09.23 _score: -
```

Exabeam Data Lake is built on a foundation of proven, scalable open source big data technology, including HDFS and Elasticsearch. Many Web-scale companies rely on these technologies today to support the massive data volumes they generate.

HDFS is tailor-made for analytics and Elasticsearch is perfect for time series data management. Exabeam Data Lake integrates these technologies with others in the Elasticsearch stack to create a thoroughly modern log management solution.

Exabeam adds enterprise features such as remote collection agent management and security data enrichment to these proven technologies, and packages the solution for easy deployment and operations.

### LOG STORAGE SHOULD BE PREDICTABLE

Unlike other log management products, Exabeam Data Lake is licensed in a predictable, per-user model so that you can capture as much data as you need for reporting and analytics. Want to add your EDR or DLP data into your log system? How about your network data? If you tried that with another product, the additional bills would  quickly drain your budget. With Exabeam Data Lake, there is no charge for extra data, so you can finally log and analyze anything necessary to detect and respond to modern threats.

Log data management has become commoditized through the use of excellent open source technologies. Exabeam offers a petabyte-scale system that extends these proven building blocks.

## KEY FEATURES

While Exabeam Data Lake is built on proven big data technologies including Elasticsearch and HDFS. The system delivers:

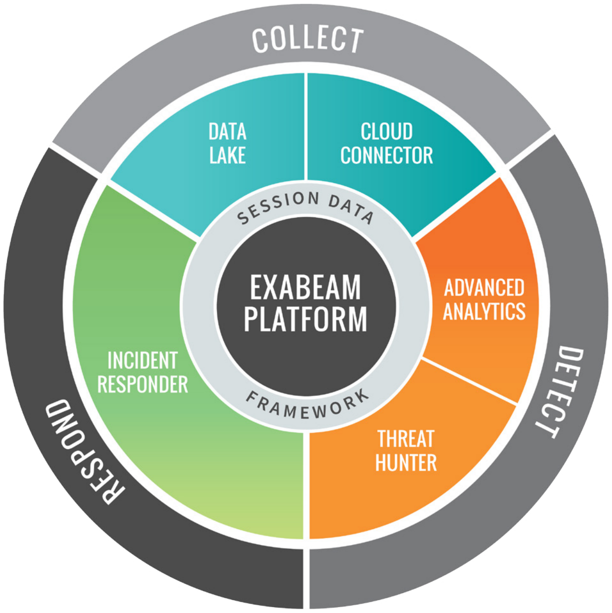
- Web-scale aggregation of log data
- Scale-out multi-node architecture
- Guaranteed at-least-once data delivery
- Search, dashboards and reporting
- Ability to enrich log events with unique security stateful context and Host-To-IP awareness
- Remote Management of agent based collectors, including update and stop/start
- User interface optimized for security analysis and reporting
- Ease of setup and use
- RESTful API
- Out of the box parsers for 750+ security and identity products
- Interoperability with any UEBA system
- Ability to deploy as a pre-sized physical appliances or as a cloud-ready VM

## EXABEAM SECURITY INTELLIGENCE PLATFORM

Exabeam Data Lake is a key component in the Exabeam Security Intelligence Platform. Any of the platform components can be used together or separately with third party products. The platform includes:

- **Exabeam Data Lake**
- **Exabeam Advanced Analytics**
- **Exabeam Threat Hunter**
- **Exabeam Incident Responder**
- **Exabeam Cloud Connectors**

To learn more about these products, please visit www.exabeam.com/products to download whitepapers, datasheets, etc.



## OPERATING INFORMATION

- Deployable as a physical appliance (in multiple sizes) or as a cloud-ready virtual machine
- Includes out of the box collection agents and parsers for over 500 security data sources
- Agents operate on Windows or Linux platforms

**For more information, please contact Exabeam at info@exabeam.com**

# Cortex XSOAR

## Redefining Security Orchestration, Automation, and Response

Security teams lack the people and scalable processes to keep pace with an overwhelming volume of alerts and endless security tasks. Analysts waste time pivoting across consoles for data collection, determining false positives, and performing repetitive, manual tasks throughout the lifecycle of an incident. As they face a growing skills shortage, security leaders deserve more time to make decisions that matter, rather than drown in reactive, piecemeal responses.

## An Industry First

Cortex® XSOAR is the industry's first extended security orchestration and automation platform that simplifies security operations by unifying automation, case management, real-time collaboration, and threat intelligence management. Teams can manage alerts across all sources, standardize processes with playbooks, take action on threat intelligence, and automate response for any security use case.

