آشنایی با معماری مرکز عملیات امنیت (SOC)

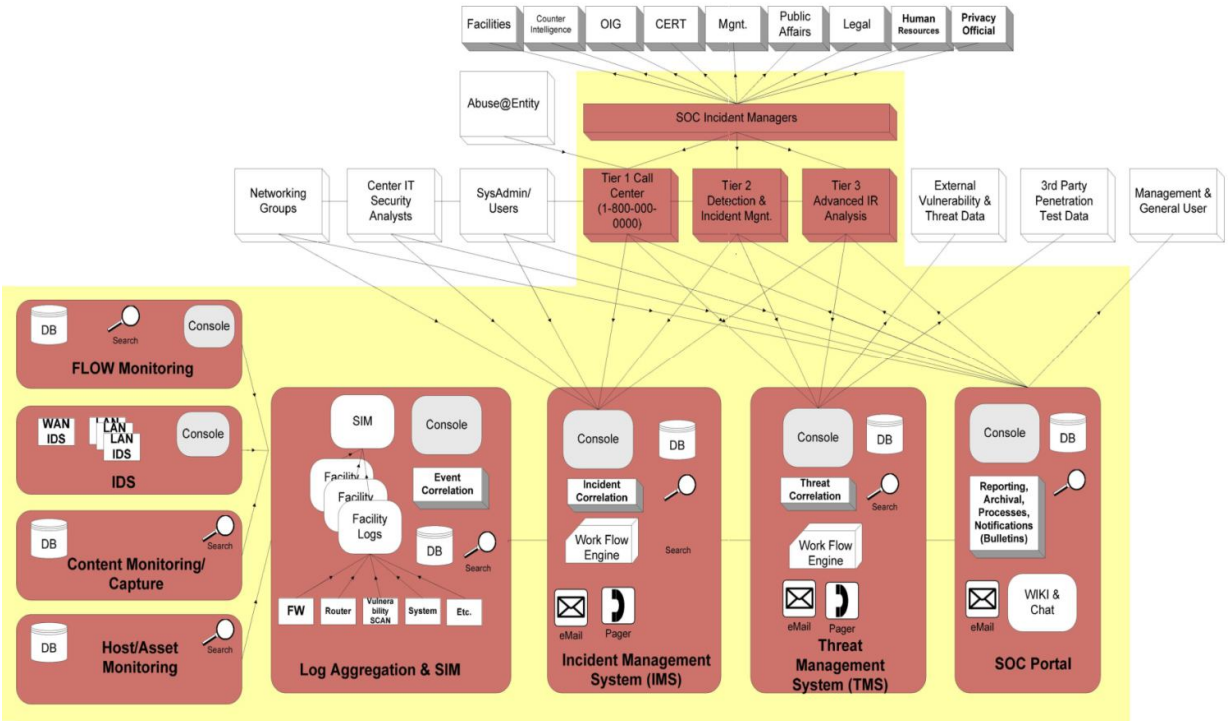
محمدامین صابریان

هر مرکز عملیات امنیت از سه لایه اصلی معرفی شده در زیر تشکیل شده است:

- لایه اول (مرکز تماس): نقطه تماس کاربران و مسئول پاسخ‌گویی به اخطارهای دریافتی از کاربران است. در این سطح به کلیه اخطارهایی که از پیچیدگی پایین‌تری برخوردارند، پاسخ داده می‌شود.
- لایه دوم (تحلیل اولیه): این سطح در حقیقت مکمل سطح یکم است و مسئول پاسخ‌گویی به مشکلات پیچیده‌تر در سیستم‌های امنیتی شبکه است. برای اخطارهایی که از اهمیت بالایی برخوردارند، سیستم‌های سطح دوم به‌طور کامل درگیر می‌شوند.
- لایه سوم (تحلیل تخصصی): در این سطح کارشناسان ارشد و مشاوران امنیتی شبکه قرار دارند. این سطح در حقیقت پشتیبان دو سطح پایین‌تر است. در صورتی که به اشکالات امنیتی در دو سطح پایین پاسخ داده نشود، کارشناسان و سیستم‌های این سطح، درگیر می‌شوند. کلیه تدابیر امنیتی و مدیریت امنیت شبکه، در این سطح اندیشیده می‌شود.

