

نام کتاب

شناسنامه

# فهرست مطالب

## فصل اول : قدرت شکار ..... 14

- 1-1- شکار تهدید چیست؟ ..... 15
- 2-1- شکار تهدید چه چیزهایی نیست؟ ..... 17
- 3-1- تهدیدات پیشرفته ..... 18
- 1-3-1- دشمنان و مهاجمین ..... 19
- 2-3-1- KILL CHAIN ..... 20
- 3-3-1- تضعیف کردن استحکامات و تجهیزات دفاعی ..... 22
- 4-1- شکاف در تشخیص نفوذ ..... 23
- 1-4-1- پویایی شکاف در تشخیص نفوذ ..... 24
- 5-1- مبانی شکار ..... 26
- 6-1- اقسام شکار تهدید ..... 29
- 1-6-1- شکار ساختار یافته ..... 29
- 2-6-1- شکار بدون ساختار ..... 30
- 7-1- فواید شکار ..... 31
- 8-1- تیم شکار ..... 32
- 9-1- تیم شکار به دنبال چه چیزی است ..... 34

## فصل دوم : فرآیند شکار ..... 36

- 1-2- مروری بر مدل بلوغ شکار ..... 37
- 2-2- مدل بلوغ شکار (HMM) ..... 38

38	1-2-2- مراحل مدل بلوغ شکار
42	2-2-2- اتوماسیون و مدل بلوغ شکار
43	3-2-2- استفاده از مدل بلوغ شکار
43	3-2- مروری بر چرخه شکار
44	4-2- بررسی چرخه شکار ENDGAME
46	1-4-2- مرحله ی مطالعه و بررسی
50	2-4-2- مرحله ی امن سازی
52	3-4-2- مرحله تشخیص
55	4-4-2- مرحله پاسخ
58	5-2- مروری بر چرخه شکار SQRRL
59	1-5-2- ایجاد فرضیه
59	2-5-2- بررسی و تحقیق از طریق ابزارها و تکنیک های مختلف
60	3-5-2- کشف TTP و الگو
61	4-5-2- تجزیه و تحلیل های خودکار

### 62..... فصل سوم : چالش های شکار

63	1-3- سرعت بخشیدن به شکار
65	2-3- ممکن ساختن تجزیه و تحلیل اتوماتیک
66	3-3- تکمیل تشخیص مبتنی بر SIGNATURE
67	4-3- پنهان سازی شکار از دشمنان

### 70..... فصل چهارم : آمادگی برای شکار

71	1-4- تعریف نقش ها و مسئولیت های شکار
71	1-1-4- مسئولیت ها و نقش های رایج
72	2-1-4- کارکنان عملیات های فناوری اطلاعات
72	3-1-4- تیم پاسخ دهی به حوادث
74	4-1-4- تیم امنیت
74	2-4- شکار چپان و تیم شکار
75	3-4- هدف گذاری شکار
76	1-3-4- گزارش ارزیابی ریسک سایبری

- 77 ..... 2-3-4- ایجاد سیاست
- 80 ..... 3-3-4- توسعه قوانین تعامل
- 81 ..... 4-4- ایجاد و نگهداری قابلیت های شکارچی
- 82 ..... 1-4-4- دانش امنیت
- 83 ..... 2-4-4- دانش فناوری اطلاعات
- 83 ..... 3-4-4- طرز فکر شکار
- 83 ..... 4-4-4- تصمیم گیری
- 84 ..... 5-4-4- مهارت های ارتباطی