### Business Benefits

With Cortex XSOAR, your organization will be able to:

- Scale and standardize incident response processes
- Speed up resolution times and boost SOC efficiency
- Improve analyst productivity and enhance team learning
- Gain immediate ROI from existing threat intelligence investments

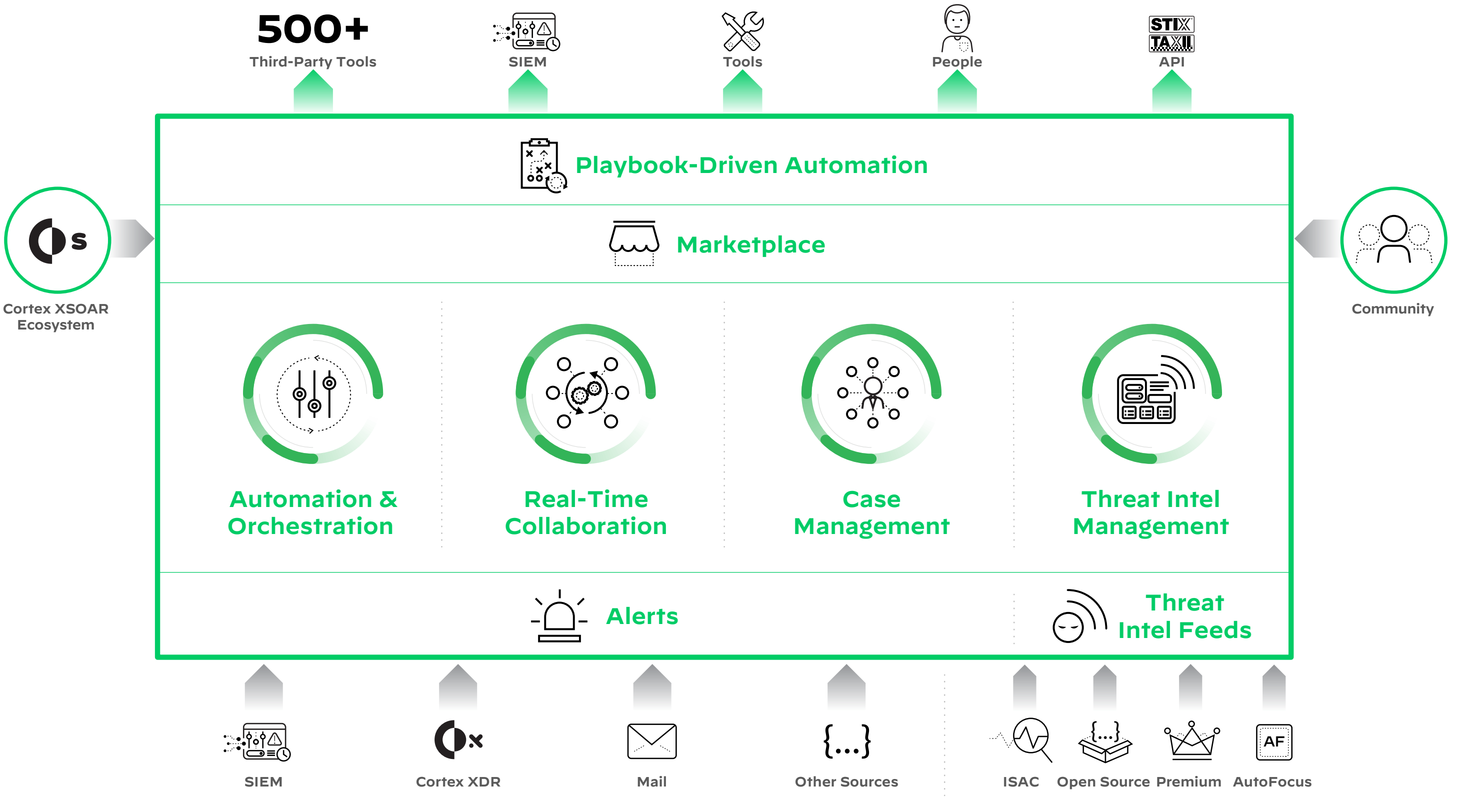


Figure 1: Cortex XSOAR platform

| Table 1: Standardize and Automate Processes for Any Security Use Case | |
|---|---|
| **Scalable, consistent incident response** | Speed up deployment with hundreds of out-of-the-box (OOTB) playbooks covering a wide range of security use cases (e.g., phishing prevention, IOC enrichment, vulnerability management, cloud security). A powerful software development kit allows you to build your own integrations. |
| **Modular, customizable playbooks** | Address simple use cases and complex, custom workflows using a visual drag-and-drop playbook editor with thousands of executable actions. Playbook blocks/tasks can be nested and reused across playbooks. Real-time editing, a playground for testing playbooks, and YAML-based sharing make playbook creation quick and easy. |
| **Perfect balance of automation and human response** | Maintain control over automated processes with manual approval tasks available as part of any playbook. |
| **Orchestration across the product stack** | Automate incident enrichment and response across more than 500 integrations with data enrichment tools, threat intelligence feeds, SIEMs, firewalls, EDRs, sandboxes, forensic tools, messaging systems, and more. |

## Security Orchestration

Cortex XSOAR empowers security professionals to efficiently carry out security operations and incident response by streamlining security processes, connecting disparate security tools, and maintaining the right balance of machine-powered security automation and human intervention.

