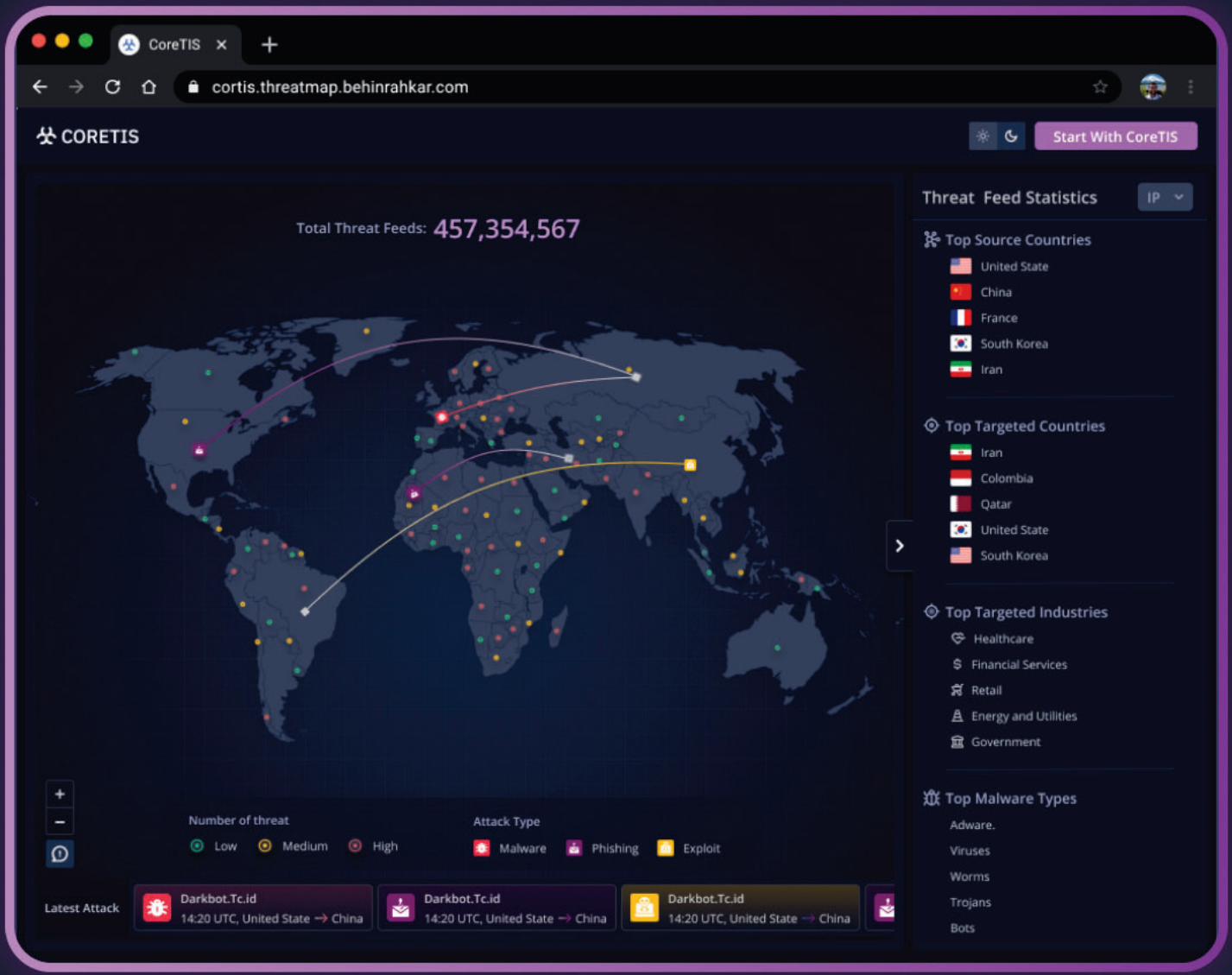
CoreTIS

Threat Intelligence System

سامانه بومی پیشرفته هوش تهدید

روزانه حملات سایبری متنوعی انجام میشود و مهاجمان همواره در حال پیچیده تر و مبهم تر کردن حملات خود هستند و با استفاده از Killchain های پیشرفته و تاکتیک ها و تکنیک های شخصی سازی شده به دنبال مختل کردن کسب و کار شما و یا آسیب رساندن به مشتریان شما میباشند. شناسایی چنین حملات پیشرفته ای، نیازمند راهکاری مدرن و امن مبتنی بر هوش تهدید میباشد. با یکپارچه کردن اطلاعات هوش تهدید که شامل شاخصه‌های مخرب IP, Domain, URL و .. می‌باشند با تجهیزات امنیتی

