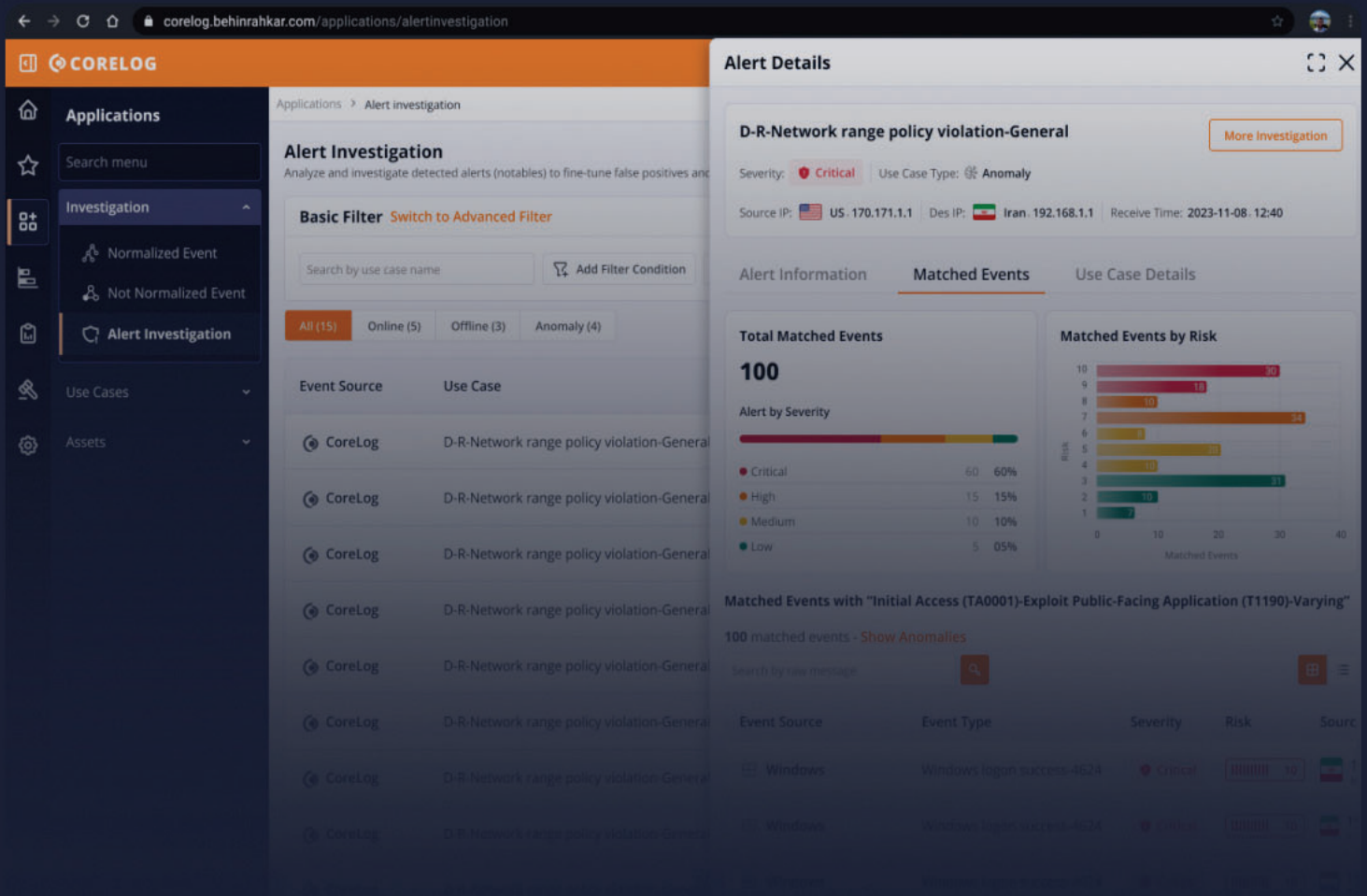
Core Log

AI-Powered Next Gen SIEM

سامانه بومی مدیریت اطلاعات و رویدادهای امنیتی

سامانه کورلاگ با بهره‌گیری از الگوریتم‌های هوش مصنوعی و یادگیری ماشین، یک پلتفرم پیشرفته جهت شناسایی، انطباق و مدیریت حوادث امنیتی از طریق جمع آوری و تجزیه و تحلیل رویدادهای امنیتی می‌باشد. این سامانه با ارائه دید جامعی از وضعیت امنیتی سازمان، به تشخیص، تحلیل و پاسخ به تهدیدات امنیتی قبل از آسیب به کسب و کار آن‌ها کمک می‌کند.

