هرم دشواری در ستیز: چارچوبی راهبردی برای دفاع سایبری پیشرفته

چکیده

چارچوب هرم دشـــواری (Pyramid of Pain) که توســـط دیوید بیانکو در ســـال ۲۰۱۳ معرفی شـــد، تحولی بنیادین در رویکردهای هوشـمندی تهدید و عملیات امنیتی ایجاد کرده اسـت. این مقاله با بررسـی پیاده‌سـازی راهبردی آن در مراکز عملیات امنیتی (SOC) مدرن، نشـان می‌دهد چگونه سـطوح مختلف دشـواری تغییر شـاخص‌ها با اثربخشـی دفاعی همبسـتگی دارد. با تمرکز بر شـاخص‌های سـطوح بالاتر، ســـازمان‌ها می‌توانند هزینه‌های عملیاتی مهاجمان را به شـــکل قابل توجهی افزایش داده و رویکردهای واکنشـــی امنیتی را به راهبردهای دفاعی پیش‌کنشگرانه تبدیل کنند.

مقدمه

در فضـای تهدیدات پیچیده امروزی، تفاوت میان صـرفاً شـناسـایی فعالیت‌های مخرب و مختل کردن مؤثر عملیات مهاجمان، نه در تعداد شاخص‌های جمع‌آوری شده، بلکه در ارزش راهبردی آنها نهفته است.

اصل بنیادین امنیت سایبری "تهاجم به دفاع آگاهی می‌بخشد" (OFFENSE informs DEFENSE)

هرگز به اندازه امروز که تیم‌های دفاعی به طور فزاینده‌ای روش‌شناسی‌های مهاجم‌محور را اتخاذ می‌کنند، موضوعیت نداشته است.

مدل مفهومی هرم دشـــواری، یکی از تأثیرگذارترین ســـهم‌ها در این رویکرد اســـت که چارچوبی ســـاختارمند برای تیم‌های امنیتی فراهم می‌کند تا قابلیت‌های دفاعی خود را بر اســـاس تأثیر عملیاتی وارده بر مهاجمان ارزیابی کنند. این چارچوب از مدل‌های ســـنتی تشـــخیص دوگانه فراتر رفته و تلاش‌های امنیتی را در طیفی از پتانسیل اختلال در عملیات مهاجم قرار می‌دهد.

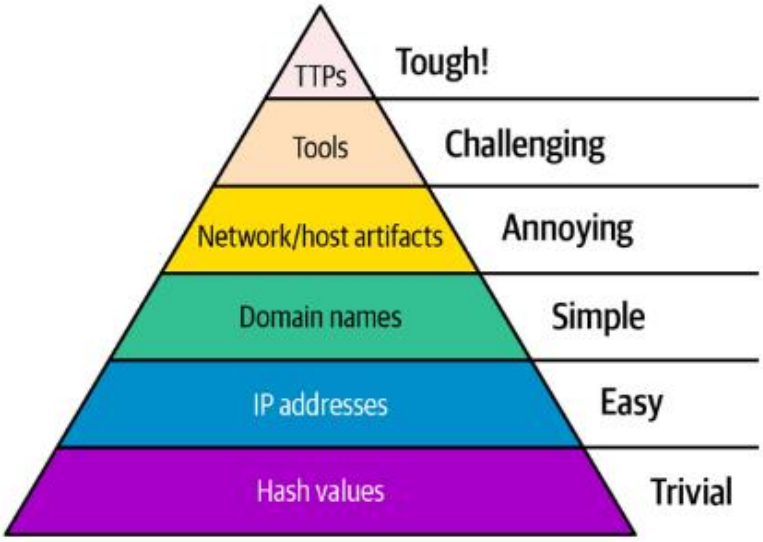
بنیان نظری

هرم دشواری، شاخص‌های سازش (IoCs) را بر اساس دو بعد حیاتی طبقه‌بندی می‌کند:

۱ .**هزینه تغییر برای مهاجم** : تلاش عملیاتی، منابع و خطر احتمالی افشا که مهاجم باید برای تغییر شاخص بپذیرد

۲ .**ارزش دفاعی** : ارزش زمینه‌ای و پایداری تشخیص که شاخص برای تیم‌های دفاعی فراهم می‌کند

این ارزیابی دوسویه، ساختاری سلسله‌مراتبی ایجاد می‌کند که در آن، شاخص‌های رأس هرم، بار عملیاتی به مراتب بیشتری برای مهاجمان جهت تغییر ایجاد می‌کنند، در حالی که همزمان به مدافعان قابلیت‌های تشـــخیصـــی پایداری می‌دهند که از تکنیک‌های ســـاده فرار فراتر می‌رود.