WWW.BEHINRAHKAR.COM



معرفی سامانه

مقدمه

روزانه حملات سایبری متنوعی انجام میشود و مهاجمان همواره در حال پیچیده تر و مبهم تر کردن حملات خود هستند و با استفاده از Killchain های پیشرفته و تاکتیک ها و تکنیک های شخصی سازی شده به دنبال مختل کردن کسب و کار شما و یا آسیب رساندن به مشتریان شما میباشند. شناسایی چنین حملات پیشرفته ای، نیازمند راهکاری مدرن و امن مبتنی بر هوش تهدید میباشد. با یکپارچه کردن اطلاعات هوش تهدید که شامل شاخصه‌های مخرب IP, Domain, URL و .. می‌باشند با تجهیزات امنیتی خود مانند SIEM, SOAR, Threat Hunting و .. میتوانید سرعت و دقت تیم ها و ابزار های امنیتی خود را به شکل چشم گیری بهبود بخشید. با در دسترس قرار دادن اطلاعات هوش تهدید که همواره آپدیت میشوند، اطلاعات و Context مورد نیاز برای شناسایی حملات را به سادگی و با سرعت در اختیار تیم های امنیتی خود قرار داده و به شکل ProActive تهدیدات را قبل از وقوع آن ها شناسایی نمایید.

چالش‌های پیش روی سازمان‌ها در حوزه هوش تهدید

ردیابی، تحلیل و تفسیر آخرین تهدیدات سایبری ، در بازه های زمانی کم از منابع اطلاعاتی مختلف برای مدیریت مناسب ریسک، همواره یکی از چالش‌های اصلی سازمان‌ها در مواجه با تهدیدات مختلف میباشد.

همچنین تیم‌های امنیت همواره برای اولویت‌بندی و واکنش مناسب به رخدادها نیازمند Context یا اطلاعات زمینه‌ای در خصوص تهدیدات هستند که جمع آوری و بررسی تمام این شواهد به ازای تمامی رخدادها فرآیندی زمان‌بر می‌باشد و ممکن است خیلی از منابع اطلاعاتی مهم مورد بررسی قرار نگیرد.

مزیت‌های کلیدی کورتیس

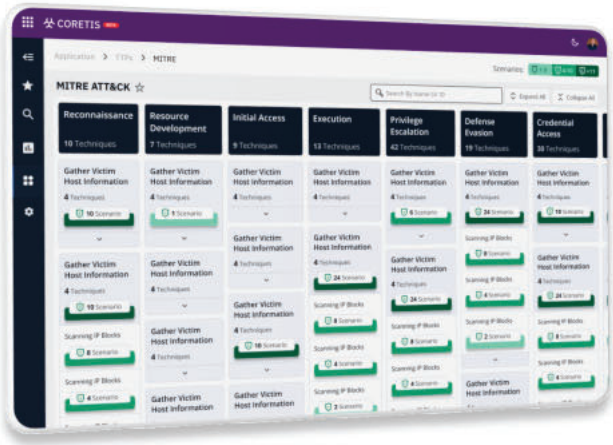
- دریافت اطلاعات زمینه‌ای و Context در خصوص تهدیدات به شکل لحظه‌ای از منابع مختلف
- ارتباط با سایر تجهیزات امنیتی برای جلوگیری موثرتر از تهدیدات
- دریافت شاخصه‌های تهدید در ۷ دسته بندی از بیش از ۱۵۰ منبع مختلف
- شناسایی و اولویت بندی آخرین تهدیدات سایبری