WWW.BEHINRAHKAR.COM



معـــرفی ســـامـانه

مقـدمـه

یکی از سامانه‌های حیاتی در زمینه امنیت فنـــاوری اطلاعات، ســامانه SIEM است که شـــرکت بهین راهکار با نام تجاری کورلاگ تولید و توسعه داده است. این سامانه با جمع آوری داده‌های Log و Flow ترافیک از دارایی های سایبری شبکه در یک نقطه مرکزی و تجزیه و تحلیل داده ها با بهره گیری از موتورهای همبستگی پیشرفته، اقدام به شناسایی تهدیدات و حملات سایبری داخلی و خارجی میکند و دید جامعی از وضعیت امنیتی سازمان جهت پاسخ سریع به رخدادهای امنیتی ارائه میدهد. ســامانه کورلاگ در نسخـــه خود به عنـــوان SIEM نسل بعدی با هـــوش مصنـــوعی (AI-powered Next Gen SIEM) شناخته میشود.

این نسخه با استفاده از الگوریتم‌های یادگیری ماشینی و تحلیل داده ها، قادر به تشخیص الگوهای غیرعادی و حملات پیچیده است که به طور سنتی ممکن است توسط ابزارهای امنیتی دیگر نادیده گرفته شوند. با بهره گیری از هوش مصنوعی، کورلاگ میتواند به طور خودکار تهدیدات را اولویت‌بندی کرده و به تیم‌های امنیتی کمک کند تا به سرعت و با دقت بیشتری به رخدادهای امنیتی واکنش نشان دهند. همچنین، این سامانه قابلیت یادگیری مداوم از رخدادهای جدید و بهبود کارایی خود را دارد، که این امر باعث میشود تا همیشه به روز و موثر باقی بماند.

مـــزایـــای کـــلیدی کـورلاگ

تـولیـــد کامـــلا بـومی تمـــام اجـــزای ســـامـــانه

+ 1800 Use-Case

امـنیتـی پیـــش‌فرض مبتنـــی بـــر MITRE ATT&CK

+ 250 Parser

بـــرای مولـــدهای لاگ‌هـــای بـــومی و خـــارجـی

۱ تشخیـــص بـــلادرنـــگ تهـــدیـدات

۲ ارائـــه دیـــد جـــامـع نسبـــت به تهـــدیـدات ســایبـری

۳ شکـار تهـــدیدات و ارائـــه نقشـــه راه اســتراتژیـک بـر اسـاس MITRE ATT&CK

۴ قـــابـلیـــت ایـجـــاد داشبـــوردهـــا، گـــزارشـــات و Use-Case های شخصـــی ســازی شـــده

۵ تـجزیه و تـــحلیل رفتـــار کاربـران جهـت تشـخیـص تهـــدیدات داخلـــی و ناشنـــاختـــه

۶ کاهـــش میـــانگـــیـن زمـان تـــشخیـــص و پـــاسخ به تهـــدیـــدات (MTTD, MTTR)

۷ ارائـه API جهـت یکپـــارچـــه ســـازی با ســـایر محصـــولات امنیتی

۸ پـــشتیبـــانی مستـــمر توسـط کارشنـاســان متخـصص

ویژگی‌های کلیدی کورلاگ

۱ جمع آوری و مدیریت لاگ‌ها

پشتیبانی از پروتکل‌های Jflow، Sflow، Netflow، Syslog، IPFIX، Database ODBC Connector جهت جمع‌آوری و تجمیع لاگ‌ها از مولدهای مختلف (دستگاه‌های شبکه، سرورها، برنامه‌ها و غیره).