ساختار هرم

سطح ۱: مقادیر هش MD5 ، SHA1، SHA256

- ☑ **هزینه برای مهاجم** : ناچیز
- ☑ **ارزش دفاعی** : محدود

تشخیص مبتنی بر هش، شکننده‌ترین شکل هوشمندی تهدید است. اگرچه در حالت اصلاح‌نشده دقت کاملی ارائه می‌دهد، اما ماهیت رمزنگاری الگوریتم‌های هش به این معناست که حتی تغییر تک‌بایت در نمونه‌های بدافزار، مقادیر هش کاملاً جدیدی تولید می‌کند. مهاجمان پیچیده از تکنیک‌های مختلفی برای بی‌اعتبار کردن تشخیص مبتنی بر هش استفاده می‌کنند:

- کد با ماهیت تغییر مداوم که در زمان اجرا خود را تغییر می‌دهد
- Wrapper زمان اجرا که در هر آلودگی، محموله‌های منحصر به فردی تولید می‌کنند
- شناسه زمانی یا شناسه‌های منحصربه‌فرد تعبیه‌شده برای هر کمپین

مورد عملی : در سال ۱۴۰۲، تیم امنیتی یک شرکت مخابراتی ایرانی گزارش کرد که مهاجمان APT با استفاده از تغییرات جزئی در یک بدافزار خاص، توانستند در کمتر از ۲۴ ساعت بیش از ۵۰ نسخه مختلف با هش‌های متفاوت تولید کنند، به طوری که تشخیص مبتنی بر هش سنتی کاملاً ناکارآمد شد.

دلالت راهبردی : تشخیص مبتنی بر هش باید به عنوان یک مزیت تاکتیکی موقت به جای یک قابلیت تشخیص راهبردی در نظر گرفته شود.

سطح ۲: آدرس‌هایIP

- ☑ **هزینه برای مهاجم** : کم
- ☑ **ارزش دفاعی** :متوسط

زیرساخت شبکه نشانگر طبقه شاخصی کمی پایدارتر است، هرچند هنوز به راحتی توسط مهاجمان مصمم دور زده می‌شود از طریق:

- زیرساخت‌های با چرخش سریعIP

- زیرساخت‌های مشروع به عنوان پروکسی
- بهره‌برداری از محدوده‌های IP ارائه‌دهندگان ابری با اعتبار بالا
- استفاده از سرویس‌های میزبانی مقاوم با بخش‌های پاسخگویی غیرفعال به سوء استفاده

مورد عملی : مرکز ماهر در گزارش سال ۱۴۰۱ خود، یک کمپین APT را مستند کرد که از بیش از ۱۰۰ آدرس IP مختلف از شش ارائه‌دهنده خدمات ابری در کمتر از یک هفته استفاده کرد. تیم‌های امنیتی که صرفاً بر مسدودسازی IP تکیه می‌کردند، به سرعت با مشکل با مواجه سنگین و پرتعداد در دریافت هشدارهای دروغین و ناتوانی در مسدودسازی مؤثر مواجه شدند.

دلالت راهبردی : مسدودسازی مبتنی بر IP عمدتاً در برابر تهدیدات فرصت‌طلبانه ارزشمند است، اما اصطکاک حداقلی در برابر عملیات هدفمند ایجاد می‌کند.

سطح ۳: نام‌های دامنه

☑ **هزینه برای مهاجم** : متوسط
☑ **ارزش دفاعی** : متوسط

زیرساخت دامنه، درگیری عملیاتی معناداری ایجاد می‌کند و مهاجمان را ملزم می‌سازد به:

- ثبت دامنه‌های جدید با روش‌های پرداخت معتبر
- اجازه انتشار دامنه از طریق زیرساخت DNS
- ایجاد پیکربندی‌های سرور جدید
- خطر افشای الگوهای ثبت

با این حال، مهاجمان پیشرفته با این موارد مقابله می‌کنند:

- الگوریتم‌های تولید دامنه (DGAs) که به صورت پویا نقاط انتهایی فرماندهی و کنترل ایجاد می‌کنند
- استفاده از دامنه‌های معتبر با غلط املایی برای گریز از تشخیص مبتنی بر الگو
- تکنیک‌های DNS over HTTPS برای دور زدن نظارت سنتی DNS
- بهره‌گیری از دامنه‌های معتبر و پذیرفته شده براساس اعتبار اثبات شده‌شان

مورد عملی : تحلیل یک سال گروه امنیت سایبری دانشگاه تهران در سال ۱۴۰۲ نشان داد که یک گروه APT با استفاده از الگوریتم تولید دامنه پیشرفته، توانست در یک دوره ۶ ماهه بیش از ۱۲۰۰ دامنه فرماندهی و کنترل (C&C) تولید کند. با این وجود، تحلیل الگوی ثبت و رفتار DNS این دامنه‌ها منجر به شناسایی الگوریتم زیربنایی شد، که امکان پیش‌بینی و مسدودسازی پیشگیرانه دامنه‌های آینده را فراهم کرد.

دلالت راهبردی : هوشمندی دامنه ارزش دفاعی متوسطی ارائه می‌دهد، به ویژه هنگامی که با تشخیص الگو و تحلیل فراداده‌های ثبت ترکیب شود.