## Case Management

Automation of incident response needs to be complemented by real-time investigations for complex use cases when human intervention is required. Cortex XSOAR accelerates incident response by unifying alerts, incidents, and indicators from any source on a single platform for lightning-quick search, query, and investigation.

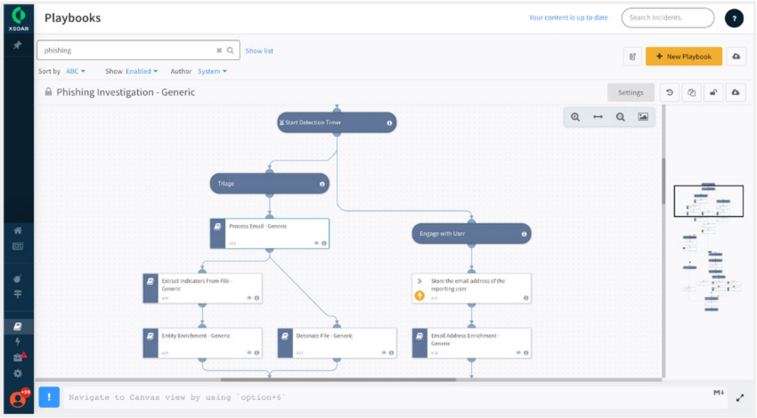
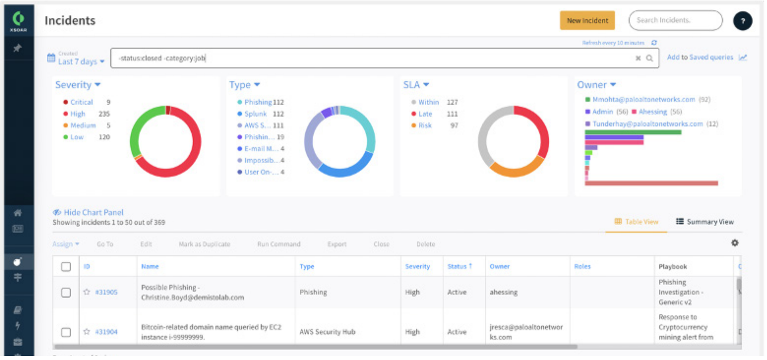

XSOAR
Playbooks
Your content is up to date
Search Incidents.
?
phishing
Show list
New Playbook
Sort by ABC
Show Enabled
Author System
Phishing Investigation - Generic
Settings
Start Detection Timer
Triage
Process Email - Generic
Engage with User
Extract Indicators From File - Generic
Store the email address of the reporting user
Entity Enrichment - Generic
Detonate File - Generic
Email Address Enrichment - Generic
Navigate to Canvas view by using `option+6`
M↓

**Figure 2:** Cortex XSOAR phishing playbook

| Table 2: Adapt to Any Alert with Security-Focused Case Management | |
|---|---|
| **Custom layouts for incidents and indicators** | Fully customizable incident and indicator layouts help you quickly surface relevant information when responding to events. |
| **Indicator and incident correlation** | A central indicator repository enables searches and automated indicator correlation across incidents from multiple sources to spot duplicates, trends, and patterns. |
| **Flexible, customizable reports and dashboards** | Widget-driven dashboards and reports offer unparalleled visibility into metrics so you can cut and dice data for your reporting needs. |
| **On-the-go incident monitoring** | The Cortex XSOAR mobile application provides dashboards, task lists, and incident actions on the go. |
| **Automated mapping across integrations** | Mirrored connections can be created with other applications so  incident updates in Cortex XSOAR will be pushed automatically to third-party applications (ServiceNow, Jira, Slack, etc.) for automated ticketing management. |

## Collaboration and Learning

Cortex XSOAR offers interactive investigation features, providing a potent toolkit to help analysts collaborate, run real-time security commands, and learn from each incident.