۲ تجزیه، تحلیل و غنی سازی لاگ‌ها

پشتیبانی بیش از ۲۵۰ پارسر پیش‌فرض در سامانه جهت تجزیه، تحلیل و غنی سازی لاگ‌ها بصورت Real-Time مبتنی بر سامانه هوش تهدید CoreTIS و سامانه مدیریت دارایی CoreInspect

۳ تشخیص خودکار ناهنجاری‌های رفتاری

توانایی تشخیص و شناسایی خودکار الگوهای ناشناخته و تهدیدات امنیتی با استفاده از الگوریتم‌های هوش مصنوعی و یادگیری ماشین

۴ تجزیه و تحلیل امنیتی و همبستگی

اعمال فرایند همبستگی بین لاگ ها به‌صورت Real-Time و مبتنی بر موتور تجزیه و تحلیل پیشرفته جهت شناسایی رخدادهای امنیتی

۵ بانک غنی Use-Caseهای امنیتی

ارائه بیش از ۱۸۰۰ سناریو امنیتی پیش‌فرض منطبق با فریم ورک MITRE ATT&CK و قابلیت بروزرسانی از طریق سامانه CoreTIS

۶ مدیریت حوادث امنیت سایبری

قابلیت انطباق با سامانه CoreUCM جهت مدیریت حوادث امنیت سایبری

۷ محتوای امنیتی مبتنی بر فرایندهای Purple Teaming

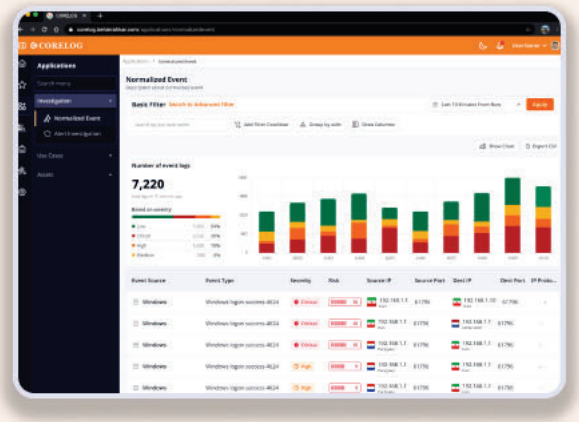
تولید و بروزرسانی Use-Case امنیت سایبری توسط تیم متخصص بنفش (Purple Team) شرکت بهین راهکار و مبتنی بر ابزارهای Gap Analysis نظیر VECTR و پوشش ۷۰% تاکتیک ها و تکنیک های MITRE ATT&CK

۸ داشبورد و گزارشات

ارائه داشبوردها و گزارشات پیشرفته جهت نمایش داده‌های مهم امنیتی، شاخصهای کلیدی عملکرد (KPIs) و اطلاعات تحلیلی برای کمک به تصمیم گیری استراتژیک در زمینه امنیت سایبری

۹ انطباق پذیری با سایر محصولات امنیتی

ارایه API جهت انطباق با ابزارهای امنیتی (نظیر UTM, Firewall و ...)