سطح ۴: آرتیفکت‌های میزبان/شبکه

- ☑ **هزینه برای مهاجم** : قابل توجه
- ☑ **ارزش دفاعی** : بالا

تشـــخیص مبتنی بر آرتیفکت، هزینه‌های عملیاتی مهاجم را با هدف قرار دادن پیاده‌ســـازی‌های تاکتیکی آنها به طور قابل توجهی افزایش می‌دهد:

- سازوکارهای پایداری بدافزار (کلیدهای رجیستری، وظایف زمان‌بندی‌شده)
- پارامترهای خط فرمان و زنجیره‌های اجرایی
- شاخص‌های مقیم در حافظه و روابط فرآیندی
- آرتیفکت‌های سیستم فایل و الگوهای تغییر

این شاخص‌ها نمایانگر اجزای اصلی فنون تخصصی مهاجم هستند که برای تغییر، نیازمند پیکربندی مجدد قابل توجهی هستند و احتمالاً خطاهای عملیاتی معرفی می‌کنند و سطح تشخیص را افزایش می‌دهند.

مورد عملی : در سال ۱۴۰۱، یک شرکت بزرگ انرژی ایران با استفاده از شناسایی آرتیفکت‌های میزبان توانست الگوی منحصربه‌فرد مسیرهای فایل موقت و ارتباطات فرآیندی یک بدافزار پیشرفته را شناسایی کند. این شاخص‌ها حتی پس از تغییر چندین باره هش، دامنه و آدرس‌هایIP ، ثابت ماندند و به تیم امنیتی امکان دادند مهاجم را در شبکه ردیابی کنند.

دلالت راهبردی : تشـخیص مبتنی بر آرتیفکت، مهاجمان را مجبور به تغییر اســاســی تکنیک‌های پس از بهره‌برداری می‌کند و غالباً در دوره‌های انتقالی فرصت‌های تشخیص جدیدی را آشکار می‌سازد.

سطح ۵: ابزارها

- ☑ **هزینه برای مهاجم** : بالا
- ☑ **ارزش دفاعی** : بالا

تشخیص مبتنی بر ابزار، قابلیت‌های عملیاتی اصلی که مهاجمان به آنها متکی هستند را هدف قرار می‌دهد:

- چارچوب‌های بهره‌برداری سفارشی یا تجاری Cobalt Strike
- ماژول‌های قابلیت تخصصی Mimikatz ، PowerSploit
- ابزارهای مختص پروتکل (تونل‌سازی، زنجیره‌های پروکسی)

تغییر یا جایگزینی ابزارهای تثبیت‌شده، اصطکاک قابل توجهی برای مهاجم ایجاد می‌کند:

- نیازمند چرخه‌های توسعه و آزمایش گسترده
- خطر معرفی ناپایداری عملیاتی
- ضرورت آموزش مجدد اپراتورها برای قابلیت‌های جدید
- احتمال حذف عملکردهای حیاتی

مورد عملی : در یک رویداد مستندشده توسط آزمایشگاه امنیت دانشگاه صنعتی شریف در سال ۱۴۰۰، تیم دفاعی یک بانک بزرگ موفق شد همه نمودهای یک ابزار اختصاصی تونل‌زنی DNS را شناسایی و مسدود کند. مهاجمان برای تغییر ابزار خود بیش از سه ماه زمان نیاز داشتند، که در این مدت فاقد امکان دسترسی مؤثر به شبکه قربانی بودند. این وقفه، عملاً به پایان عملیات مهاجم در آن سازمان منجر شد.

دلالت راهبردی : تشخیص جامع ابزار می‌تواند مهاجمان را مجبور به رها کردن روش‌شناسی‌های عملیاتی ترجیحی کند و به طور قابل توجهی زمان‌بندی‌های کمپین آنها را مختل و نرخ شکست را افزایش دهد.

سطح ۶: تاکتیک‌ها، تکنیک‌ها و روش‌ها(TTPs)

- ☑ **هزینه برای مهاجم** : بسیار بالا
- ☑ **ارزش دفاعی** : حداکثر

تشخیص مبتنی بر TTP نمایانگر رأس هرم است که روش‌شناسی‌های بنیادی تعریف‌کننده عملیات مهاجم را هدف قرار می‌دهد:

- راهبردهای حرکت بطئی و جانبی
- توالی‌های افزایش امتیاز
- روش‌شناسی‌های استخراج داده
- معماری‌های فرماندهی و کنترل

این عناصر، هسته دکترین عملیاتی مهاجم را تشکیل می‌دهند و معمولاً به دلایل زیر در سراسر کمپین‌ها ثابت می‌مانند:

- نیازمندی‌های دانش سازمانی عمیق
- الگوهای موفقیت عملیاتی تثبیت‌شده
- سرمایه‌گذاری‌های آموزشی و مستندسازی
- ترجیحات روان‌شناختی و مناطق آسایش

مورد عملی : مرکز مدیریت راهبردی افتا در سال ۱۴۰۲ توانست با تحلیل عمیق چندین کمپین مرتبط با یک گروهAPT ، الگوی منحصربه‌فرد افزایش امتیاز آنها را شناسایی کند. این الگو شامل یک توالی خاص از اجرای اسکریپت‌ها، دستکاری رجیستری، و استفاده از فرآیندهای سیستمی مشروع بود. پس از پیاده‌سازی تشخیص این TTP در سازمان‌های حیاتی کشور، مهاجمان تلاش کردند روش‌های خود را تغییر دهند، اما به دلیل نیاز به بازآموزی کامل تیم و توسعه تکنیک‌های جدید، مجبور به توقف عملیات خود برای بیش از ۶ ماه شدند.