### 85 ..... فصل پنجم : سازمان دهی شکار

- 86..... 1-5- برگزیدن یک چارچوب
- 87 ..... 1-1-5- چارچوب های سفارشی
- 88 ..... 2-5- سازمان دهی یک فرآیند شکار
- 89 ..... 1-2-5- مرحله اول : ارائه یک فرضیه
- 89 ..... 2-2-5- مرحله دوم: شناسایی شواهد برای اثبات فرضیه
- 90 ..... 3-2-5- مرحله سوم: توسعه تجزیه و تحلیل
- 91 ..... 4-2-5- مرحله چهارم: خودکار سازی یا اتوماسیون
- 91 ..... 5-2-5- مرحله پنجم: مستند سازی
- 92 ..... 6-2-5- مرحله ششم: ارتباط و گزارش
- 93 ..... 3-5- انتقال به پاسخ دهی حوادث
- 94 ..... 4-5- اندازه گیری شکار
- 94 ..... 1-4-5- آیا فرضیه اثبات می شود؟
- 95 ..... 2-4-5- شکار در یافتن مسائل چه اندازه مفید بوده است؟
- 96..... 3-4-5- تیم در فراهم ساختن امنیت تا چه اندازه موثر بوده است؟

### 98 ..... فصل ششم : تجربه ی شکار

- 99 ..... 1-6- سناریو شکار
- 100..... 2-6- آماده سازی
- 101..... 1-2-6- مشخص کردن اولویت های شکار
- 102..... 2-2-6- بررسی اطلاعات شبکه و دارایی های موجود فناوری اطلاعات

- 102.....3-2-6- فهمیدن این که چه چیزی به عنوان فعالیت عادی تلقی می شود
- 103.....4-2-6- پیکربندی و قرار دادن نرم افزار سنسور شکار
- 104.....3-6- تحقیق و بررسی
- 104.....1-3-6- هدف گذاری تحقیق
- 104.....2-3-6- پروسس ها و سرویس هایی که در حال حاضر در حال اجرا هستند
- 105.....3-3-6- سرویس ها یا پروسس هایی که اخیرا اجرا شده است
- 106.....4-3-6- پروسس ها یا سرویس هایی که برای اجرا شدن در آینده تنظیم شده اند
- 106.....5-3-6- جمع آوری و آنالیز اطلاعات
- 108.....6-3-6- گسترش تحقیقات
- 108.....7-3-6- اولویت بندی مجدد شکار
- 109.....4-6- حذف دشمن
- 112.....5-6- چکیده ی شکار
- 113.....6-6- گزارش شکار

### 115..... فصل هفتم : انتخاب فناوری شکار

- 116.....1-7- نهنکاری
- 117.....2-7- اتوماسیون
- 118.....3-7- پشتیبانی جریان کار
- 118.....4-7- یکپارچگی سازمانی
- 119.....5-7- مقیاس پذیری

مقدمه ناشر

## تقدیر و تشکر

سپاس خدای را که سخنوران، در ستودن او بمانند و شمارندگان، شمردن نعمت های او ندانند و کوشندگان، حق او را گزاردن نتوانند. و سلام و مورد بر محمد و خاندان پاک او، طاهران معصوم، هم آنان که وجودمان وامدار وجودشان است؛ و نفرین پیوسته بر دشمنان ایشان تا روز رستاخیز...

## تقدیم به

پدر و مادر عزیز و مهربانم

که در سختی ها و دشواری های زندگی همواره یآوری دلسوز و فداکار و پشتیبانی محکم و مطمئن برایم بوده اند.

با تشکر و سپاس از استاد دانشمند و پر مایه ام جناب آقای عادل کریمی که از محضر پر فیض ایشان ، بهره ها برده ام.



## پیشگفتار

کتابی که در حال حاضر پیش روی شماست بیانگر راهکارهای پیاده سازی و مدیریت شکار تهدید سایبری می باشد. در این کتاب سعی شده است تا مباحث مدیریتی که برای راه اندازی شکار تهدید در سازمان مورد نیاز است بصورت عملی ارائه گردد.

هدف ما در این کتاب برطرف کردن سوءتفاهمات در مورد مأموریت شکار و ارائه ی توصیه هایی برای ساختار بندی تیم شکار و بینش عملی برای استفاده از تکنیک های شکار می باشد که با استفاده از یک استراتژی مبتنی بر حمله، سازمان ها می توانند کنترل شبکه های خود را به دست بگیرند و از دارایی های بسیار مهم خود محافظت کنند.