ویـــژگی‌های کلیـدی کـــورتیس

دریافت اعلان آخرین آسیب پذیری و اکسپلویت های منتشر شده

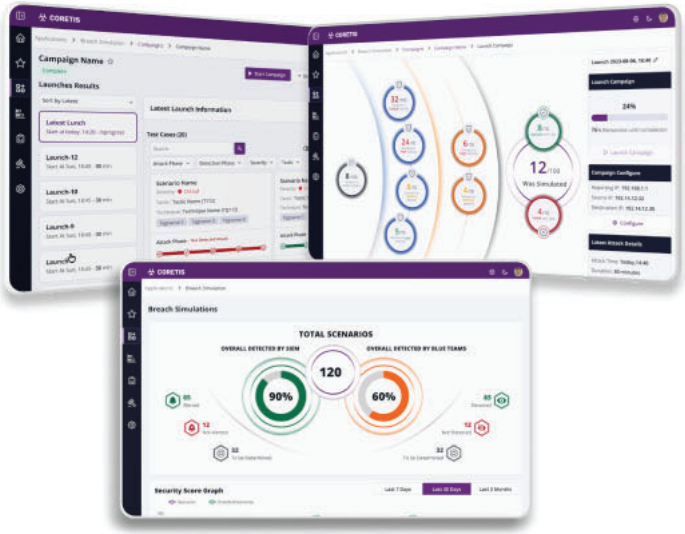
روزانه تعدادی زیادی آسیب پذیری با تنوع بالا منتشر میشود و رصد و بررسی تمامی آن ها فرآیندی زمان بر و سخت میباشد.
به کمک سامانه کورتیس به طور خودکار به آخرین آسیب پذیری ها به همراه اکسپلویت های آن ها دسترسی دارید و میتوانید اطلاعات آن‌ها را مشاهده کنید. همچنین میتوانید لیست دارایی های خود را منطبق بر ساختار استاندار CPE در سامانه وارد کرده و به محض منتشر شدن آسیب پذیری جدید مرتبط با دارایی های خود، اعلان دریافت نمایید.

دسترسی به مخزنی بیش از ۱۸۰۰ سناریو SIEM منطبق بر Mitre ATT&CK



سامانه کورتیس شامل مخزنی بیش از ۱۸۰۰ سناریو SIEM میباشد که به شکل روزانه توسط تیم بنفش بهین راهکار آپدیت و Tune میشوند.
تمام سناریو ها مطابق با فریمورک Mitre ATT&CK با Tactic و Technique های مرتبط با آن ها ایجاد شده اند و راهکار های Mitigation و شناسایی تهدیدات مطابق با این Freamwork برای تمامی UseCase ها در دسترس میباشد

ارزیابی عملکرد SIEM و تیم آبی با شبیه سازی بیش از ۱۸۰۰ حمله SIEM



در سامانه کورتیس علاوه بر دسترسی به مخزنی بیش از ۱۸۰۰ سناریو SIEM، میتوانید به کمک ماژول Breach and Attack Simulation (BAS) ، تمام سناریو هارا بر روی سامانه SIEM خود شبیه سازی نمایید و عملکرد و دقت تشخیص تهدیدات خود را مورد ارزیابی قرار دهید. همچنین میتوانید با شبیه سازی حملات، دقت و سرعت تیم واکنش به رخداد خود را سنجیده و عملکرد آن را مورد ارزیابی قرار دهید.

کورتیس چگونه کار میکند؟

دریافت شاخصه‌ها

ورودی ها:

- بیش از ۱۵۰ فیدر free/commercial شامل:
  Cisco Talos, OpenPhish, VirusTotal, SpamHouse,
  ... ,InfraGaurd, NVD, CrowdStrike Falcon
- هانی پات اختصاصی با سرویس های پرکاربرد (مانند ssh, web, ftp, telnet, ...)
- گزارش فعال کاربران در پروژه های مختلف
- گزارشات انجمن های فعال مهاجمان در Surface Web و Dark Web

خروجی ها:

- IP, Domain, URL, File Hash, UserAgent, SSL Certificate
- CVE, Exploits

اولویت بندی و اختصاص Credibility به هر شاخصه

بعد از فرایند جمع آوری اطلاعات، تمامی شاخصه های استخراج شده با الگوریتم های یادگیری ماشین (Machine Learning) و هوش مصنوعی (Artificial Intteligence) تجزیه و تحلیل میشوند و بر اساس رفتار و ماهیت مخرب آن ها امتیازی از بین ۱ الی ۱۰ به هر شاخصه تخصیص میابد که باعث میشود تیم ها و ابزار های امنیتی تمرکز و زمان خود را روی تهدیداتی که ریسک بالاتری دارند قرار دهند.

اطلاعات زمینه ای و Context جمع آوری شده در خصوص هر Indicator

تمامی افراد تیم آبی و همچنین ابزار های امنیتی، برای کشف تهدیدات نیازمند Context یا اطلاعات زمینه ای در خصوص شاخصه ای که در حال بررسی آن هستند میباشند تا بتوانند به کمک آن به اطلاعات بیشتری دست پیدا کرده و تصمیم قطعی تری در خصوص علت False Positive یا True Positive بودن رخداد ها بگیرند. سامانه کورتیس با دردسترس قرار دادن اطلاعات زیر به شکل Real-Time و آپدیت شده، کیفیت شناسایی تهدیدات تیم ها و ابزار های امنیتی شما را بهبود میبخشد

- گزارش بیش از ۹۰ Engine آنتی ویروس
- گزارش کاربران دنیا در خصوص شاخصه مورد نظر
- دریافت اطلاعات Port Scan به شکل Passive
- اطلاعات هویتی شامل Whois, ...
- بررسی Blacklist ها و تاریخچه

ارسال گزارشات و داشبوردها

بعد از جمع آوری اطلاعات لازم برای شناسایی تهدیدات، سامانه کورتیس به طور خودکار تمامی خروجی ها را در قالب گزارش هایی با فرمت PDF, STIX, IODEF و ... به همراه داشبورد های متنوع در اختیار کاربر قرار میدهد تا بتواند در سریع ترین زمان ممکن به خروجی مدنظر خود دسترسی داشته باشد و همواره دسترسی مناسب تری به چشم انداز تهدیدات به شما ارایه میدهد

کاربـــردهـای عمـــلی Feature ها

KEY BENEFITS

ایجـاد هشـدار و اعلان هـای شـخصی سـازی شـده

دریافت هشدار به شکل بلادرنگ (RealTime) از طریق ایمیل یا sms و .. به همراه راهکار Mitigation از Reference های آسیب پذیری و اولویت بندی مناسب جهت انجام وصله های امنیتی در کمترین زمان با توجه به دارایی های سازمان

شبیـه سـازی حمـــلات از طـریق مـاژول BAS

ارزیابی عملکرد سامانه SIEM (شامل Parsing, Correlation, ..) و تیم واکنش به رخداد (زمان شناسایی آسیب پذیری، تشخیص TP/FP، ...) با شبیه سازی حملات و دریافت خودکار اطلاعات در خصوص SIEM و واکنش تیم آبی

داشبـــورد هـــای تهـــدیـدات و Threat Map

دسترسی به آخرین چشم انداز تهدیدات و حملات فعال و تمرکز بر روی تهدیداتی که مهاجمان به شکل فعال در حال اکسپلویت آن هستند و اولویت بندی مناسب برای مدیریت ریسک و انجام وصله های امنیتی

دسترسی به آخرین اطلاعات زمینه‌ای (Context) در خصوص تهدیدات

افزایش دقت و کیفیت خروجی تیم واکنش به رخداد و کاهش زمان موردنیاز برای بررسی و تحلیل حملات و رخداد های امنیتی به کمک دریافت آنی اطلاعات به شکل تحلیل شده و دسته بندی شده توسط کورتیس و ارایه گزارش فنی و مدیریتی در خصوص شاخصه های مختلف

دسـتـــرسی به مخـــزن UseCase هـــای SIEM

شناسایی آخرین حملات و Tactic ها و Technique های مورد استفاده مهاجمان همراه با Tunning و آپدیت های مستمر و جلوگیری موثر تر در مقابل حملات مختلف مهاجمان