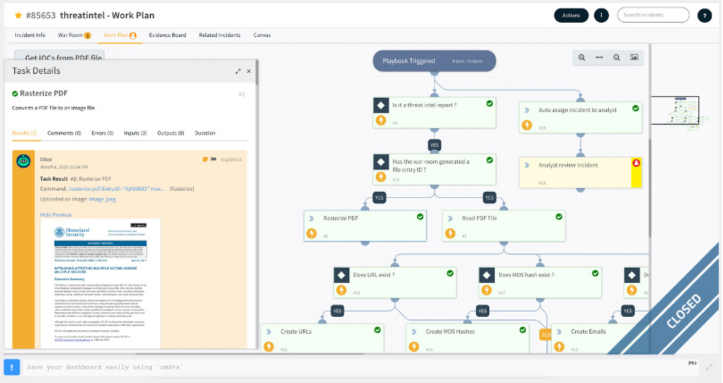
| | ID | Name | Type | Severity | Status | Owner | Roles | Playbook |
|---|---|---|---|---|---|---|---|---|
| □ | ☆ #31905 | Possible Phishing - Christine.Boyd@demistolab.com | Phishing | High | Active | ahessing | | Phishing Investigation - Generic v2 |
| □ | ☆ #31904 | Bitcoin-related domain name queried by EC2 instance i-99999999. | AWS Security Hub | High | Active | jresca@paloaltonetworks.com | | Response to Cryptocurrency mining alert from |

**Figure 3:** Customizable incident views

| Table 3: Boost SecOps Efficiency with Real-Time Collaboration | |
|---|---|
| **Real-time investigation and collaboration** | Each incident has a virtual War Room with built-in ChatOps and command line interface (CLI) so analysts can collaborate and run security actions in real time. |
| **Machine learning assistance** | An ML-driven virtual assistant learns from actions taken in the platform and offers guidance on analyst assignments and commands to execute actions. |
| **Continuous learning** | Auto-documentation of all investigation actions aids analyst learning and development. |
| **Streamlined, automated reporting** | Flexible, widget-driven dashboards and reports eliminate manual reporting and can be fully customized to your organization’s needs. |

## Threat Intelligence Management

Cortex XSOAR takes a new approach with native threat intelligence management, unifying aggregation, scoring, and sharing of threat intelligence with playbook-driven automation.



Task Details

Rasterize PDF #2

Converts a PDF file to an image file.

Results (1) Comments (0) Errors (0) Inputs (3) Outputs (0) Duration

DBot
March 6, 2020 12:56 PM

Task Result #2: Rasterize PDF

Command: !rasterize-pdf EntryID="4@85653" max... (Rasterize)

Uploaded an image: image.jpeg

Hide Preview

Save your dashboard easily using `cmd+s`

**Figure 4:** Intelligence-based automated playbook

| Table 4: Act on Threat Intelligence with Confidence and Speed | |
|---|---|
| **Automated multi-source feed aggregation** | Eliminate manual tasks with automated playbooks to aggregate, parse, deduplicate, and manage millions of daily indicators across dozens of supported sources. |
| **Granular indicator scoring and management** | Take charge of your threat intelligence with playbook-based indicator lifecycle management and transparent scoring that can be extended and customized with ease. |
| **Best-in-class operational efficiency** | Boost collaboration and reveal critical threats by layering third-party threat intelligence with internal incidents to prioritize alerts and make smarter response decisions. |
| **Powerful native threat intelligence** | Supercharge investigations with built-in, high-fidelity threat intelligence from Palo Alto Networks AutoFocus™ contextual threat intelligence service. |
| **Hands-free, automated playbooks with extensible integrations** | Take automated action to shut down threats across more than 500 third-party products with purpose-built playbooks based on proven SOAR capabilities. |

## Breadth of Use Cases

Cortex XSOAR provides an open, extensible platform applicable to a wide range of use cases—even processes outside the purview of the security operations center (SOC) or security incident response team. The flexible platform can be adapted to any use case, with common ones including phishing, security operations, incident alert handling, cloud security orchestration, vulnerability management, and threat hunting.