شایان ذکر است در ترجمه این کتاب از منابعی همچون مقالات شرکت Endgame، Red Canary، FireEye، Sqrrl استفاده شده است، لازم به ذکر است در برخی بخش ها توضیحات بیشتر لحاظ کرده یا از جملات و کلمات دیگری برای ارائه مفهوم مورد نظر به شخص خواننده استفاده کرده ام، تا بتوانم حداکثر مطالب کتاب را به شخص خواننده منتقل کنم. با این حال مجموعه حاضر خالی از اشکال نمی باشد. لذا از تمام اساتید ارجمند، صاحب نظران و دانشجویان محترم استدعا دارم با نظرات و پیشنهادات خودشان من را راهنما باشند.

محمد قنبری

[www.linkedin.com/in/mghanbari7](http://www.linkedin.com/in/mghanbari7)

[mghanbari777@gmail.com](mailto:mghanbari777@gmail.com)

## مقدمه مولف

صرف نظر از بخش صنعتی، سازمان‌ها در سراسر جهان یک چالش مشترک را به اشتراک می‌گذارند: یافتن یک روش موثر برای شناسایی و اقدام سریع علیه تهدیدات سایبری. با در نظر گرفتن "dwell time" متوسط 150 روز، مهاجمین زمان زیادی برای برنامه ریزی و انجام سرقت مالکیت معنوی، اطلاعات مشتری و سایر اطلاعات ارزشمند دارند. به علاوه، با دسترسی آسان و ارزان به ابزارهای پیشرفته ی هک و سرویس‌های "اجاره یک هکر" از طریق دارک وب، مهاجمین هرساله نوع و تعداد حملات را افزایش داده‌اند. برای سخت‌تر کردن موفقیت مهاجمین نیاز داریم که از راه حل‌ها و تکنولوژی‌های جدید برای مقاوم سازی سازمان‌ها و دارایی‌های خود استفاده کنیم.

ابزارهای تشخیص حملات موجود در طول زمان از کار افتاده به نظر می‌رسند. آن‌ها برای این‌که کشف کنند چه اتفاقی افتاده است، از روش‌های Big Data کلاسیک مانند کشف یا جستجو در مجموعه‌ای از داده‌ها مانند (لاگ‌ها و ...) گذشته استفاده می‌کنند. زمانی که یک حمله موفقیت آمیز کشف می‌شود، آن‌ها قوانینی برای هدایت کشف وقوع حملات مشابه بعدی وضع می‌کنند. هدف این کار یادگیری از گذشته و پشتیبانی در برابر تلاش‌های آینده است. فقط یک مشکل وجود دارد: این‌که احتمالاً حملات بعدی متفاوت است.

سال‌ها است که ما (گروه‌های امنیتی) به خوبی با دشمنانی که به سیستم‌های سازمان ما حمله می‌کنند مبارزه کرده‌ایم. ما برای سیستم‌عامل‌ها و برنامه‌های کاربردی خود در سریع‌ترین زمان

ممکن وصله هایی را مورد استفاده قرار داده ایم. ما به آنتی ویروس ها، فایروال ها، سیستم های جلوگیری از نفوذ (IPS) و سایر ابزارها برای ممانعت از حمله متکی هستیم.

زمان آن است که بپذیریم رویکردهای متداول برای امنیت سازمان کافی نمی باشد. ما نیاز داریم که یک قدم به عقب بازگردیم و در فرضیات خود تجدید نظر کنیم. به جای آن که تمام تمرکزمان را بر روی امنیت reactive بگذاریم و برای یک هشدار منتظر بمانیم، باید یک رویکرد proactive برای امنیت استفاده کنیم و تلاش کنیم آن ها را پیدا کنیم و به سرعت از محیط خود حذف کنیم.

این به این معنی نیست که کنترل های امنیتی موجود را از بین ببریم، پیشگیری هنوز هم بسیار اهمیت دارد. اما به این معنی است که به منظور تشخیص دشمنان یا مهاجمین و حذف آن ها از شبکه هایمان باید بسیار بیشتر فعال بود. بهترین روش برای تغییر موقعیت از reactive به proactive، شکار می باشد که هدف این کتاب است.

