

THEHIVE یک پلتفرم متن‌باز و پیشرفته برای مدیریت و پاسخگویی به حوادث امنیتی سایبری (INCIDENT RESPONSE) است که اختصاصاً برای تیم‌های SOC و CERT طراحی شده است. این پلتفرم امکان بررسی، مدیریت، ردیابی و تحلیل تهدیدات را در یک محیط کاملاً مشارکتی فراهم می‌سازد و به ابزارهای کلیدی مانند CORTEX و MISP متصل می‌شود.

آسان‌سازی مدیریت پرونده‌های امنیتی (TheHive 5): ساختاردهی کامل به حوادث و کاهش پیچیدگی‌های عملیاتی.

The
Hive

قابلیت‌های کلیدی

خودکارسازی فرآیند پاسخ به حادثه: تسریع در روند Investigation و صادر کردن دستورات خودکار.



نظارت کامل و کاهش Alert Fatigue: فیلتر هشدارهای تکراری و تمرکز تیم روی تهدیدات واقعی.



Knowledge Base: پایگاه دانش درون‌برنامه‌ای برای مستندسازی تجربیات و شواهد پرونده‌ها.



محیط‌های چند سازمانی (Multi-Tenant Environments): پشتیبانی کامل از ساختارهای چندسازمانی و تیم‌های MSSP جهت جداسازی کامل داده‌ها، مشتریان و پرونده‌ها در یک زیرساخت واحد.



مدیریت پیشرفته کاربران و دسترسی‌ها: تعریف دقیق نقش‌ها و مجوزها (Role & Permission) و اتصال یکپارچه به سامانه‌های مدیریت هویت LDAP / Active Directory.



شاخص‌ها و داشبوردهای مدیریتی (Metrics & Dashboards): پایش زنده روند بررسی حوادث، ارزیابی عملکرد تحلیلگران SOC و گزارش‌گیری دیداری از وضعیت امنیت سازمان.



Metrics & Dashboards: نمایش زنده شاخص‌های عملکردی، Timeline مشترک پرونده‌ها و گزارش‌گیری مدیریتی.



تایم‌لاین تعاملی (Timeline) و Knowledge Base: ثبت زمانی و کرونولوژیک تمام اقدامات صورت‌گرفته روی پرونده و مستندسازی تجربیات (Lessons Learned) در پایگاه دانش داخلی.



یکپارچه‌سازی با MISP و MITRE ATTACK: دریافت و ارسال هوشمند IOCها به MISP و نگاشت (Mapping) تاکتیک‌ها و تکنیک‌های حملات بر اساس استاندارد جهانی MITRE ATTACK.



APIهای جامع و یکپارچه‌سازی پیشرفته (Integrations & APIs): توسعه‌پذیری کامل: ارائه REST API جامع و Client Libraries جهت اتصال بی‌درنگ TheHive به کلیه ابزارها، سامانه‌ها و اسکریپت‌های داخلی سازمان.



پشتیبانی از استانداردهای امنیتی: یکپارچه‌سازی کامل با MISP جهت تبادل هوش تهدید و نگاشت تکنیک‌ها و تکنیک‌ها بر اساس فریم‌ورک MITRE ATTACK.

طراحی الگوها و فرم‌ها: سفارشی‌سازی کامل فرم‌های پرونده، متدولوژی‌های پاسخ و هشدارهای اختصاصی متناسب با نیاز سازمان.



اطلاع‌رسانی لحظه‌ای: ارسال خودکار و آنی نوتیفیکیشن‌ها به ایمیل، Webhook و سامانه‌های چت سازمانی (مانند Slack/Teams) به محض تغییر وضعیت پرونده‌ها.

گردش کار عملیاتی



01 تحلیل و پاسخ خودکار

Automation Response

بیش از 200 Analyzer و Responder آماده

تحلیل خودکار داده ها و امکان تعریف موارد سفارشی

تحلیل همزمان Observables

پردازش حجیم و سریع داده ها و اجرای اکشن های فوری (Active Response) جهت مهار تهدیدات

02 ارتباط قدرتمند TheHive و Cortex

Powerful Integration

تحلیل همه جانبه

بررسی هوشمند IP, Email, URL, Domain, File, Hash

پاسخ فعال (Active Response)

اجرای اسکریپت ها و دستورات امنیتی بلافاصله پس از شناسایی ، آلودگی

تبادل داده

ارسال و مدیریت بی-درنگ Ob-servable ها میان TheHive و MISP

03 گزارش و اشتراک گذاری دانش

Reporting & Sharing

گزارش های سفارشی و الگوها

ایجاد Template های حرفه ای گزارش برای ذینفعان و مدیران

مستند سازی

ثبت تجربیات حاصل از هر حادثه جهت امنیت آتی

خروجی به MISP

امکان Export کردن IOC ها و Tactic/Technique های یک Case به صورت مستقیم به MISP Event

04 یکپارچه سازی ها

Over 300+ Integration

SIEM & Analytics

Splunk | Elastic | QRadar | Microsoft Sentinel

EDR & Endpoint

CrowdStrike | Cortex XDR | Microsoft Defender | SentinelOne | Symantec | Bitdefender GravityZone | Trend Micro Vision One

Cloud & Network

Wiz | Vectra AI | VMware

Management & Intel

MISP | Jira

روش های استقرار

Deployment Options



SaaS / Cloud Platform

اجرای Cloud در زیرساخت اختصاصی AWS، همراه با مدیریت کامل زیرساخت و پشتیبانی.



On-prem / Self-Hosted

نصب مستقیم در زیرساخت سازمان با کنترل ۱۰۰٪ بر روی Configu-ration، Update و Monitoring.



IaaS / Cloud Images

استفاده از Image های آماده AWS و Azure همراه با کدهای De-ployment و به روزرسانی آسان.

مدیریت SLA و Escalation خودکار

تعریف قوانین زمان بندی پاسخگویی (SLA) برای هر نوع حادثه، ردیابی زنده مهلت بررسی و ارجاع خودکار پرونده در صورت تجاوز از زمان مجاز.

تحلیل دیداری ارتباطات

(Visual Graph & Correlation)

ترسیم خودکار نقشه ارتباطی میان شاخص های آلودگی (IOCs) در پرونده های مختلف جهت شناسایی کمپین های پیچیده سایبری.

زنجیره استناد شواهد

(Chain of Custody & Forensics)

ثبت غیرقابل تغییر تاریخچه دستکاری شواهد و هش فایلهای جهت ارزیابی های فنی و ارائه های قانونی/جرم یابی دیجیتال.