

معرفی هاردنت (Hardent)

اسلاید ۱ — عنوان

هاردنت (Hardent)

راهکار ارزیابی و بهبود مقاومت‌سازی برای کاهش سطح حمله در زیرساخت‌های سازمانی

زیرعنوان:

رویکردی پیشگیرانه برای ارتقای وضعیت امنیتی پیش از وقوع رخداد

نوت ارائه‌دهنده:

ارائه را با این پیام شروع کنید که هاردنت فقط یک ابزار فنی نیست؛ بلکه پاسخی به یک نیاز حاکمیتی و عملیاتی برای کاهش سطح حمله پیش از بهره‌برداری مهاجم است.

اسلاید ۲ — ابعاد تهدید

چرا این موضوع فوری است؟

بر اساس گزارش‌های معتبر بین‌المللی:

- میانگین هزینه جهانی هر رخداد نقض داده: ۴.۴۴ میلیون دلار
- تعداد حوادث امنیتی بررسی‌شده در سال ۲۰۲۴: ۲۲,۰۵۲ مورد
- تعداد نقض‌های داده تأییدشده: ۱۲,۱۹۵ مورد
- ۴۴٪ از نقض‌ها با باج‌افزار مرتبط بوده‌اند

پیام کلیدی:

رخداد سایبری دیگر یک احتمال دور نیست؛ یک هزینه قطعی و تکرارشونده برای سازمان‌های فاقد آمادگی است.

منابع:

IBM Cost of a Data Breach 2025, Verizon DBIR 2025

اسلاید ۳ — توزیع حملات و خسارات

مهاجمان بیشتر از چه مسیرهایی وارد می‌شوند؟

مطابق گزارش‌های بین‌المللی:

- ۷۰٪ موارد مرتبط با بهره‌برداری از آسیب‌پذیری‌ها
- ۴۴٪ از نقض‌ها مرتبط با باج‌افزار
- ۳۰٪ از داده‌های سرقت‌شده در لاگ‌های Infostealer شامل اعتبارنامه‌ها بوده‌اند

برداشت مدیریتی:

بخش بزرگی از تهدیدها از همان‌جا شروع می‌شود که با مقاومت‌سازی درست، قابل کاهش است:

- ضعف پیکربندی
- آسیب‌پذیری‌های اصلاح‌نشده
- دسترسی‌ها و اعتبارنامه‌های ناایمن

اسلاید ۴ — مسئله اصلی

مسئله چیست؟

بخش مهمی از نفوذها نه از حملات پیچیده، بلکه از **ضعف‌های پایه‌ای و قابل پیشگیری** آغاز می‌شود:

- تنظیمات ناایمن پیش فرض
- سرویس‌ها و پورت‌های غیرضروری
- وصله‌نشدن یا اصلاح‌نشدن ضعف‌ها
- نبود دید متمرکز از وضعیت امنیتی جاری

پیام کلیدی:

در بسیاری از سازمان‌ها، مقاومت‌سازی هنوز یک فعالیت دستی، پراکنده و غیریوسته است.

اسلاید ۵ — تعریف مقاومت‌سازی

مقاومت‌سازی چیست؟

مقاومت‌سازی، فرایند **کاهش سطح حمله** در سامانه‌ها، شبکه‌ها و سرویس‌ها از طریق حذف، محدودسازی یا اصلاح ضعف‌های قابل اجتناب است.

جایگاه در دفاع چندلایه:

- پیش از تشخیص
- پیش از پاسخ
- پیش از رخداد

پیام کلیدی:

مقاومت‌سازی یکی از **اولین و کم‌هزینه‌ترین لایه‌های دفاعی** در امنیت سایبری است.

نوت ارائه‌دهنده:

اگر لازم بود، تأکید کنید که مقاومت‌سازی صرفاً «بستن چند تنظیم» نیست؛ بلکه کاهش سیستماتیک احتمال موفقیت مهاجم است.

