معرفی راهکار نظارت بر شبکه Stealthwatch Cloud محصول شرکت سیسکو

معرفی راهکار نظارت بر شبکه Stealthwatch Cloud محصول شرکت سیسکو

Stealthwatch Cloud یک راهکار تشخیص و واکنش به تهدیدات سایبری شبکه بر اساس رویکرد نرم‌افزار است. شرکت Aspire Technology Partners در این مطلب از تجربیات خودش در زمینه استفاده از این محصول برای یکی از مشتریانی که در شرایطی سخت قرار داشت و یک بدافزار به کل شبکه آن نفوذ کرده بود، می‌گوید.

بدون وجود یک ابزار شناسایی و واکنش به تهدیدات سایبری مثل Stealthwatch Cloud مرکز عملیات امنیتی همیشه یک کار ثابت انجام می‌دهد. هر چند وجود راهکارهای حفاظت از امنیت محیط شبکه و کاربران نهایی آن مهم و حیاتی است اما کافی نیست چون عملکرد کلی آنها فقط شامل شناسایی بدافزارها و تفکیک سیستم‌های آلوده است در حالی که ممکن است شبکه همچنان در معرض خطر قرار داشته باشد. بدون نظارت کامل و داشتن دیدی جامع بر ترافیک رمزنگاری شده، احتمال اجرای حملات بعدی پس از ورود بدافزار به شبکه وجود دارد. اگر تیم امنیت سازمان شما قادر به تشخیص چگونگی نفوذ تهدیدات امنیتی به شبکه نباشد، بدافزار می‌تواند تا ماه‌ها یا حتی سال‌ها مخفی بماند.

مشتری شرکت Aspire Technology Partners از تیم واکنش به حادثه برای مقابله با تهدیدی که تصور می‌شد باج‌افزاری باشد که کل شبکه را در بر گرفته کمک گرفت. تیم واکنش به حوادث Aspire تصمیم به نصب سیستم Stealthwatch Cloud برای دنبال کردن بدافزار و ردپاهای آن در ترافیک شبکه گرفت. در ادامه دلایل اهمیت استفاده از سیستم Stealthwatch Cloud برای تشخیص و متوقف کردن این تهدید سایبری را مرور می‌کنیم:

امکان نصب به صورت تقریباً فوری

سیستم Stealthwatch Cloud تنها در عرض 2 ساعت روی شبکه خصوصی مشتریِ Aspire نصب شد. به این ترتیب امکان بررسی سریع شبکه جهت شناسایی

تهدید فراهم شد.

قابلیت تشخیص تهدیدات سایبری بر اساس رفتار آنها

Stealthwatch Cloud از شبکه به عنوان یک سنسور استفاده می‌کند و امکان تشخیص تهدیدات به صورت خودکار و همچنین جستجوی دستی تهدیدات سایبری را دارد. تیم واکنش به حوادث باید ردپاهای مهاجم را شناسایی می‌کرد و با وجود دید کاملی که توسط Stealthwatch Cloud فراهم شده، توانست تشخیص دهد که بدافزار از طریق یکی از تجهیزات آسیب‌پذیر به شبکه نفوذ کرده است. هیچ یک از راهکارهای امنیتی قادر به تشخیص این موضوع نبودند.

مجهز بودن به راهکارهای واکنش فوری

Stealthwatch Cloud امکان ادغام با انواع محصولات سیسکو و سایر شرکت‌ها را دارد. به این ترتیب کاربران می‌توانند یک مرحله جلوتر رفته و سیستم‌های سرتاسر سازمان را به هم متصل کنند و در صورت لزوم از ابزارهای دیگر برای انجام تحقیقات و کارهای دیگر استفاده کنند. هشدارهای این سیستم به همراه مشاهدات، در قالب گزارش هایی عرضه می‌شود که کاربران می‌توانند از آنها برای تحقیق بیشتر استفاده کنند.

پس همانطور که مشخص شد، حتی با وجود راهکارهای محافظت از شبکه و مبتنی بر Agent باز هم ممکن است شبکه شما در معرض خطر باشد. می‌توانید با استفاده از Stealthwatch Cloud این خلا را پر کرده و دیدی کامل نسبت به محیط شبکه خودتان به دست آورید.