در هر یک از لایه‌های مطرح‌شده، ابزارهایی برای مدیریت سیستم‌های امنیتی در نظر گرفته می‌شود. این ابزارها، امنیت شبکه را از دو دیدگاه درون‌سازمانی و برون‌سازمانی مورد بررسی قرار می‌دهند. برای این منظور، هر مرکز عملیات امنیت دارای یک سری تجهیزات در داخل شبکه و یک سری تجهیزات در خود مرکز عملیات امنیت است و تمامی سرویس‌هایی که ارائه می‌شوند، مانیتور و مدیریت می‌شوند.

شکل زیر معماری کلان یک مرکز عملیات امنیت را نشان می‌دهد.



شکل 1 - معماری کلان مرکز عملیات امنیت

همان‌طور که در شکل مشاهده می‌شود، سیستم جمع‌آوری اطلاعات به‌عنوان زیرسیستم اولیه و اصلی مرکز عملیات امنیت اقدام به جمع‌آوری فایل‌های لاگ تجهیزات شبکه، سرورهای مهم سازمان و سامانه‌های اطلاعاتی مهم سازمان کرده و به‌علاوه، با سیستم‌های امنیتی سازمان مانند سیستم‌های تشخیص نفوذ، آنتی‌ویروس‌ها، ابزارهای مانیتورینگ گردش ترافیک و محتوا، ابزارهای مانیتورینگ دارایی‌های سازمان و میزبان‌ها در ارتباط است و اطلاعات جمع‌آوری شده را برای سیستم مدیریت

رویدادها ارسال می‌کند، سیستم مدیریت رویدادها، لاگ‌ها و اطلاعات خام دریافتی را بررسی نموده و موارد مشکوک را شناسایی کرده و ارتباط و همبستگی اطلاعات خام دریافتی را مورد بررسی قرار می‌دهد و رویدادها که بیانگر موارد منفی و غیرمطلوب هستند را استخراج می‌کند و علاوه بر آن مدیران سیستم‌ها و متخصصین امنیت و شبکه سازمان نیز در صورت برخورد با یک رویداد امنیتی، می‌توانند از طریق کنسول ارتباطی سیستم مدیریت رویداد؛ اطلاعات مربوط به رویداد را در سیستم ذخیره کنند. متخصصین فعال در لایه دو و لایه سه مرکز عملیات امنیت، رویدادهای شناسایی شده را مورد بررسی قرار داده و در صورت صحت رویداد، اطلاعات هر رویداد را به‌عنوان یک بلیط جدید در سیستم Service Desk تعریف می‌کنند، بلیط مربوط به هر رویداد تا زمان پاسخ، برخورد و نابودسازی عوامل رویداد باز خواهد ماند و بعد از آن بسته خواهد شد.

سیستم مدیریت تهدیدات با توجه به رویدادهای شناسایی شده، اقدام به استخراج تهدیدات و آسیب‌پذیری‌های موجود در دارایی‌ها که منجر به وقوع رویداد مورد نظر شده است می‌پردازد و نتایج نهایی مربوط به تهدیدات، آسیب‌پذیری‌ها و رویدادها از طریق پورتال در قالب داشبوردهای مدیریتی و نیز گزارش‌های Drill Down ارائه می‌شود.

در ادامه هر یک از بخش‌های اصلی مرکز عملیات امنیت به‌صورت جزئی‌تر توصیف شده‌اند.