POSITION BENEFITS

SOC

- اولـویت بندی منـاسب تهدیدات برای ارایه پاسخ در زمان مناسب
- کاهـش چشـم گـیر False Positive هـــا
- کاهش زمـان مـورد نیـــاز بـرای بـررسی و تـحلیـل رخـدادها
- خـــودکار ســـازی فـــرآینـــدهای روتیـــن تیـــم های امنیـتی

SEC/IT ANALYST

- بـهبود چشـم‌گیـر در پیشگیری از تـــهدیـدات و شناســایی آن‌ها
- افـزایـــش دقـت و کـیفیـت فـرآیـندهای Threat Hunting

SIEM

- دستـــرســی به مخـــزن جـــامـــعی از UseCase های امنیـتی
- غنـی سـازی اطـــلاعـــات دریـــافت شـــده
- شناسـایی طیف وسیـعی از تهدیدات منطبق بر Mitre ATT&CK

CSIRT

- بهبـــود فـــرآینـــدهـــای Investigation و Prioritization در رخـــدادها
- دستـــرسی به اطلاعـــات تاریخچـه‌ای (Historical) تهـدیدات

اجزا و نیازمندیهای سخت افزاری سامانه

نسخه آفلاین کورتیس بر روی تنها یک سرور پیاده سازی میشود و جدول زیر نیازمندی های سخت افزاری سامانه را به تفکیک Component های مورد استفاده آن نمایش میدهد و سخت افزار مورد نیاز نهایی مجموع نیازمندی های زیر میباشد.

کورتیس OFFLINE

CoreTIS Frontend Requirements	
Component	**CoreTIS Offline**
PROCESSOR	3Core
MEMORY	6GB
STORAGE	25GB
NIC	1GB Ethernet or higher

CoreTIS Backend Requirements	
Component	**CoreTIS Offline**
PROCESSOR	5Core
MEMORY	8GB
STORAGE	50GB
NIC	1GB Ethernet or higher

CoreTIS Database Requirements	
Component	**CoreTIS Offline**
PROCESSOR	5Core
MEMORY	8GB
STORAGE	200GB
NIC	1GB Ethernet or higher

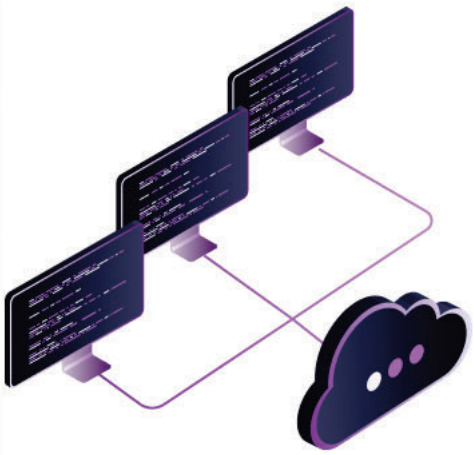
CoreTIS MessageBroker Requirements	
Component	**CoreTIS Offline**
PROCESSOR	3Core
MEMORY	4GB
STORAGE	25GB
NIC	1GB Ethernet or higher

CoreTIS ObjectStore Requirements	
Component	**CoreTIS Offline**
PROCESSOR	3Core
MEMORY	4GB
STORAGE	50GB
NIC	1GB Ethernet or higher

اجزا و نیازمندیهای سخت افزاری سامانه

اجزا و نیازمندیهای سخت افزاری سامانه CoreTIS در بستر Cloud و Offline در جدول زیر نمایش داده میشود.

