Core Trap

Deception Technology Solution

سامانه بومی فناوری‌های فریب

سامانه CoreTrap یک پلتفرم پیشرفته در حوزه فناوری‌های فریب است که با استفاده از راهکارهای نوین و متنوع، مهاجمان را به‌طور دقیق شناسایی کرده و رفتارهای آنها را ثبت می‌کند. این ابزار قدرتمند با هماهنگی با سایر سامانه‌های امنیتی، می‌تواند فرآیند شناسایی تهدیدات امنیتی را به صورت **خودکار** و **بدون False Positive** انجام دهد. با CoreTrap، شما می‌توانید به راحتی و با اطمینان بیشتر از امنیت شبکه خود حفاظت کنید و با خیالی آسوده به توسعه کسب‌وکار خود بپردازید.

WWW.BEHINRAHKAR.COM

دیتاشیت نسخه ۲.۲
آبان ۱۴۰۳

معـــرفی ســـامـانه

مقـدمـه

در دنیـای امروز که امنیت سایبـــری با سرعتی بی‌ســابقه‌ای در حال تحـول است، روش‌های دفـاعی سنتی دیـگر پاسخگو نمی‌باشد. سامانه فناوری‌های فریب با هدف ارائه یک راهکار پیشـــرفته جهت مقـــابله با حملات پیچیده و هدفمند سایبـــری طراحی شده اند. فناوری‌های فریب به شما این امکان را می‌دهد تا با قـــدرت و اطمینـان در برابر تهـــدیدات نوظهور، موضعی فعـــال اتخـــاذ کنید.

«مهمتـرین چالـش‌هـای برطـــرف شده تـــوســـط فنـــاوری‌های فـــریب»

- Compromised Users
- Real-Time Detection
- Insider Threats
- Lateral Movement
- Advanced and Targeted Threats
- False-Positive Alerts and Reports

حذف False Positive در هشـــدارها

ســامانه‌های فنـــاوری فـــریب با تـــوجه به مـــاهیـــت هـــر نـــوع فعـــالیتی که شنـــاســـایی نمـــاید، قطعـــاً مخـــرب بـــوده و تیـــم‌هـــای امنیتـــی می‌تـــوانند بـــدون هیـــچ گـــونه تـــردیدی وارد فـــرآینـــد پاســـخ به رخـــداد امنیتـــی شنـــاســـایی شـــده شـــوند.

شنـــاســـایی Lateral Movement

شنـــاســـایی مهـــاجمـــانی که در تـــلاش بـــرای انجـــام فـــرآیند Lateral Movement بیـــن ســـرورها، برنـــامه‌ها و دیتـــابیس‌هـــا هستنـــد.

شنـــاســـایی کـــاربـــران قـــربانـــی شـــده

با استفـــاده از کلمه‌عبـــورها، کوکی‌ها و طعمـــه‌ها، مهـــاجمـــانی که از ایـــن دارایی‌هـــای جعلی استفـــاده می‌کنند، شنـــاســـایی می‌شـــوند.

گزارش‌های فـــارنزیـــک برای حمـــلات شنـــاســـایی شـــده

فنـــاوری‌هـــای فـــریب می‌تواننـــد گـــزارش دقیقـــی از تمـــامی فعـــالیت‌هـــای مهـــاجم در طـــی حملـــه ارائـــه دهنـــد.

CoreTrap به عنـــوان یک ســـامانه فنـــاوری هـــای فـــریب از طـــریق طیـــف وسیـــعی از دارایی‌هـــای جعـــلی، ســـازمان را در جهت شنـــاسایی اهداف و رفتار مهاجمین و همچنین سطح نفوذ آن‌ها به شبکه سازمان، آگاه می‌نمـــاید.

ویـژگی‌هـــای کلیـــدی کورتـرپ

CoreTrap به عنـــوان اولیـــن ســـامـــانه کامـــلا بـــومی فنـــاوری‌هـــای فـــریب (Deception Technologies) شنـــاخته می‌شـــود. بـــرخی از مهـــم‌تـــرین قابـلیـــت‌های این ســـامـــانه عبـــارتنـــد از:

۱ امـکان پیـاده سازی Decoy Node های مـتنوع

پـشـــتیبـــانـی از دارایـی‌هـــای جـــعلـی در ســـطـح VM ،Network Device، Service/Application

۲ امـکان پیاده سـازی Decoy Object هـای متنـــوع

پشـــیبـــانی از انـواع مختـلف Decoy Object هـا شـامـل: Document، User، Token، Email Account، Malware و ...