1-1- سیستم جمع‌آوری لاگ‌ها

سیستم جمع‌آوری لاگ‌ها، مسئولیت جمع‌آوری لاگ‌های تجهیزات مختلفی مانند فایروال‌ها، روترها، سوییچ‌ها، سرورها و سرویس‌های حساس سازمان و نیز سیستم‌های اطلاعاتی برجسته سازمان را بر عهده داشته و بخشی از اطلاعات اولیه خود را از سیستم‌های تشخیص نفوذ، آنتی‌ویروس‌ها، سیستم مانیتورینگ گردش کار، مانیتورینگ محتوا و میزبان‌ها به‌دست می‌آورد؛ این سیستم مسئولیت جمع‌آوری داده‌های خام اولیه جهت تحلیل توسط واحد سیستم مدیریت رویداد را بر عهده دارد.

1-2- سیستم مدیریت رویداد

سیستم مدیریت رویداد، مسئولیت شناسایی رویدادها (incident) را با توجه به وقایع (log) شناسایی شده توسط سیستم مدیریت لاگ و نیز با توجه به گزارش‌های دریافتی از مدیران سیستم‌ها، مدیران شبکه و متخصصین امنیت، بر عهده دارد و رویدادهای شناسایی شده را در جهت تشخیص تهدید به واحد مدیریت تهدیدها (TMS) ارسال می‌کند. سیستم مدیریت رویداد باید قابلیت شناسایی ارتباط رویدادهای مختلف و نیز قابلیت بررسی ارتباط رویداد و سوابق رویدادهای قبلی ثبت شده را داشته باشد.

سیستم مدیریت رویداد باید مجهز به Service Desk، جهت ثبت رویدادها باشد؛ کاربران مرکز عملیات امنیت در ارتباط نزدیک با سیستم مدیریت رویـداد بوده و بعد از اطمینان از حقیقی بودن یک رویداد اطلاعات مربوط به آن‌را به‌صورت بلیط در Service Desk یا Help Desk ثبت می‌کنند؛ بلیط مربوط به هر رویداد تا زمان پاسخ مطلوب، برخورد یا ریشه‌کن کردن عوامل موثر در رویداد، باز خواهند ماند.

در ادامه وظایف سیستم مدیریت رویداد ارائه شده است:

- مانیتورینگ مداوم وضعیت عامل رویداد[1] و چرخه حیات کلی مدیریت وقایع و مسیریابی
- به اشتراک‌گذاری داده رویداد، همبستگی، وابستگی و تحلیل آن
- بهبود میزان تاثیر، گردش کار خودکار، اطلاع‌رسانی و گزارش‌دهی
- کنترل دسترسی مبتنی بر نقش
- تشخیص ناهنجاری و پیامدهای آن
- تحلیل علت ریشه‌ای
- استفاده از پایگاه داده قابل جستجو
- رساندن داده خام تهدید به سیستم مدیریت تهدیدات

1-3- سیستم مدیریت تهدیدات

1- Incident

بعد از شناسایی رویداد توسط سیستم مدیریت رویداد، سیستم مدیریت تهدیدات، باید آسیب‌پذیری‌ها و تهدیدهای مرتبط با هر رویداد را شناسایی کند، به این منظور در مرحله اول سیستم باید پایگاه داده خود را بررسی کرده و در صورت عدم تشخیص تهدید و آسیب‌پذیری مربوط به هر رویداد، سیستم باید قابلیت ارتباط با پایگاه‌داده‌های آسیب‌پذیری بیرونی را نیز داشته باشد و اقدام به شناسایی تهدیدها و عامل آسیب‌پذیریی که منجر به بروز رویداد شده است، شود. سیستم باید قابلیت شناسایی ارتباط تهدیدهای مختلف و نیز ارتباط تهدید با تهدیدهای قبلی شناسایی شده را نیز داشته باشد. پایگاه داده تهدیدها و آسیب‌پذیری‌ها باید به‌صورت آنلاین و آفلاین قابلیت به‌روز رسانی را داشته باشد.