اسلاید ۶ — توجیه اقتصادی و ROI

چرا مقاومت‌سازی از نظر اقتصادی منطقی است؟

طبق گزارش IBM Cost of a Data Breach 2025:

- میانگین جهانی هزینه هر رخداد: **۴.۴۴ میلیون دلار**

و از منظر عملیاتی:

- هزینه اجرای مقاومت‌سازی در مقایسه با هزینه رخداد، به مراتب پایین‌تر است
- پیشگیری از ضعف‌های پایه‌ای، از **بالاترین ROI** در میان اقدامات امنیتی برخوردار است

پیام کلیدی:

عدم اجرای مقاومت‌سازی، صرفه‌جویی نیست؛ پذیرش یک ریسک پرهزینه است.

نوت ارائه‌دهنده:

اگر خواستید لحن را کمی بومی‌تر کنید، می‌توانید شفاهی بگویید:

«هزینه اجرا معمولاً در مقایسه با خسارات بالقوه، ناچیز است؛ اما هزینه عدم اجرا می‌تواند چندین برابر باشد.»

اسلاید ۷ — خلاً موجود در سازمان‌ها

وضعیت فعلی در بسیاری از محیط‌ها

در اغلب سازمان‌ها، مقاومت‌سازی به یکی از این شکل‌ها انجام می‌شود:

- چک‌لیست‌های دستی
- ارزیابی‌های مقطعی
- وابستگی به نیروی خبره محدود
- نبود دید یکپارچه از وضعیت میزبان‌ها
- نبود مسیر مشخص از کشف تا اقدام اصلاحی

نتیجه:

- خطای انسانی بالا
- کندی در اجرا
- ناپیوستگی در ارزیابی
- دشواری در گزارش‌دهی و پیگیری

اسلاید ۸ — معرفی هاردنت

هاردنت چیست؟

هاردنت یک راهکار متمرکز بر ارزیابی و بهبود وضعیت مقاومت‌سازی است که با رویکردی ساختاریافته، به سازمان کمک می‌کند:

- وضعیت امنیتی جاری را مشاهده کند
- نقاط ضعف قابل‌اصلاح را شناسایی کند
- فرایند مقاومت‌سازی را از حالت پراکنده و دستی خارج کند

پیام کلیدی:

هاردنت مقاومت‌سازی را از یک فعالیت موردی، به یک فرایند قابل‌مدیریت تبدیل می‌کند.

اسلاید ۹ — ارزش پیشنهادی هاردنت

ارزش پیشنهادی

هاردنت به سازمان‌ها کمک می‌کند:

- سطح حمله را پیش از سوءاستفاده کاهش دهند
- دید بهتری نسبت به وضعیت امنیتی جاری داشته باشند
- مقاومت‌سازی را ساختاریافته‌تر و قابل‌پیگیری‌تر اجرا کنند
- شکاف بین کشف ضعف و اقدام اصلاحی را کاهش دهند
- آمادگی بهتری برای محیط‌های حساس و الزامات حاکمیتی ایجاد کنند

افزوده پیشنهادی شما:

- هاردنت برای کاهش خطای تشخیص، از چندلایه کنترلی و راستی‌آزمایی در فرایند ارزیابی بهره می‌گیرد

نکته:

برای دفاع‌پذیری بیشتر، این عبارت را به‌صورت کیفی نگه داشته‌ایم و از بیان جزئیات اثبات نشده پرهیز کرده‌ایم.

اسلاید ۱۰ — معماری و رویکرد فنی

رویکرد معماری

بر اساس مستندات فنی، هاردنت از معماری لایه‌ای (Layered Architecture) بهره می‌برد.