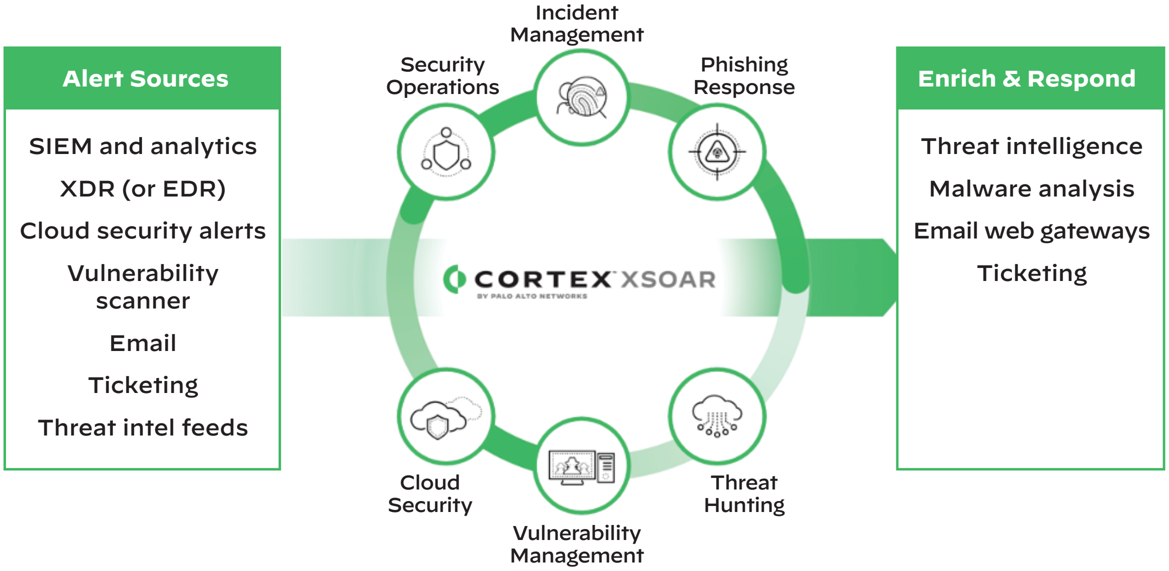
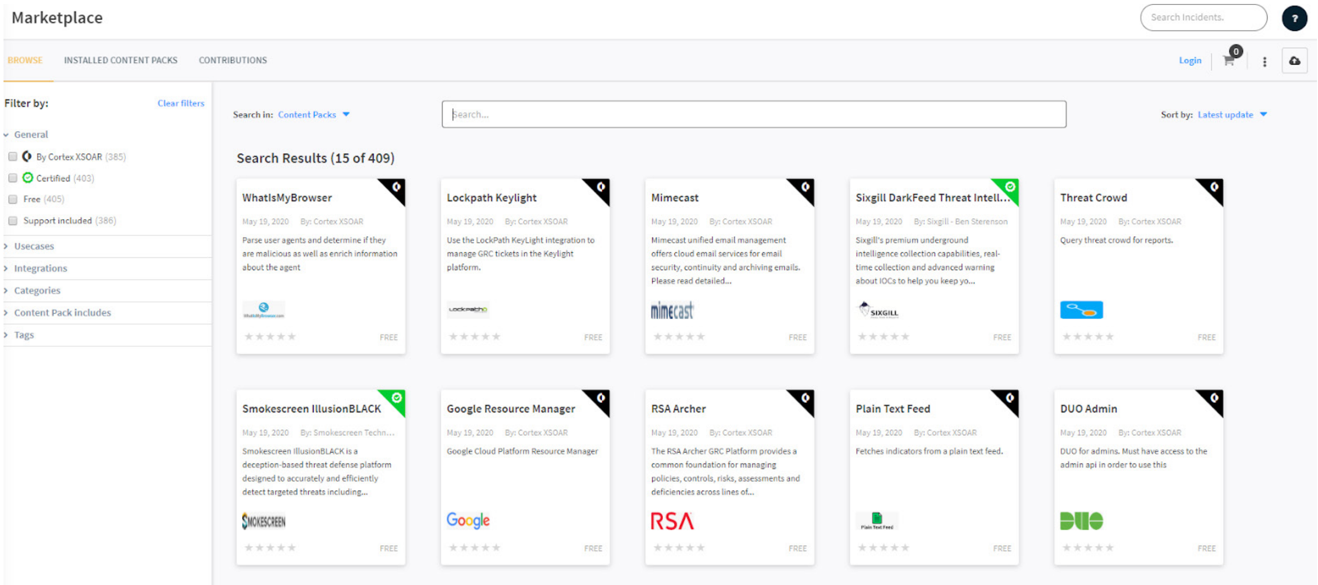


**Figure 5:** Ingestion of alerts and IOCs in Cortex XSOAR

# Cortex XSOAR Marketplace

Cortex XSOAR Marketplace is the industry's most comprehensive security orchestration marketplace. As a native extension of Cortex XSOAR, the Marketplace enables you to discover, share, and consume content packs contributed by the industry's largest SOAR community.

Content packs are pre-built bundles of integrations, playbooks, dashboards, fields, and subscription services designed to address specific security use cases. Packs can be deployed with a single click, simplifying and speeding up the adoption of automation.



Marketplace

Search Incidents.

BROWSE | INSTALLED CONTENT PACKS | CONTRIBUTIONS

Login | 0

Filter by: Clear filters

General
- □ By Cortex XSOAR (385)
- □ Certified (403)
- □ Free (405)
- □ Support included (386)

› Usecases
› Integrations
› Categories
› Content Pack includes
› Tags

Search in: Content Packs

Search...

Sort by: Latest update

Search Results (15 of 409)

**WhatIsMyBrowser**
May 19, 2020 By: Cortex XSOAR
Parse user agents and determine if they are malicious as well as enrich information about the agent
★★★★★ FREE

**Lockpath Keylight**
May 19, 2020 By: Cortex XSOAR
Use the LockPath KeyLight integration to manage GRC tickets in the Keylight platform.