دلالت راهبردی : تشخیص و مقابله مؤثر باTTP ها، مهاجمان را مجبور به ارزیابی مجدد اساسی کل رویکرد عملیاتی خود می‌کند در اصل، نیازمند آن است که "مهاجمان متفاوتی شوند".

ارتباط هرم دشواری با سایر چارچوب‌های امنیتی

یک نقطه قوت مهم هرم دشواری، قابلیت همگرایی آن با سایر چارچوب‌های شناخته‌شده امنیتی است:

هم‌پوشانی با MITRE ATT&CK

چارچوب ATT&CK ، تاکتیک‌ها و تکنیک‌های مهاجمان را دسته‌بندی می‌کند که مستقیماً با دو سطح بالایی هرم دشواری هم‌راستا هستند:

- بخش «نرم‌افزار» ← سطح ۵ هرم (ابزارها)
- بخش «تاکتیک‌ها» و «تکنیک‌ها» ← سطح ۶ هرم (TTPs)

رویکرد تلفیقی : ترسیم نگاشت شاخص‌های هرم دشواری به ماتریس ATT&CK به تیم‌های امنیتی امکان می‌دهد تحلیل جامع‌تری از پوشش تشخیصی خود انجام دهند.

تکمیل مدل زنجیره کشتار (Kill Chain)

زنجیره کشتار لاکهید مارتین مراحل مختلف یک حمله را نشان می‌دهد، در حالی که هرم دشواری، شاخص‌های تشخیصی در هر مرحله را طبقه‌بندی می‌کند:

- مراحل اولیه زنجیره (شناسایی، تسلیح) ← (IPهش،) شاخص‌های سطح پایین هرم
- (C2 بهره‌برداری، نصب) مراحل پیشرفته زنجیره ← (TTPsابزارها،) شاخص‌های سطح بالای هرم

رویکرد تلفیقی : طراحی راهبردهای تشخیصی که به طور سیستماتیک هر مرحله زنجیره کشتار را با تمرکز بر شاخص‌های سطح بالای هرم پوشش می‌دهند.

تقویت چارچوب Diamond Model

مدل الماس تهدید، چهار بعد یک رویداد سایبری را مشخص می‌کند: مهاجم، زیرساخت، قابلیت و قربانی. هرم دشواری با تمرکز خاص بر اجزای زیرساخت و قابلیت این مدل را تقویت می‌کند:

- سطوح ۱-۳ هرم ← بعد «زیرساخت» در مدل الماس
- سطوح ۴-۶ هرم ← بعد «قابلیت» در مدل الماس

رویکرد تلفیقی : استفاده از هرم دشواری برای ارزیابی نیمه فنی مدل الماس، در حالی که از ابعاد مهاجم و قربانی برای زمینه‌سازی تهدید استفاده می‌شود.

پیاده‌سازی هرم دشواری درSOC های مدرن

انتقال از درک تئوریک به پیاده‌سازی عملیاتی، نیازمند روش‌شناسی ساختارمند است:

۱ . ارزیابی بلوغ و راهکارهای پیاده‌سازی تدریجی

SOCهای با منابع محدود می‌توانند رویکرد تدریجی برای پیاده‌سازی چارچوب هرم دشواری اتخاذ کنند:

مرحله ۱ – پایه (با منابع حداقلی):

- تمرکز بر تشخیص‌های هش و IP (سطوح ۱-۲) با سیستم‌های SIEM موجود
- پیاده‌سازی آزمایشی جمع‌آوری و تحلیل رویدادهای میزبان برای آرتیفکت‌ها (سطح ۴)
- ارزیابی شاخص‌های تشخیص فعلی و شناسایی شکاف‌ها در سطوح مختلف هرم

مرحله ۲ – میانی (با منابع متوسط):

- اضافه کردن ابزارهای EDR پایه برای تشخیص آرتیفکت‌های میزبان (سطح ۴)
- پیاده‌سازی تحلیل دامنه و شناسایی DGA (سطح ۳)
- شروع **پروژه‌های شکار تهدید** با تمرکز بر ابزارهای شناخته‌شده (سطح ۵)

مرحله ۳ – پیشرفته (با منابع کامل):

- پیاده‌سازی تحلیل رفتاری با هدف شناسایی TTPs (سطح ۶)
- ادغام تحلیل‌های خودکار با سیستم‌های SOAR
- توسعه قابلیت‌های هوشمندی تهدید داخلی

مورد عملی : یک شرکت متوسط فناوری در اصفهان با تیم امنیتی ۵ نفره، در سال ۱۴۰۱ رویکرد تدریجی را اتخاذ کرد. آنها ابتدا با بهبود سیستم‌های ثبت رویداد شروع کردند، سپس یک EDR ساده پیاده‌سازی نمودند، و در مدت ۱۸ ماه، توانستند به تشخیص سطح ۵ (ابزارها) دست یابند. این رویکرد تدریجی، در مقایسه با تلاش برای پیاده‌سازی همزمان همه سطوح، منجر به موفقیت پایدارتری شد.