۳ کـــنسول مـــدیریـت یکـــپارچـــه

مدیریت متمـــرکز چـرخه حیـات تمامی دارایی‌های جعـلی

۴ Breadcrumbs

هدایـت مهـاجمان به سـرورهای از پیـش بـرنامه ریزی شـده

۵ Forensic

قابلیت ارائـه گـزارش کامـلاً خـــودکار از Time Line حمـــلات شنـــاسـایی شـــده

۶ API First

قابلیت ایجـــاد دارایی‌هـای جعلی و دریافـــت گزارشـــات از طـــریق REST-API

۷ داشبـــورد و گـــزارشـــات

قابلیت تولیـــد داشـــبورد و گـزارش‌های شخـصـی سـازی شـــده‌ی مـدیـــریتی و فنـی

۸ شبیـــه سـازی سـامـانـه‌هـای اخـتـصـــاصـی

قـابلـیـت شـبیـه سـازی سـامـانـه‌هـای اخـتصـاصی سـازمان به عـنـوان Decoy Node

۹ امـــکان اطـلاع رســـانی رخـــدادهـــا

پـــشـتـیبـــــانی از SMS، Email، REST-API

۱۰ Deep Investigation

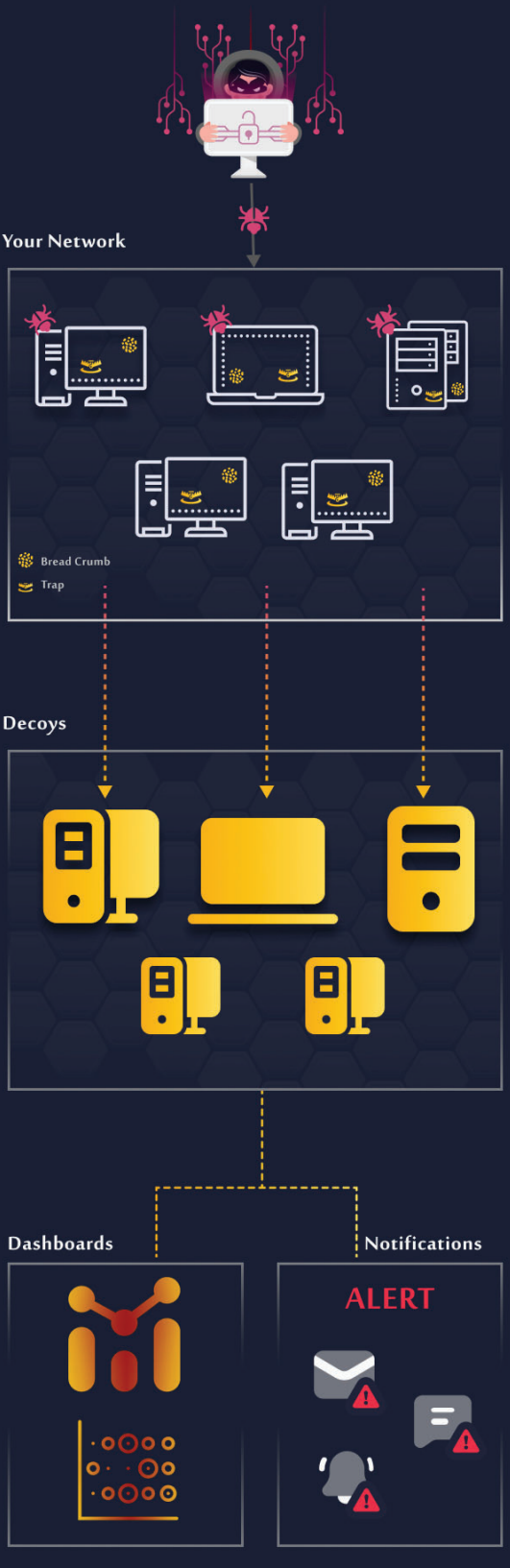
قابلیـــت جستجـوی پیشـرفته بـر روی تمـامی فعـالیت‌های شناســایی شده از مهـــاجمـــان

کـــورترپ، نســـــل جدید هـانی پات

فریب و به دام انـداختن هکـرها و مهـاجمان سایبـری

کورترپ چگونه کار میکند؟

Inspired by: **MITRE D3FEND** | **Deception Technologies** | **Honeypot**



نحوه جایگذاری دارایی‌های جعلی (Decoy Entities)

برای استفاده از CoreTrap در شبکه سازمان، پاسخ به سوالات زیر ضروری است:

۱. مکان جایگذاری

داده‌ها و نودهای جعلی باید در کدام زیرساخت قرار بگیرند؟
(شبکه اصلی سازمان یا زیرساخت اختصاصی جعلی)

۲. نوع دارایی جعلی

سازمان نیازمند چه نوع داده‌ها و نودهای جعلی می‌باشد؟
(Service ،Network Traffic ،Server ،User ،Document)

پیاده سازی دارایی‌های جعلی

پس از پاسخ به سوالات ذکر شده، می‌توان با استفاده از سامانه CoreTrap و مخزن غنی آن، داده‌ها و نودهای جعلی را بصورت خودکار در زیرساخت مناسب پیاده‌سازی کرده و روش ارتباطی آنها با CoreTrap را تعیین نمود.