من هر روزه در مورد شکار تهدید با سازمان ها صحبت می کنم. بعضی تصور می کنند که شکار تهدید استفاده از شاخص های شناخته شده ی آلودگی<sup>1</sup> یا IoC از فیدهای هوش تهدید<sup>2</sup> و جستجوی آن ها می باشد. اما با این حال خوب است که بدانید آیا نسبت به حملات کشف شده ی پیشین حساس هستید یا نه، این مانند این است که در حین رانندگی تنها به آینه ی عقب نگاه کنید.

همه ی ما می دانیم که حوادث سایبری اجتناب ناپذیر هستند. حال با این دانش چگونه عمل می کنیم؟ برای متوقف کردن یک نفوذ چگونه می توانیم متفاوت عمل کنیم؟ این صنعت نیازمند روش جدیدی است که به اندازه ی این تهدیدات و محیط سازمان ها پویا باشد. سازمان ها به دنبال روش هایی هستند که با تشخیص و مسدود کردن دشمنان پیش از وقوع آسیب، از رویداد های ناگوار و سانحه جلوگیری کنند. نگاه به آینه ی عقب و واکنش پس از اتفاق دیگر کافی نیست. متأسفانه راه حل

---

1 compromise

2 threat intelligence feed

های امنیتی به سرعت دشمنان و مهاجمین پیشرفت نکرده است. با این که تکنولوژی در زمان گیر افتاده است، صنعت با به کار بردن نام های جدید برای راه حل های منسوخ و آراستن اصطلاحات علمی ادامه می دهد.

شکار اغلب با قابلیت های جستجوی شاخص یا طبقه بندی لاگ های غنی شده اشتباه گرفته می شود ولی این تشخیص و حذف به صورت proactive، پنهانی و دقیق دشمنان و مهاجمین در شبکه بدون وجود شاخص های شناخته شده ی آلودگی می باشد. شکار یک استراتژی مبتنی بر حمله می باشد؛ شکارچی مانند مهاجم فکر می کند. اگر شما مهاجم بودید، چه چیز را با چه هدفی و چگونه مورد حمله قرار می دادید؟ مهاجمین یک ماموریت دارند. شکار باید بتواند این ماموریت را از مسیر خارج سازد.

شکار تهدید نسبتاً یک تخصص جدید به شمار می آید. با این وجود که خود این فعالیت جدید نیست، اما ابزارهای مخصوص شکار تهدید، مدل ها و بهترین روش ها در طی سال های اخیر توسعه یافته اند. اغلب ابهاماتی در مورد حوزه های این فعالیت وجود دارد همانطور که در مورد تمامی حوزه های تحقیقی جدید این ابهامات به وجود می آید. همانطور که رویکردهای متعارفی در مورد چگونگی انجام چنین فعالیت هایی وجود ندارد تعاریف خوبی نیز ارائه نشده است.

شکار می تواند تعادل را به نفع مدافعین تغییر دهد اما نیاز دارد که از حالت واکنشی به ذهنیت و نگرش مهاجمین تغییر کند. اگر شما دقیقاً ندانید که کدام یک از روش های مهاجمین را مسدود کنید نمیتوانید آلوده سازی و نفوذ را متوقف کنید. اکثر دشمنان و مهاجمین بدون توجه با اهدافشان باید توانایی دسترسی اولیه، تقویت امتیازات (escalate privileges)، سرقت credentialها، حرکت در تمام داریی ها، دور زدن استحکامات، تجهیزات دفاعی و پایداری<sup>3</sup> در شبکه ها را دارا باشند. تشخیص این ساختارها مولفه ی اصلی شکار است زیرا به شما می گوید که کجا شکار کنید. به جای تمرکز بر

---

3 Persistence

گذشته مانند بدافزارها یا شاخص های آلودگی که قبلا کشف شده است، سازمان ها می توانند شکار کنند و مانع تمام انواع تکنیک های مهاجمین شوند، به این معنی است که می توانند در مقابل تهدیدات ناشناخته به دفاع بپردازند. به علاوه، شکار سیستماتیک به سازمان اجازه می دهد که به سادگی به جمع آوری و آنالیز اطلاعات صحیح موجود در دارایی بپردازد تا بتواند فعالیت های مشکوک و مخرب را پیدا کند.