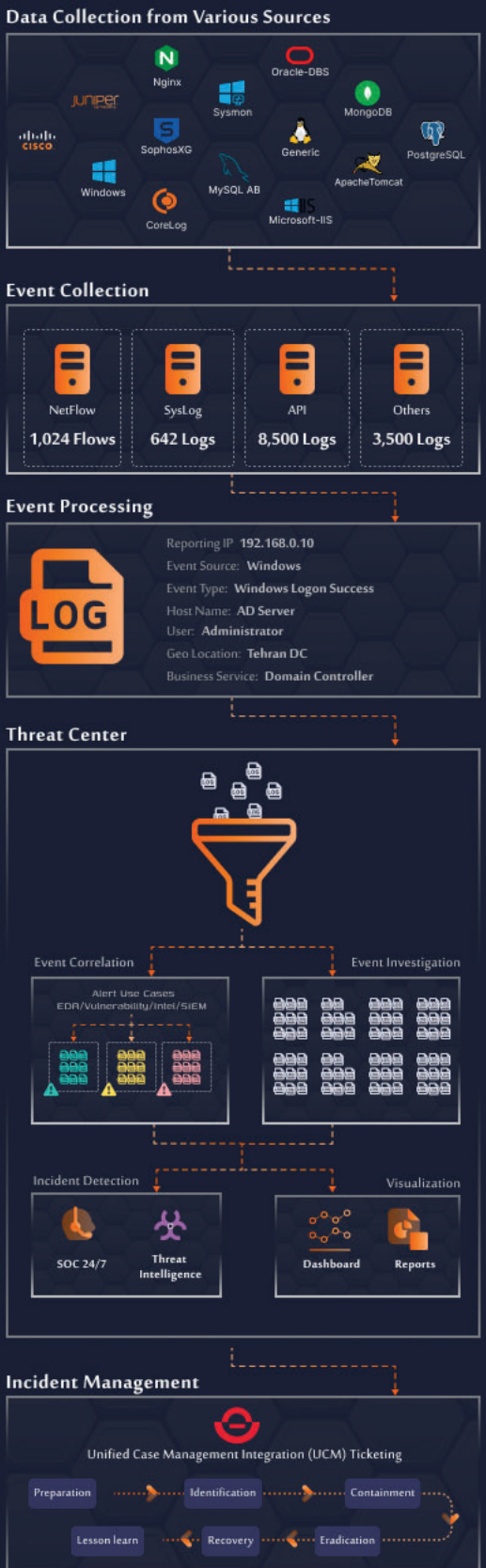


کورلاگ، هوش متمرکز شناسایی حوادث امنیتی سایبری

درخواست دمو

کورلاگ چگونه کار میکند؟

Powered by: **Artificial Intelligence | Advanced Correlation | Threat Intelligence**



ارسال لاگ از دارایی های سایبری سازمان

بر مبنای اهداف سازمان و دامنه دارایی های سایبری تحت پوشش مرکز عملیات امنیت (SOC)، اقدام به پیکربندی مولدهای داده جهت ارسال لاگ یا ترافیک شبکه آنها به کورلاگ میگردد.

جمع آوری و نظارت بر لاگ‌های دریافت شده

اولین و مهمترین مرحله در جریان کاری سامانه‌های SIEM جمع آوری لاگ می‌باشد. سامانه کورلاگ از طریق روش‌های Agent-Based و Agent-Less و مبتنی بر نیازمندی‌های امنیتی، لاگ دارایی‌های سایبری مختلف در شبکه را جهت پردازش جمع‌آوری میکند.

تجزیه، تحلیل، نرمال سازی، غنی سازی و دسته بندی لاگ‌ها

سامانه کورلاگ با تجزیه و تحلیل، نرمال‌سازی، غنی‌سازی و دسته بندی لاگ‌ها، اطلاعات جامع و قابل فهم از لاگ های خام دریافت شده، ایجاد می‌کند. این اقدامات، افزایش دقت و کارایی سامانه و همچنین تشخیص بلادرنگ و پاسخ به حوادث امنیت سایبری را میسر می سازد.

تجزیه و تحلیل و نظارت بر تهدیدات و مقابله با آن‌ها

در این مرحله، کورلاگ با تحلیل همبستگی بین لاگ ها نسبت به شناسایی حملات و ناهنجاری های رفتاری اقدام کرده و از این اطلاعات برای تشخیص الگوهای ناهنجار و افزایش دقت در تشخیص تهدیدات امنیتی استفاده می کند. همچنین در این مرحله امکان جستجو بر روی رویدادها و هشدارهای امنیتی شناسایی شده به همراه قابلیت مشاهده و ایجاد داشبوردها و گزارشات امنیتی در اختیار کاربر قرار داده شده است.

انطباق با سامانه CoreUCM

پس از ثبت هشدارهای امنیتی شناسایی شده، امکان ارسال آنها در قالب تیکت به سامانه رسیدگی به حوادث امنیت سایبری (CoreUCM) فراهم میگردد.