کورتیس CLOUD



CoreTIS Hardware Requirements	
Component	**CoreTIS Cloud**
PROCESSOR	Provided by vendor in cloud environment
MEMORY	Provided by vendor in cloud environment
STORAGE	Provided by vendor in cloud environment
NIC	Provided by vendor in cloud environment

سطوح خدمات کـــورتیس

سـامانه کورتـیس قابلـیت‌هـای خـود را در سـه سـطح **CoreTIS Repository**، **CoreTIS Cloud** و **CoreTIS Enterprise** ارائـه می دهـد. جـدول ذیل مقایسه دقیـق این سه سطح از خدمات را نشان می دهد:

CoreTIS Cloud

در ایـن لایسنـس کاربر میتواند به مخـزنی بروز از شـاخصه‌هـای امنیـتی در ۷ دسته‌بندی مختـلف (شـــامـل: IP, Domain, URL, File Hash, UserAgent, Email, SSL Certificate Hash)، آخـرین آسیـب پذیری ها، آخـرین اکسپلویت ها و همچنیـن به بـروزترین مخزن UseCase های SIEM مبتنـی بـر Mitre ATT&CK دستـرسی داشته باشـد.

در این نوع لایسنـس ویژگـی های مرتبط با مـاژول Breach and Attack Simulation (BAS) غیـرفعال میباشد.

در ایـن نـوع لایسنس امـکان دریافت Context در خصوص تهدیدات به شکل Real-Time وجود داشته و امکان استفاده از گزارشات و داشبورد های لحظه ای دردسترس میباشد.

این نوع لایسنس با توجه به نیازمندی های سازمان و تعداد درخواسـت های ارسال شده به سمت سامانه هـوش تهدید به ۳ دسته بندی مقابل تقسیم میشود

- **Gold**
- **Silver**
- **Boronz**

CoreTIS Repository

در ایـن لایسنـس کاربر میتواند به مخـزنی بروز از شـاخصه‌هـای امنیـتی در ۷ دسته‌بندی مختـلف (شـــامـل: IP, Domain, URL, File Hash, UserAgent, Email, SSL Certificate Hash)، آخـرین آسیـب پذیری ها، آخـرین اکسپلویت ها و همچنیـن به بـروزترین مخزن UseCase های SIEM مبتنـی بـر Mitre ATT&CK دستـرسی داشته باشـد.

در ایـن نوع لایسنـس به دلیل عـدم ارتبـاط با سرویس‌های Cloud امـکان استفاده از ویژگی‌های Threat Hunting سامانه وجـود ندارد و همچنین ویژگـی‌های مـرتبط با Breach and Attack Simulation (BAS) نیـز در ایـن لایسنـس غیرفعـال میباشد.

در این نوع لایسنس تمـامی ویژگی های سامانه به غیـر از ویژگـی های Threat Hunting و Breach and Attack Simulation (BAS) در دستـرس قـرار دارد.

- **Access to CoreTIS Cloud (Gold)**
- **Repository Updates**

CoreTIS Enterprise

در ایـن لایـسنـس امـکان استـفاده از **تمـامی ویـژگی‌های سـامانه** شـامل مـخزن شاخصه‌ها و آسیب پذیری‌های امنیتی، ویژگی‌های Threat Hunting و مـاژول Breach and Attack Simulation (BAS) در دستـرس می‌باشد. برای استفاده از ویژگی های Threat Hunting لازم است تا امکان دسترسی به coretis.behinrahkar.com روی بستـر اینتـرنت فـراهم باشد.

در ایـن نوع لایسنس **تمـامی ویژگی‌های سامانه** در دسترس کاربـر قـرار میگیرد. در صورتی که امکان برقـرار دستـرسی به سـرویـس‌های Cloud بهین راهـکار برای تمـامی Client ها برقرار نباشد، تمامی آپدیت‌ها میتـواند از طریق یک سـرویس به نام CoreTIS Proxy (به شـکل On-Promise) دریافت شود.

- **Access to CoreTIS Cloud (Gold)**
- **On-Premises Service**
  (Indicator + Repository + BAS)

پیـشنیـاز راه انـدازی لایسنـس

CoreLog

پیـشنیـاز راه انـدازی لایسنـس

CoreLog CoreUCM

فهـــرست قابلیت‌های کـــورتیس

سـامانه کورتـیس قابلـیت‌هـای خـود را در سـه سـطح **CoreTIS Repository**، **CoreTIS Cloud** و **CoreTIS Enterprise** ارائـه می دهـد. جـدول ذیل مقایسه دقیـق این سه سطح از خدمات را نشان می دهد:

فهـرست قـابلیـت‌هـا	CoreTIS Cloud (Indicator per day) یکـسـاله			CoreTIS Repository یکـساله	CoreTIS Enterprise یکـساله
	طرح بـرنـز	طرح نقـره ای	طـرح طـلایی		
مـاژول‌های تـحلـیـلـی					
اسکـن تـوسط آنتـی ویـروس	۲۰ / روز	۵۰ / روز	۱۲۰ / روز	–	۱۲۰ / روز
تـحلیـل Dynamic فایـل هـا	۲۰ / روز	۵۰ / روز	۱۲۰ / روز	–	۱۲۰ / روز
تحلیـل گـزارشات abuse کاربـران	۲۰ / روز	۵۰ / روز	۱۲۰ / روز	–	۱۲۰ / روز
مـاژول‌هـای آنـالیـز ایـمیـل	۱۵ / روز	۳۰ / روز	۴۵ / روز	–	۴۵ / روز
تحلیـل تـوسـط OTX	۲۰ / روز	۵۰ / روز	۱۲۰ / روز	–	۱۲۰ / روز
تحلیـل گـراف شاخصـه‌های تهـدید	۵ / روز	۱۵ / روز	۳۵ / روز	–	۳۵ / روز
تحلیـل خـروجی IP Blocklist هـا	۲۰ / روز	۵۰ / روز	۱۲۰ / روز	–	۱۲۰ / روز
تحلیـل شـاخصه‌هـای UserAgent	۳۰ / روز	۶۰ / روز	۱۲۰ / روز	–	۱۲۰ / روز
تحلیـل رفتـاری URL هـا	۳۰ / روز	۶۰ / روز	۱۲۰ / روز	–	۱۲۰ / روز
تحلیـل پـورت اسکـن شـاخصه‌هـا	۱۰ / روز	۳۰ / روز	۵۰ / روز	–	۵۰ / روز
دریـافت خـروجی Whois	۳۰ / روز	۶۰ / روز	۱۲۰ / روز	–	۱۲۰ / روز
دریـافت اطلاعـات SSL Certificate SHA-۱	۳۰ / روز	۶۰ / روز	۱۲۰ / روز	–	۱۲۰ / روز
دریـافت خروجـی SSL Certificate Scan	۳۰ / روز	۶۰ / روز	۱۲۰ / روز	–	۱۲۰ / روز
شـاخصـه‌های تـهدیـد					
جسـت و جـوی شـاخصه‌ها به شکـل Bulk	۲۰۰ / روز	۵۰۰ / روز	۸۰۰ / روز	–	۸۰۰ / روز
جست و جوی شـاخصه‌هـای تهـدید در سامانه	نامحدود	نامحدود	نامحدود	–	نامحدود
دریافت خـروجی و Export از شـاخصه‌هـا	نامحدود	نامحدود	نامحدود	–	نامحدود
دسـتـرسی به لیـست شـاخصه‌هـا	نامحدود	نامحدود	نامحدود	نامحدود	نامحدود
دسـتـرسی به آخـرین آسیـب پـذیری‌هـای منتشـر شـده	نامحدود	نامحدود	نامحدود	نامحدود	نامحدود
دسـتـرسی به آخـرین اکـسپـلویـت هـای منتشـر شـده	نامحدود	نامحدود	نامحدود	نامحدود	نامحدود
دریـافت اعـلان آسیـب پـــذیری‌هـا	۷ اعلان	۱۵ اعلان	۴۵ اعلان	–	۴۵ اعلان