★★★★★ FREE

**Mimecast**
May 19, 2020 By: Cortex XSOAR
Mimecast unified email management offers cloud email services for email security, continuity and archiving emails. Please read detailed...
★★★★★ FREE

**Sixgill DarkFeed Threat Intell...**
May 19, 2020 By: Sixgill - Ben Sterenson
Sixgill's premium underground intelligence collection capabilities, real-time collection and advanced warning about IOCs to help you keep yo...
★★★★★ FREE

**Threat Crowd**
May 19, 2020 By: Cortex XSOAR
Query threat crowd for reports.
★★★★★ FREE

**Smokescreen IllusionBLACK**
May 19, 2020 By: Smokescreen Techn...
Smokescreen IllusionBLACK is a deception-based threat defense platform designed to accurately and efficiently detect targeted threats including...
★★★★★ FREE

**Google Resource Manager**
May 19, 2020 By: Cortex XSOAR
Google Cloud Platform Resource Manager
★★★★★ FREE

**RSA Archer**
May 19, 2020 By: Cortex XSOAR
The RSA Archer GRC Platform provides a common foundation for managing policies, controls, risks, assessments and deficiencies across lines of...
★★★★★ FREE

**Plain Text Feed**
May 19, 2020 By: Cortex XSOAR
Fetches indicators from a plain text feed.
★★★★★ FREE

**DUO Admin**
May 19, 2020 By: Cortex XSOAR
DUO for admins. Must have access to the admin api in order to use this
★★★★★ FREE

**Figure 6:** Highly rated, validated content to discover

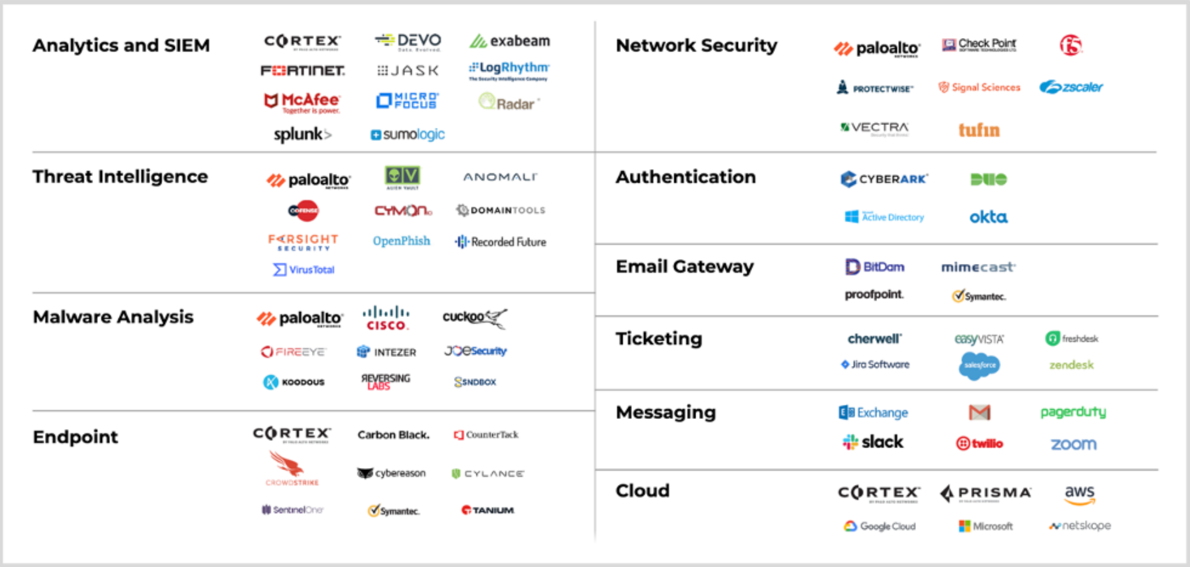
## Breadth of Integrations

Cortex XSOAR has the industry's most extensive and in-depth OOTB integrations with security and non-security tools used by security teams. New integrations and content packs are continuously added to the Cortex XSOAR Marketplace to facilitate quick and seamless deployments for our customers.

### Benefits of Our Extensive Integration Ecosystem

- Promote your platform and solution offerings
- Develop a strategic partnership with Palo Alto Networks
- Take advantage of co-marketing activities and lead generation
- Gain brand recognition in the security industry

Join the Marketplace today.