اجزاء و نیازمندیهای سخت افزاری سامانه

سامانه کورلاگ از اجزا (کامپوننت‌های) مختلفی تشکیل شده که هر کدام نیازمندی‌های سخت افزاری متفاوتی بر اساس میزان EPS و زمان نگهداری لاگ‌ها نیاز دارند. این اجزاء از طریق زیرساخت مجازی، قابل پیاده سازی هستند.

در جدول زیر این اجزاء و نیازمندی‌های آن‌ها بر اساس مدت زمان نگهداری لاگ (Log Retention) **یک ماهه** مشخص شده اند، در صورتی که مدت زمان نگهداری لاگ‌ها بیشتر از یک ماه باشد منابع سخت افزاری مورد نیاز تحت تاثیر قرار خواهند گرفت.

For 1,000 EPS

Component	PROCESSOR	MEMORY	STORAGE	NIC
CoreLog APP (OVF)	48 threads	128 GB	300 GB (OS)+ 700 GB (Data)	1 Gb Ethernet or higher
Message Broker (OVF)	32 threads	32 GB	100 GB (OS) + 1 TB(Data)	1 Gb Ethernet or higher
Identity Gateway (OVF)	4 threads	16 GB	50 GB	2 Gb Ethernet or higher
Database (OVF)	48 threads	256 GB	300 GB (OS)+ 1 TB (Data)	1 Gb Ethernet or higher

۱ اندازه لاگ خام در محاسبات، ۹۰۰ بایت و اندازه لاگ نرمال شده نیز ۹۰۰ بایت در نظر گرفته شده است. این سند تنها تخمین نیازمندی های LOM را براساس مشخصات لاگ خام نمونه برآورد می کند و در صورتی که تعداد یا نوع سناریو ها و نرمال سازی رخدادها، قابلیت ها و سرویس های سامانه و فرکانس پردازشگر پیشنهادی و یا تعداد کاربران همزمان به میزان قابل توجهی تغییر کند، این LOM با درصد تغییری که از مشخصات نمونه اتفاق می افتد، تغییر پیدا خواهد کرد. لازم به ذکر است که لاگ های از نوع Windows و Sysmon ممکن است سربار پردازشی به میزان ۲۰ درصد بالاتر به سامانه تحمیل کنند. پس در صورتی که بیش از ۵۰ درصد رخدادها از این نوع هستند این ۲۰ درصد سربار پردازشی باید در نظر گرفته شود.

۲ در LOM حاضر فرکانس CPU از اهمیت خاصی برخوردار است. لذا با لحاظ کردن اولویت فرکانس نسبت به تعداد هسته های پردازشگر عمل شود. حداقل پردازشگر پیشنهادی برای این LOM، پردازشگر های زیر است:

Intel Xeon Gold 6248R Cache 35.75MB Cache 3.00 GHz

Intel Xeon Gold 6242 Cache 22MB 2.80 GHz

Intel Xeon Gold 6226R Cache 22 MB CPU 2.90 GHz

۳ سرورهای نسل ۱۰ شرکت HP برای این LOM مناسب می باشند و تست های سامانه با استفاده از این نسل از سرورها انجام گرفته است.

۴ هارد دیسک های پیشنهادی هارد دیسک های با IO > 5000 IOPS و Data Transfer Rate: 1200MB/s می باشد.

۵ بسته به نیازمندی های کارشناسان برای واکشی و نمایش داده ها استفاده از هارد دیسک های SSD و نیز RAID 10 با تعداد دیسک بالا می تواند تاثیر بسزایی در تامین نیازمندی ها داشته باشد.

۶ LOM حاضر با معماری Centralized Deployment ارائه شده است. در این معماری کلیه داده ها از سایتهای مختلف بصورت مستقیم به مرکز ارسال شده و عملیات پردازش و ذخیره سازی بر روی آنها انجام می شود.

۷ میزان دیسک تعیین شده برای نرخ رخداد به صورت پیوسته محاسبه شده است. برای نرخ رخداد نوسانی و یا دوره ای که ممکن است در ساعت های مختلف روز متفاوت باشد و نیز برای مدت زمان های کمتر نگهداری رخداد به نسبت زمان نگهداری و یا نرخ رخداد میزان دیسک مورد نیاز کاهش می یابد.