۲ . ادغام هوشمندی تهدید

توسعه راهبردهای جمع‌آوری هوشمند که شاخص‌های سطوح بالاتر را اولویت‌بندی می‌کنند، در حالی که پوشش پایه را حفظ می‌کنند:

- استفاده از منابع متن‌باز OSINT با تمرکز بر گزارش‌های تحلیلی به جای فیدهای ساده IoC
- عضویت در گروه‌های اشتراک‌گذاری اطلاعات صنعتی (ISACs) برای دسترسی به هوشمندیTTP
- توسعه فرآیندهای داخلی برای استخراج TTPs از رویدادهای امنیتی سازمان
- فیلتر کردن هوشمند در آستانه ورودی‌های ترافیکی برای کاهش شاخص‌های سطح پایین با ارزش دفاعی محدود

معیارهای سنجش موفقیت:

- نسبت شاخص‌های سطح بالا به سطح پایین در هوشمندی وارده

- میزان پوشش گروه‌های تهدید مرتبط با صنعت در سطوح ۵-۶ هرم
- کیفیت زمینه‌ای همراه با هر شاخص (چگونگی، چرایی و زمان استفاده مهاجم)

۳ . مهندسی تشخیص

طراحی منطق تشخیصی که شاخص‌های چندین سطح هرم را همبسته می‌کند و الگوهای تشخیص ترکیبی مقاوم در برابر فرار ساده ایجاد می‌کند:

رویکردهای تشخیص چندسطحی:

- **تشخیص ترکیبی** : همبستگی شاخص‌های چندین سطح هرم برای کاهش خطاهای مثبت کاذب

  مثال:

  شناسایی یک دامنه مشکوک (سطح ۳) + الگوی مشخص خط فرمان پاورشل (سطح ۴) + تماس با پورت غیرمعمول سطح ۴) = اطمینان بالاتر از تشخیص نسبت به هر شاخص به تنهایی

- **تشخیص سلسله‌مراتبی** : استفاده از شاخص‌های سطح پایین به عنوان محرک برای تحلیل‌های عمیق‌تر سطوح بالاتر

  مثال:

  شناسایی یک IP مشکوک (سطح ۲) ⟵ بررسی خودکار رفتار میزبان‌های متصل شده برای آرتیفکت‌ها (سطح ۴) ⟵ فعال‌سازی شکار تهدید برای شناسایی ابزارها (سطح ۵)

- **تشخیص رفتاری** :مدل‌سازی رفتارهای TTP بدون وابستگی به شاخص‌های سطح پایین

  مثال: تشخیص الگوهای مشخص افزایش امتیاز صرف‌نظر از ابزار یا دامنه خاص مورد استفاده

- **پیاده‌سازی در سیستم‌های مدرن:**
  - **در SIEM**
    - طراحی قوانین چندمرحله‌ای با آستانه‌های متغیر
    - کاهش وزن دهی به هشدارهای مبتنی بر شاخص‌های سطح پایین
    - ایجاد قوانین همبستگی مبتنی بر رفتار
  - **در EDR/XDR**
    - تمرکز بر تشخیص رفتاری به جای تطبیق الگوی ساده
    - استفاده از یادگیری ماشین برای شناسایی انحرافات رفتاری
    - پایش زنجیره‌های رویداد کامل به جای رویدادهای منفرد
  - **مورد عملی** : مرکز عملیات امنیت یک سازمان مالی بزرگ در تهران، از رویکرد تشخیص ترکیبی استفاده کرد تا نرخ هشدارهای مثبت کاذب را ۷۰٪ کاهش دهد. آنها متوجه شدند که همبستگی یک درخواست DNS مشکوک (سطح ۳) با مشاهده یک الگوی خاص فعالیت فایل در همان میزبان (سطح ۴)، میزان اطمینان تشخیص را به طور قابل توجهی افزایش می‌دهد. این رویکرد منجر به کاهش چشمگیر زمان بررسی تحلیلگران و افزایش نرخ تشخیص موفق شد.

۴ .شکار تهدید مبتنی بر فرضیه

- انجام جستجوهای فعالانه بر اساس نمایه مورد انتظار TTP به جای شاخص‌های خاص:
  - ⊕ توسعه فرضیه‌های شکار بر اساسTTP های شناخته‌شده گروه‌های تهدید مرتبط با صنعت
  - ⊕ استفاده از تکنیک‌های تحلیل رفتاری برای شناسایی الگوهای مشکوک حتی بدون شاخص‌های خاص
  - ⊕ پیاده‌سازی رویکردهای خودکارسازی برای گسترش قابلیت‌های شکار تهدید محدود

فناوری‌های نوظهور برای تقویت شکار تهدید:

- **یادگیری ماشین برای شناسایی TTP :** استفاده از الگوریتم‌های یادگیری ماشین برای تشخیص الگوهای رفتاری پیچیده که برای تحلیلگران انسانی دشوار است :
  - ⊕ الگوریتم‌های تشخیص ناهنجاری برای شناسایی انحرافات از رفتار عادی
  - ⊕ مدل‌های یادگیری عمیق برای تشخیص الگوهای حمله پیچیده
  - ⊕ تحلیل رفتاری کاربر و موجودیت (UEBA) برای شناسایی رفتارهای عجیب

- **خودکارسازی شکار تهدید** : استفاده از فناوری‌های SOAR برای خودکارسازی فرآیندهای تکراری شکار تهدید :
  - ⊕ اجرای خودکار پرس‌وجوهای شکار بر اساس زمان‌بندی یا محرک
  - ⊕ پاسخ خودکار به یافته‌های اولیه برای جمع‌آوری اطلاعات بیشتر
  - ⊕ مستندسازی خودکار نتایج برای بهبود مستمر فرضیه‌های شکار

مورد عملی :تیم امنیتی یک شرکت دانش‌بنیان در پارک علم و فناوری پردیس، با استفاده از فرضیه‌سازی مبتنی بر TTP توانست یک کمپین جاسوسی سایبری مخفی را که بیش از ۹ ماه در شبکه آنها فعال بود، شناسایی کند. آنها با تمرکز بر الگوهای معمول دسترسی به داده‌های حساس (سطح ۶) به جای جستجوی شاخص‌های سطح پایین، توانستند فعالیت‌های مشکوکی را شناسایی کنند که از تشخیص‌های سنتی فرار کرده بودند.

۵ .چرخه بازخورد مستمر

مستندسازی انطباق‌های مهاجم با تشخیص، اطلاع‌رسانی به استراتژی تشخیص آینده:

- ایجاد فرآیند رسمی برای ثبت تغییرات تاکتیکی مهاجمان پس از تشخیص
- تحلیل روند شاخص‌های مشاهده‌شده برای ارزیابی اثربخشی راهبردهای دفاعی
- اشتراک‌گذاری یافته‌ها با جامعه امنیتی وسیع‌تر برای افزایش دانش جمعی

معیارهای سنجش اثربخشی

برای اندازه‌گیری اثربخشی پیاده‌سازی هرم دشواری، SOCها باید معیارهای سطح‌بندی شده را پایش کنند:

- **معیارهای سطح پایین هرم** :
  - ⌦ میانگین زمان شناسایی (MTTD) برای تهدیدات مبتنی بر هش/ IP
  - ⌦ میزان مثبت کاذب در تشخیص‌های مبتنی بر شاخص‌های سطح پایین
  - ⌦ طول عمر متوسط شاخص‌های سطح پایین قبل از منسوخ شدن
- **معیارهای سطح میانی هرم** :
  - ⌦ نسبت آرتیفکت‌های شناسایی شده به حوادث تأیید شده
  - ⌦ MTTD برای آرتیفکت‌های میزبان/شبکه
  - ⌦ توانایی همبستگی آرتیفکت‌ها با کمپین‌های تهدید شناخته‌شده
- **معیارهای سطح بالای هرم** :
  - ⌦ نرخ شناسایی TTP های جدید از طریق شکار تهدید
  - ⌦ زمان پایداری مهاجم در شبکه قبل از تشخیص (دوره سکونت)
  - ⌦ درصد حوادث شناسایی شده از طریق تشخیص‌های مبتنی بر TTP در مقابل شاخص‌های سطح پایین

مطالعه موردی جامع : یک بانک بزرگ ایرانی در سال ۱۴۰۱ پس از تجربه یک حادثه امنیتی، چارچوب هرم دشواری را به طور کامل پیاده‌سازی کرد. طی یک دوره ۱۸ ماهه، آنها دستاوردهای قابل توجهی را گزارش کردند:

- کاهش ۸۵٪ در میانگین زمان شناسایی تهدیدات (MTTD)
- کاهش ۶۷٪ در میانگین زمان پاسخ به تهدیدات (MTTR)
- کاهش ۹۰٪ در دوره سکونت متوسط مهاجمان در شبکه
- افزایش ۷۰٪ در نرخ شناسایی حملات در مراحل اولیه زنجیره کشتار

این موفقیت عمدتاً به دلیل تغییر تمرکز از تشخیص‌های مبتنی بر هش و IP به سمت تشخیص‌های مبتنی بر آرتیفکت، ابزار و TTP بود. تیم امنیتی بانک تخمین زد که هزینه‌های عملیاتی برای مهاجمان هدفمند حداقل ۴ برابر افزایش یافته است.