| | |
|---|---|
| Analytics and SIEM | CORTEX, DEVO, exabeam, FORTINET, JASK, LogRhythm, McAfee, MICRO FOCUS, Radar, splunk, sumologic |
| Threat Intelligence | paloalto, ANOMALI, CYMON, DOMAINTOOLS, FARSIGHT SECURITY, OpenPhish, Recorded Future, VirusTotal |
| Malware Analysis | paloalto, CISCO, cuckoo, FIREEYE, INTEZER, JOESecurity, KOODOUS, REVERSING LABS, SNDBOX |
| Endpoint | CORTEX, Carbon Black, CounterTack, CROWDSTRIKE, cybereason, CYLANCE, SentinelOne, Symantec, TANIUM |
| Network Security | paloalto, Check Point, F5, PROTECTWISE, Signal Sciences, zscaler, VECTRA, tufin |
| Authentication | CYBERARK, DUO, Active Directory, okta |
| Email Gateway | BitDam, mimecast, proofpoint, Symantec |
| Ticketing | cherwell, easyVISTA, freshdesk, Jira Software, salesforce, zendesk |
| Messaging | Exchange, pagerduty, slack, twilio, zoom |
| Cloud | CORTEX, PRISMA, aws, Google Cloud, Microsoft, netskope |

**Figure 7:** Some of our 500+ OOTB integrations

## Industry-Leading Customer Success

Our Customer Success team is dedicated to helping you continuously optimize your security posture and get the most out of your Cortex XSOAR implementation.

**Standard Success**, included with every Cortex XSOAR subscription, makes it easy for you to get started. You'll have access to self-guided materials and online support tools to get you up and running quickly.

**Premium Success**, the recommended plan, includes everything in the Standard plan plus guided onboarding, custom workshops, 24/7 technical phone support, and access to the Customer Success team to give you a personalized experience to help you realize optimal return on investment (ROI).

| | | Standard | Premium |
|---|---|---|---|
| | Summary Value | Self-Help | Optimized Experience |
| Onboarding Assistance | Customer journey kickoff | ● | ● |
| | Onboarding assistance | | ● |
| | Initial service configuration | | ● |
| | Use case assistance | | ● |
| Technical Support | Access to support community | ● | ● |
| | Access to Support Portal | ● | ● |
| | Telephone support | | 24/7 |
| | Response time (S1) | | < 1 hour |
| | Slack DFIR private channel | | ● |
| Education Training | Access to online documentation | ● | ● |
| | Access to online training | ● | ● |
| | Custom workshop | | ● |
| Optimized Experience | Annual health check | ● | ● |
| | Customized success plans | | ● |
| | Periodic operation reviews | | ● |
| | Executive business reviews | | ● |
| | Prioritized integration development | | ● |

**Figure 8:** Key aspects of Standard and Premium Customer Success plans

### Cortex XSOAR Community Edition

To experience the capabilities of Cortex XSOAR, try the free Community Edition. With its included 30-day enterprise license, it's the perfect way to test-drive Cortex XSOAR.

Sign up for our free Community Edition.

## Cortex XSOAR Mobile App

Use Cortex XSOAR to track and respond to security incidents on the go with a mobile-first experience for iOS and Android®. Create and access personalized dashboards, assign and complete tasks from any device, and improve investigation quality by working together.

Get the app from the App Store® and Google Play®.

## Designed for MSSPs

Cortex XSOAR supports full multitenancy with data segmentation and scalable architecture for managed security service providers (MSSPs). MSSPs can build their managed service operations on Cortex XSOAR to provide best-in-class offerings for their customers and optimize internal team productivity.

**Table 5: The Connective Fabric for Your Security Infrastructure and Teams**

| Feature | Value |
|---|---|
| **True multitenancy** | MSSPs can create playbooks and enforce policy at both the master and tenant levels for high availability, creating flexibility to quickly onboard new customers, offer different levels of service, and expand into additional management options. |
| **Modular playbooks** | MSSPs can also build custom playbooks for specific services and service levels. Inside each playbook, tool actions can be simply "copied" and reused in other playbooks at both the master and tenant levels for efficient scaling with new customer additions. |
| **SLA and team performance tracking** | Cortex XSOAR features built-in SLA tracking capabilities to help MSSPs guarantee timely service outcomes to their customers. An MSSP can trigger a notification—via Slack, email, etc.—to the analyst team to handle a timely incident before an SLA breach. |

**Table 5: The Connective Fabric for Your Security Infrastructure and Teams (continued)**

| Feature | Value |
|---|---|
| Extensive APIs | MSSPs can leverage all Cortex XSOAR capabilities as a powerful backend automation and orchestration enabler for their services while maintaining existing customer-facing portals. |
| Threat intelligence management | For MSSPs, adding threat intelligence to any service to increase customer value is vastly simplified. Threat intelligence feeds can be compiled at the master and tenant levels to cater to different customer types and use cases. |

## Flexible Deployment

Cortex XSOAR can be deployed on-premises, in a private cloud, or as a fully hosted solution. We offer the platform in multiple tiers to fit your needs.