برداشت کاربردی این معماری:

- تفکیک مسئولیت‌ها
- توسعه‌پذیری بهتر
- قابلیت سازمان‌دهی مناسب‌تر فرایند ارزیابی و اقدام
- امکان مدیریت ساختاریافته‌تر اجزای سامانه

افزوده پیشنهادی شما:

- در توسعه محصول، اصول کدنویسی امن و الزامات شناخته‌شده امنیت نرم‌افزار مدنظر قرار گرفته است

نکته:

چون در مستندات موجود شاهد صریح استانداردهای نام‌برده‌شده یافت نشده، بهتر است این گزاره در ارائه شفاهی نیز با لحن «مدنظر قرار گرفته / رعایت شده در فرایند توسعه» بیان شود، نه با ادعای استاندارد محور جزئی.

اسلاید ۱۱ — هاردنت چگونه کار می‌کند؟

جریان کاری هاردنت

بر اساس مستندات داخلی، هاردنت دارای اجزایی برای:

- **Discovery**: شناسایی و اکتشاف
- **Scan**: ارزیابی و اسکن
- **Security Current Status**: نمایش وضعیت امنیتی جاری
- هدایت کاربر در مسیر انتخاب و اجرای سناریوهای ارزیابی/اقدام

خروجی موردانتظار:

از دید سازمان، مقاومت‌سازی از «حدس و ارزیابی دستی» به «فرایند قابل‌مشاهده و قابل‌پیگیری» نزدیک می‌شود.

اسلاید ۱۲ — مقایسه با روش‌های سنتی

هاردنت در برابر رویکردهای سنتی

رویکرد	محدودیت اصلی
چک‌لیست دستی	زمان‌بر، خطا‌پذیر، وابسته به فرد
اسکن مقطعی	ناپیوسته و فاقد پیگیری ساختاریافته
اتکای صرف به نیروی خبره	مقیاس‌پذیری محدود
هاردنت	حرکت به سمت فرایند منظم کشف، ارزیابی و پیگیری

پیام کلیدی:

مزیت اصلی هاردنت، صرفاً «اسکن» نیست؛ بلکه نظم‌بخشی به چرخه مقاومت‌سازی است.

اسلاید ۱۳ — ملاحظات و پیشنهاد مسیر همکاری

ارزیابی قابل دفاع برای نهادهای حاکمیتی

بر اساس مستندات موجود:

- برخی قابلیت‌های کلیدی معماری و جریان کاری قابل مشاهده‌اند
- برای برخی ادعاهای جزئی‌تر، مستندات تکمیلی یا ارزیابی عملیاتی لازم است
- ارزیابی کنترل شده می‌تواند مبنای قضاوت دقیق‌تر درباره دقت، پوشش و بلوغ محصول باشد

مسیر پیشنهادی:

- (۱) ارزیابی آزمایشگاهی در سناریوهای کنترل شده
- (۲) سنجش دقت، پوشش و کاربردپذیری
- (۳) اجرای پایلوت محدود در محیط واقعی
- (۴) تحلیل نتایج و بهبود
- (۵) حرکت به سمت استفاده عملیاتی و سازمانی

اسلاید ۱۴ — جمع‌بندی و دعوت به اقدام

جمع‌بندی

- مقاومت‌سازی یکی از مهم‌ترین نقاط شروع دفاع سایبری است
- آمارهای جهانی نشان می‌دهند که هزینه رخدادهای بالاست و بسیاری از مسیرهای حمله، با اقدامات پیشگیرانه قابل کاهش‌اند
- هاردنت تلاش می‌کند مقاومت‌سازی را از یک فعالیت پراکنده، به یک فرایند ساختاریافته، قابل مشاهده و قابل پیگیری تبدیل کند

دعوت به اقدام

پیشنهاد می‌شود محصول در یک فاز ارزیابی کنترل شده بررسی شود تا امکان سنجش عملی ارزش آن برای محیط‌های حساس و دولتی فراهم گردد.

پایان‌بندی پیشنهادی شفاهی:

«هدف هاردنت، کاهش سطح حمله پیش از تبدیل شدن ضعف‌های پایه‌ای به رخدادهای پرهزینه است.»