اعلان رخداد و تحلیل داده‌ها

با نظارت بر رفتار دارایی‌های جعلی، می‌توان اطلاعات زیر را ارزیابی کرد:

۱. منشأ حملات سایبری
۲. سطح تهدید آنها
۳. روش‌های نفوذ مورد استفاده
۴. داده‌ها یا برنامه‌های هدف
۵. تأثیر کنترل‌های امنیتی در جلوگیری از حملات سایبری

لایسنس سامانه کورترپ

سامانه CoreTrap به شما این امکان را می‌دهد تا بر اساس نیاز کسب و کار خود، تعداد Decoy Object و Decoy Node را انتخاب کنید.

Features	BASIC	PRO	ADVANCED
Object Malware، Document، User، Token، Email Account	5	10	20
VM Windows 7 / 10 / 11, Win 10 / 11 (customizable, BYOL), Win Server 2016/2019/2022 (customizable, BYOL), Ubuntu 16.04 / 18.04 /20.04, Redhat (customizable, BYOL), CentOS 7.9, SSL-VPN, ESXI Decoy, FortiGate, Network Device(Routers, Switch, Printers and IP-Camera)	2	5	20
Service basicauth, ssh, telnet,ftpd, vnc, postgress, mssql, redis, mysql, oracle, ldap, rdp, dns, mariadb, git, synology, pop3, imap, smtp, socks5, squid, elasticsearch, owa, irc, elasticsearch, winbox, printer, mongodb, tomcat-ssl, tomcat, mqtt, apache-ssl, apache, pptp, memcached, ilo, tplink-web, nginx, nginx-ssl, smbd	10	25	100
Security Policy	✓	✓	✓
Notification	✓	✓	✓
Integration (SIEM)	✓	✓	✓
Log Retention	1 month	6 months	12 months
API Access	✓	✓	✓
Audit Logs	✓	✓	✓
VLAN	✓	✓	✓
Investigation	✓	✓	✓
Breadcrumbs	-	-	✓

اجزا و نیازمندیهای سخت افزاری سامانه

CoreTrap_ App (OVA)	
PROCESSOR	20 Core (>=2.4 GHz)
MEMORY	64 GB
STORAGE	1.2 TB
NIC	1 Gb + 1GB

Identity Gateway (OVA)	
PROCESSOR	4 threads
MEMORY	16 GB
STORAGE	50 GB
NIC	2 NICs (Gb Ethernet or higher)

Update Proxy (OVA)	
PROCESSOR	4 Core
MEMORY	8 GB
STORAGE	50 GB
NIC	1 Gb Ethernet or higher

CoreTrap_VM Worker (OVA) For Basic Model	
PROCESSOR	12 Core (>=2.4 GHz)
MEMORY	32 GB
STORAGE	700 GB
NIC	1 Gb

CoreTrap_Service Worker (OVA) For Basic Model	
PROCESSOR	10 Core (>=2.4 GHz)
MEMORY	32 GB
STORAGE	400 GB
NIC	1 Gb

خـــدمات پشـتیبـانـی

با اسـتـفاده از خـدمات پشتیبـــانی CoreTrap، می‌تـــوانید به ســـرعت به متـخصصیـــن فنی دستـــرسی پیـــدا کـــرده و با هـــزینه‌ای مقـــرون به صـــرفه، چالـــش‌های مـــرتبط با نگـــهداری، عیـــب‌یابی و بهینـــه‌سازی ســـامانه خود را بـــرطـــرف نمـــایید.

خـدمـات	پـایه	پیـــشرفـته
پـشتیبـــانی از طـریق تیکـت	✓	✓
پـشتیبـــانی در زمـان اداری (۸x۵)	✓	✓
دستـــرسی به پایـگاه دانـش (KB)	✓	✓
پـشتیبـــانی جهـت رفـع باگ (مطابق SLA)	✓	✓
تـولید داشبـورد/ریپـورت/پالیسی شخصی سـازی شده (مطابق SLA)		✓

Core Trap
Deception Technology Solution

در مسیر امنیت در هر قدم کنار شما هستیم.

۰۲۱-۴۱۸۷۸۰۰۰

info@behinrahkar.com

https://behinrahkar.com/coretrap

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

بهین راهکار
راهکارهای جامع امنیت فناوری اطلاعات