۸ با توجه به این که سرعت پردازش کوئری های همزمان، داشبورد های فعال، کاربران همزمان و Alert ها می تواند بر میزان Ram و Cpu مصرفی تاثیر گذار باشد، این منابع به صورت پیش بینی شده می باشند و پس از پیاده سازی و عملیاتی شدن سامانه، ممکن است افزایش یابند.

۹ نقش ماشین های ارائه شده به صورت تقریبی است و در صورت کمبود منابع ممکن است به تعداد ماشین ها افزوده شود.

۱۰ شرایط لازم برای تامین UPS و برق بی وقفه را برای سرور فیزیکی و سایر ماژول ها فراهم نمایید.

میـزان دریافـت و مدت نگهـداری رخـدادها

سازمان ها بنابر الزامات نهادهای نظارتی و یا با هدف شناسایی حملات پیشرفته APT، ملزم به ذخیره سازی لاگ‌های خود را برای زمان معینی در سامانه می باشد. نحوه Licensing سامانه کورلاگ بر اساس میزان EPS ورودی و مدت زمان نگهداری لاگ‌ها مطابق جدوال زیر می‌باشد:

لایسنس‌های EPS ورودی سامانه					
۱k EPS	۲k EPS	۳k EPS	۵k EPS	۷k EPS	۱۰k EPS
۱۲k EPS	۱۵k EPS	۱۷k EPS	۲۰k EPS	۲۵k EPS	۳۰k EPS
۳۵k EPS	۴۰k EPS	۵۰k EPS	۱۰۰k EPS		

مدت زمان نگهداری لاگ‌ها			
۱ مـــاهه	۳ مـــاهه	۶ مـــاهه	۱۲ مـــاهه

خـــدمات پشـتیبـانـی

با استـفاده از خـدمات پـشتیبـانی کـورلاگ می‌تـوانیـد در کم‌تـرین زمـان به متـخصـصیـن پشتـبانی فنـی دستـرسی داشته باشـید و بـا هـزینه‌ای مقـرون به صـرفه بسیاری از چالـش‌های کاربـری و فنی خود را برطرف کنید.

خـدمـات	پـایه	پیـشرفـته
پـشتیبـانی از طـریق تیکـت	✓	✓
پـشتیبـانی در زمـان اداری (۸x۵)	✓	✓
دستـرسی به پایـگاه دانـش (KB)	✓	✓
پـشتیبـانی جهـت رفـع باگ (مطابق SLA)	✓	✓
تـولید/بـهینه سـازی پـارسرهای شخصی سازی شده و پیشرفته		✓
تولید داشبوردها، گزارشات وUse-Caseهای شخصی سازی شده و پیشرفته		✓

پـشتـیبـانی پـایـه

این سطح پـشتیبانی، بصورت پیش‌فـرض در فروش تمامی محصولات لحاظ میشود و صرفاً در قبـال وجـود باگ‌هـای احتمـالی روی سـامانه، ارائـه میشـود. در پشتیبـانی پایـه ارائه سـایر خـدمات پـس از فـروش نظیـر توسعه آداپـتور جـدید، تـدوین داشبـورد، ریپـورت یا پـالیسی هـای شخصی سازی شده و... مستلزم محاسبه نفر/سـاعت و پـرداخت هـزینه میباشد.

پـشتـیبـانی پیـشرفتـه

این سـطح پـشتیبانی عـلاوه بـر رفـع مشـکلات سیـستمی (مطابـق SLAهای پشـتیبانی پایه)، شامل بـرخی خدمات پشتیبـانی شخصی سـازی شده نیز میباشد.

Core Log
AI-Powered Next Gen SIEM

در مسیر امنیت در هر قدم کنار شما هستیم.

۰۲۱-۴۱۸۷۸۰۰۰

info@behinrahkar.com

https://behinrahkar.com/corelog

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

بهین راهکار
راهکارهای جامع امنیت فناوری اطلاعات