هرم دشواری در عصر تحول دیجیتال

چارچوب هرم دشواری باید با محیط‌های فناوری نوظهور سازگار شود:

- **در محیط‌های ابری:** محیط‌های ابری چالش‌ها و فرصت‌های جدیدی برای پیاده‌سازی هرم دشواری ایجاد می‌کنند
  - **چالش‌ها** :
    - ماهیت موقتی منابع باعث می‌شود آرتیفکت‌های میزبان سنتی کمتر پایدار باشند
    - پیچیدگی مدیریت هویت چند ابری تشخیص تاکتیک‌های دسترسی را دشوارتر می‌کند
    - معماری‌های بدون سرور ابزارهای تشخیص سنتی را محدود می‌کنند
  - **فرصت‌ها** :
    - APIهای ابری، لایه‌های جدیدی از آرتیفکت‌های تحلیلی ارائه می‌دهند
    - مقیاس‌پذیری ابری امکان تحلیل‌های پیچیده‌تر برای تشخیص TTP را فراهم می‌کند
    - امنیت تعریف‌شده با کد (IaC) امکان دفاع مبتنی بر قاعده را افزایش می‌دهد
  - **رویکرد سازگاری** : تیم‌های امنیتی باید هرم دشواری را با تمرکز بر آرتیفکت‌ها و TTPs خاص ابر بازتعریف کنند:
    - سطح ۴ (آرتیفکت‌ها): تمرکز بر رویدادهایAPI ، ناهنجاری‌هایCloudTrail ، و تغییراتIAM
    - سطح ۵ (ابزارها): شناسایی ابزارهای مختص ابر مانند ابزارهای استخراج اعتبارنامه محیط
    - سطح ۶ : (TTPs) مدل‌سازی تکنیک‌های خاص ابر مانند الگوهای افزایش امتیاز IAM یا حملات زنجیره تأمینCI/CD

مورد عملی : یک شرکت ارائه‌دهنده خدمات ابری داخلی در ایران، در سال ۱۴۰۲ یک چارچوب هرم دشواری سازگارشده با ابر را پیاده‌سازی کرد. آنها با تمرکز بر تشخیص الگوهای غیرعادی فراخوانی‌های API به جای شاخص‌های سنتی، توانستند یک کمپین نفوذ پیشرفته را شناسایی کنند که از الگوهای امتیاز افزایی در IAM استفاده می‌کرد و از تمام تشخیص‌های سنتی فرار می‌کرد.

- **در رویکردهای DevSecOps :** ادغام هرم دشواری با فرآیندهای DevSecOps ، امکان شناسایی و مقابله زودهنگام‌تر با تهدیدات را فراهم می‌کند
  - **دفاع Shift-Left Defense**
    - ⌦ ادغام تشخیص‌های آرتیفکت و ابزار در پایپ لاین CI/CD
    - ⌦ اسکن خودکار برای تکنیک‌های شناخته‌شده مهاجمان در کد و زیرساخت
    - ⌦ ایجاد محیط‌های امن با عدم دسترسی به منابع بر اساس الگوهای TTP شناخته‌شده
  - **ایمنی زنجیره تأمین نرم‌افزار** :
    - ⌦ اعمال تشخیص‌های هرم دشواری به فرآیند زنجیره تأمین نرم‌افزار
    - ⌦ تحلیل رفتاری بسته‌های وابسته برای شناسایی TTPs مشکوک
    - ⌦ مدل‌سازی تهدید مبتنی بر TTP برای اجزای حیاتی برنامه‌ها

مورد عملی :یک شـــرکت نرم‌افزاری فعال در حوزه انرژی، رویکرد DevSecOps خود را با هرم دشـــواری ادغام کرد. آنها توانسـتند با اجرای خودکار ابزارهای تشـخیص در CI/CD، یک کتابخانه آلوده شـده را که حاوی کد مخرب با الگوی مشـابه یک گروه APT شناخته‌شده بود، قبل از ورود به محیط تولید شناسایی کنند.

- **در راهبردهای Zero Trust** : هرم دشواری می‌تواند به تقویت معماری‌های Zero Trust کمک کند
  - **تشخیص پیشرفته نقض تأییدیه** :
    - ⌫ استفاده از تشخیص‌های مبتنی بر TTP برای شناسایی سوءاستفاده از اعتبارنامه‌های معتبر
    - ⌫ نظارت بر الگوهای دسترسی برای شناسایی رفتارهای غیرعادی حتی با اعتبارنامه‌های درست
    - ⌫ افزودن لایه‌های احراز هویت بر اساس الگوهای تهدید شناخته‌شده
  - **ارزیابی مداوم اعتماد** :
  - استفاده از شاخص‌های سطح بالای هرم برای تنظیم پویای سطوح اعتماد
  - تلفیق داده‌های هوشمندی تهدید با تصمیمات دسترسی در زمان واقعی
  - افزایش حساسیت نظارت برای سیستم‌هایی که نشانه‌های TTPs شناخته‌شده را نشان می‌دهند

مورد عملی :یک سازمان دولتی حساس در ایران، چارچوب Zero Trust خود را با الگوهای تشخیصی مبتنی بر TTP ترکیب کرد. این سـیسـتم با تحلیل الگوهای رفتاری کاربران، حتی با وجود داشـتن اعتبارنامه‌های معتبر، توانسـت چندین مورد سـازش حساب کاربری را شناسایی کند که از تمام لایه‌های سنتی احراز هویت عبور کرده بودند.