## Cortex XSOAR Hosted Solution

With our hosted solution, security teams can improve response times and efficiencies without having to devote dedicated resources for infrastructure, maintenance, and storage. Cortex XSOAR will manage and maintain the infrastructure and platform layer, enabling SOCs to focus on the critical aspects of incident response.

### Benefits of a Hosted Solution

- Reliable, flexible, and scalable technology
- Ironclad security and privacy
- Lower total cost of ownership
- Accelerated, standardized incident response

**Table 6: Cortex XSOAR Server—System Requirements for On-Premises Deployment**

| Component | Minimum | Recommended |
|---|---|---|
| CPU | 8 CPU cores | 16 CPU cores |
| Memory | 16 GB RAM | 32 GB RAM |
| Storage | 500 GB SSD | 1 TB SSD with minimum 3K dedicated IOPS |
| Physical or virtual server | Linux OS: Ubuntu 16.04, 18.04; RHEL 7.x & 8; Oracle Linux 7.x; Amazon Linux 2; CentOS 7.x & 8 | |

**Table 7: Cortex XSOAR Engine—System Requirements for On-Premises Deployment**

| Component | Minimum | Recommended |
|---|---|---|
| CPU | 8 CPU cores | 16 CPU cores |
| Memory | 16 GB RAM | 32 GB RAM |
| Storage | 500 GB SSD | 1 TB SSD with minimum 3K dedicated IOPS |
| Operating system | macOS, Windows, Linux | |

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

CLICO

На вниманието на:<br>
**Г-н Христо Пачев**<br>
**Гл. експерт „Маркетинг”**<br>
**"АЕЦ Козлодуй" ЕАД**

**Относно:** Пазарна консултация за Доставка и изграждане на система за наблюдение, събиране, съхранение и анализ на събития /SIEM/ и автоматизирани инструменти за защита /SOAR/ в информационната система на "АЕЦ Козлодуй" ЕАД, реф. номер 46660

Уважаеми господин Пачев,

Клико България ЕООД в качеството си на оторизиран дистрибутор за продуктите на Exabeam за територията на България, потвърждава, че ТИНК СМАРТ ЕООД с ЕИК 205946661 и адрес София, Младост, бл. 31, вх. 8, ет. 4 е оторизиран партньор на Exabeam и е упълномощен да разпространява и предоставя софтуерна поддръжка на лицензите (Exabeam продукти) на територията на Република България.

ТИНК СМАРТ ЕООД не е упълномощен да се съгласява с каквито и да е общи условия от името на Exabeam и Клико България ЕООД и никакви условия не бива да се прилагат или да са приложими за Exabeam и Клико България. Всички продукти се продават при спазване на условията на лиценз за краен потребител на Exabeam и споразумение за ограничена гаранция.

Заличено на основание ЗЗЛД

20.04.2021 год.<br>
София

С уважение,<br>
Александър Стаменов<br>
Управител<br>
Клико България ЕООД

paloalto NETWORKS

2021-04-20
Attention: Hristo Pachev
NPP Kozloduy EAD
Zone NPP Kozloduy,Kozloduy,Bulgaria,3321

Manufacturer Authorization Letter in Connection with our Authorized Partner Think Smart EOOD **(the 'Partner')** participation in your competitive Tender/ RFP with Reference 46660 / "Delivery and implementation of SIEM and SOAR in the information system of NPP Kozloduy"
**(the 'Tender')**

Dear Sir/Madam:

We, Palo Alto Networks (Netherlands) B.V having an address at Oval Tower, 5th Floor, De Entree 99-197, 1101HE Amsterdam, The Netherlands (**'Palo Alto Networks'**), publish and manufacture certain next generation security of ware and hardware products (the 'Products'), and do hereby authorize our Partner to participate and bid in the above mentioned Tender as at the date of this letter.

In consideration of the above, and whether delivered from Partner or through alternative authorized Palo Alto Networks partner(s) in your territory, we agree to:

a) provide commercially available Palo Alto Networks maintenance and technical support services ordered for the Products as part of a current support agreement;

c) extend, to the extent applicable, our full guarantee and/or warranty; and

e) confirm that the Product(s) quoted by Partner is a current model;

in accordance with Palo Alto Networks then-current terms and conditions, support policies, and processes for commercially available Product(s) available on our public website or at https://support.paloaltonetworks.com.

Please note that the Partner is an independent contractor and has no authority to commit and/or bind Palo Alto Networks or its affiliates in any way. This authorization is valid for the above mentioned Tender/RFP only.

Заличено на основание ЗЗЛД

[redacted]

Omar Durrani
Senior Director of Finance International
Palo Alto Networks (Netherlands) B.V.