ادامه فهـــرست قابلیت‌های کـــورتیس

فهـــرست قـــابلیـت‌هـــا	CoreTIS Cloud (Indicator per day) یکـــســـاله			CoreTIS Repository یکـساله	CoreTIS Enterprise یکـساله
	طرح بـرنـــز	طرح نقـره ای	طرح طـلایی		
شبیـــه ســـازی حمـــلات (BAS)					
ایجـاد و مدیـــریـت Campaign هـا	-	-	-	-	نامحدود
شبیـــه ســازی حمـــلات	-	-	-	-	نامحدود
دریـــافت خـــروجی Whois	۳۰ / روز	۶۰ / روز	۱۲۰ / روز	-	۱۲۰ / روز
فعـــالیـــت کاربـــــران					
دستـــرسی به گـــزارشات کاربـــران	نامحدود	نامحدود	نامحدود	-	نامحدود
ثبـــت گـــزارش	نامحدود	نامحدود	نامحدود	-	نامحدود
ثبـــت رای و Vote	نامحدود	نامحدود	نامحدود	-	نامحدود
داشبـــوردهـــا					
داشبـــوردهـــای Honeypot Activity	نامحدود	نامحدود	نامحدود	-	نامحدود
داشبـــوردهـــای CVE	نامحدود	نامحدود	نامحدود	-	نامحدود
داشبـــوردهـــای اطلاعـات شـاخصه های تهدید	نامحدود	نامحدود	نامحدود	-	نامحدود
داشبـــوردهـــای اطلاعـات شـاخصه‌های IPv۴	نامحدود	نامحدود	نامحدود	-	نامحدود
داشبـــوردهـــای Mitre Att&ck	نامحدود	نامحدود	نامحدود	-	نامحدود
داشبـــوردهـــای تـــحلیـــل تهـــدیـــدات (Threat Activity)	نامحدود	نامحدود	نامحدود	-	نامحدود
داشبـــوردهـــای تـــحلیـــل فعـــالیت کاربـــران (User Activity)	نامحدود	نامحدود	نامحدود	-	نامحدود
داشبـــوردهـــای Threat Statistics	نامحدود	نامحدود	نامحدود	-	نامحدود
سـایر ماژول‌ها					
ATT&CK Matrix	نامحدود	نامحدود	نامحدود	-	نامحدود
دستـــرسی به دیتـــای Mitre Att&ck	نامحدود	نامحدود	نامحدود	نامحدود	نامحدود
دستـــرسی به مخـــزن SIEM Usecase	نامحدود	نامحدود	نامحدود	نامحدود	نامحدود

خدمات پشتیبانی

با استفاده از خدمات پشتیبانی کورتیس می‌توانید در کم‌ترین زمان به متخصصین پشتبانی فنی دسترسی داشته باشید و با هزینه‌ای مقرون به‌صرفه بسیاری از چالش‌های کاربری و فنی خود را برطرف کنید.

خدمات	پایه	پیشرفته
پشتیبانی ریموت	✓	✓
پشتیبانی از طریق تیکت	✓	✓
پشتیبانی در زمان اداری (۸X۵)	✓	✓
دسترسی به پایگاه دانش (KB)	✓	✓
پشتیبانی جهت رفع باگ (مطابق SLA)	✓	✓
تولید/بهینه سازی پارسر		✓
تولید داشبورد/ریپورت/پالیسی شخصی سازی شده (مطابق SLA)		✓
ایجاد macro شخصی سازی شده		✓

پشتیبانی پایه

این سطح پشتیبانی، بصورت پیشفرض در فروش تمامی محصولات لحاظ میشود و صرفاً در قبال وجود باگ‌های احتمالی روی سامانه، ارائه میشود. در پشتیبانی پایه ارائه سایر خدمات پس از فروش نظیر توسعه آداپتور جدید، تدوین داشبورد، ریپورت یا پالیسی های شخصی سازی شده و... مستلزم محاسبه نفر/ساعت و پرداخت هزینه نیز میباشد.

پشتیبانی پیشرفته

این سطح پشتیبانی علاوه بر رفع مشکلات سیستمی (مطابق SLAهای پشتیبانی پایه)، شامل برخی خدمات پشتیبانی شخصی سازی شده میباشد.

کورتیس
یک قدم جلوتر از مهاجمان!

در مسیر امنیت در هر قدم کنار شما هستیم.

۰۲۱-۴۱۸۷۸۰۰۰

info@behinrahkar.com

https://behinrahkar.com/coretis

تهران خیابان کریمخان زند، خیابان استاد نجات الهی (ویلا)، کوچه رضا مقدسی (بیمه)، پلاک ۲۴