هرم دشواری برای گروه‌های مختلف تهدید

اثربخشی هرم دشواری بسته به سطح پیچیدگی و توانمندی مهاجمان متفاوت است:

- **برای تهدیدات عمومی (کرم‌ها، بدافزارهای عمومی)**
  - **سطوح مؤثر** : ۳-۱ (هش، IP، دامنه)
  - **دلیل** : این تهدیدات معمولاً تغییر کمتری در الگوهای خود دارند
  - **استراتژی** : تشخیص‌های مبتنی بر امضا همچنان مؤثر هستند
  - **چالش** : حجم بالای هشدارها و شاخص‌های مرتبط
- **برای مهاجمان سازمان‌یافته متوسط**
  - **سطوح مؤثر** :۵-۳ (دامنه، آرتیفکت، ابزارها)
  - **دلیل** : این گروه‌ها معمولاً زیرساخت و ابزارهای خود را تغییر می‌دهند اما TTPs آنها نسبتاً ثابت است
  - **استراتژی** : تمرکز بر تشخیص آرتیفکت‌ها و ابزارهای خاص این گروه‌ها
  - **چالش** : تمایز بین گروه‌های مختلف با ابزارهای مشابه
- **برای تهدیدات پیشرفته پایدار (APTs)**
  - **سطوح موثر:** ۶-۵ (ابزارها، TTPs)
  - **دلیل:**APT ها به سرعت زیرساخت را تغییر می‌دهند اما تغییر ابزارها و TTPs برای آنها پرهزینه است
  - **استراتژی** : تمرکز بر تشخیص رفتاری و الگوهای عملیاتی منحصربه‌فرد
  - **چالش** : پیچیدگی تشخیص و نیاز به دانش عمیق درباره هر گروه

مورد عملی تفاوت اثربخشی : مرکز ماهر در تحلیل یک حمله APT در سال ۱۴۰۱ به بخش انرژی کشور نشان داد که مهاجمان ۹ بار زیرساخت IP و دامنه (سطوح ۲-۳) خود را تغییر دادند، ۳ بار آرتیفکت‌های میزبان (سطح ۴) را اصلاح کردند، اما تنها یک بار ابزار اصلی خود (سطح ۵) را تغییر دادند و TTPs اصلی (سطح ۶) در طول کل کمپین ثابت ماند. این مشاهده تأیید می‌کند که سطوح بالای هرم برای مقابله با تهدیدات پیشرفته اثربخش‌تر هستند.

- **برای تهدیدات ناشناخته (Zero-Day)**
  - **سطوح مؤثر**: ۶-۴ (آرتیفکت، ابزارها، TTPs)
  - **دلیل** : حتی حملات کاملاً جدید معمولاً الگوهای رفتاری قابل تشخیصی دارند
  - **استراتژی** : تشخیص ناهنجاری و تحلیل رفتاری برای شناسایی رفتارهای غیرعادی
  - **چالش** : تنظیم حساسیت برای کاهش مثبت‌های کاذب

مورد عملی : یک سازمان مالی در ایران با استفاده از تشخیص رفتاری مبتنی بر TTP توانست یک بدافزار zero-day را قبل از شناسایی آن توسط هر محصول ضدبدافزار شناسایی کند. سیستم‌های آنها رفتار غیرعادی اجرای فرآیندها و دسترسی به فایل‌ها را شناسایی کردند که با الگوهای شناخته‌شده حرکت جانبی مطابقت داشت، حتی با وجود اینکه ابزار مورد استفاده کاملاً جدید بود.

نتیجه‌گیری

چارچوب هرم دشواری، دفاع سایبری را از یک پارادایم تشخیص دوگانه به یک مدل اختلال راهبردی مهاجم تبدیل می‌کند. با تمرکز عملیات امنیتی بر تشخیص و مقابله با شاخص‌های سطوح بالاتر به ویژه TTPs و ابزارهای مهاجمان سازمان‌ها می‌توانند هزینه عملیاتی حملات را به طور چشمگیری افزایش دهند و احتمالاً همه مهاجمان به جز مصمم‌ترین و با منابع کافی را دلسرد کنند.

مراکز عملیات امنیتی مدرن باید از این چارچوب برای ارزیابی سرمایه‌گذاری‌های دفاعی، اولویت‌بندی تلاش‌های مهندسی تشخیص و سنجش اثربخشی برنامه امنیتی از دیدگاه تأثیر بر مهاجمان به جای صرفاً معیارهای پوشش فنی استفاده کنند. همانطور که مهاجمان به تکامل ادامه می‌دهند، اصول راهبردی تجسم‌یافته در هرم دشواری، مزیتی پایدار با هدف قرار دادن پایدارترین و پرهزینه‌ترین عناصر عملیات مهاجم فراهم می‌کند.

معیار نهایی اثربخشی امنیتی نه در پیشگیری کامل، بلکه در تبدیل حملات موفق به اقداماتی با هزینه غیرقابل تحمل برای مهاجمان نهفته است—تبدیل امنیت از یک مسابقه تسلیحاتی فناورانه به یک رقابت اقتصادی پایداری عملیاتی.