قابلیت‌ها و ویژگی‌های سیستم مدیریت تهدیدها عبارتند از:

- جمع‌آوری اطلاعات مربوط به تهدیدها از طریق رویدادها، منابع خارجی (تجاری، عمومی و ...)، همکاران و ...
- سازماندهی و تعیین اطلاعات مرتبط با هم
- تحلیل ارتباط اطلاعات به عامل‌ها
- تعیین نیازها و مسیر حرکت
- اجرای عملیات‌هایی مانند: بلاک، نگهبانی و ...
- ارزیابی نتایج
- استفاده از پایگاه داده به‌منظور ارزیابی رویدادهای جدید
- ارائه هشدار و اخطار
- یکپارچه‌سازی مدیریت تهدیدات، فراهم‌سازی فرایند مدیریت تهدیدهای قابل تکرار و پایدار
- پشتیبانی از پایگاه داده متمرکز و ساختار یافته تهدیدها، ضبط آسیب‌پذیری‌ها، کدهای بدخواه و وصله‌هایی که باعث تغییر تکنولوژی‌ها و فرایندهای بحرانی می‌شوند. پشتیبانی از مخزن متمرکز برای داده تهدیدها و آسیب‌پذیری‌ها از طریق منابع مطمئن با استفاده از یک پایگاه داده منطبق با استاندارد و قابل جستجو
- ارائه محتوای تهدیدها، اطلاعات مربوط به داده تهدید که از طریق تحقیقات داخلی آژانس‌های مربوطه سفارشی شده‌اند، محتوای مربوط به یک تهدید تجاری آماده شده و مشاوره تهدید از طریق ایمیل ارائه می‌شود.
- تحلیل و اصلاح داده تهدید، تحلیل و عکس‌العمل در مقابل آسیب‌پذیری‌ها و کد بدخواه
- هشداردهی به کاربران در مورد تهدیدهای پدیدار شده، اخطار خودکار به پرسنل مسئول باعث می‌شود که آنها بتوانند تهدیدهای پدیدار شده را شناسایی و از آنها پیش‌گیری کنند.
- گزارش در زمینه سطح تهدید و فعالیت‌های آن، تولید گزارش‌های زمان اجرا و ارائه داشبوردهای مخصوص کاربر به‌منظور مشاهده تکنولوژی، استحکام، نوع و تاثیر تهدید بر سازمان هدف
- اعتبارسنجی آسیب‌پذیری درمان شده، گزارش‌گیری از فعالیت‌های مرتبط با برخورد با تهدید

به‌طور کلی روش عملکرد سیستم مدیریت تهدید در ادامه توصیف شده است:

در ابتدا وقایع (events) مرتبط با عملیات با توجه به فایل‌های لاگ مربوط به سیستم‌های هدف مورد کنترل، استخراج شده و از درون وقایع، رویدادها (Incidents) استخراج می‌شوند؛ رویدادها وقایعی هستند که بار منفی داشته و خرابی به‌دنبال دارند. توسط سیستم مدیریت رویداد، رویدادها با توجه به پایگاه داده رویدادهای موجود، مورد تحلیل قرار می‌گیرند و سپس تهدیدهای مربوط به هر رویداد توسط سیستم مدیریت تهدیدات شناسایی می‌شوند.

4-1- پورتال مرکز عملیات امنیت

پورتال محل ارائه گزارش‌های مدیریتی و محل ارائه نتایج تحلیلی رویدادها است. همچنین گروه‌های کاربری شبکه و مدیران سیستم‌ها می‌توانند اخبار و اطلاعات امنیتی را از طریق پورتال، اطلاع‌رسانی کنند. پورتال داده‌ها و اطلاعات خود را از سیستم مدیریت تهدیدها، سیستم مدیریت رویداد، سیستم مدیریت وقایع، مدیران سیستم‌ها، تحلیلگران مرکز امنیت فناوری اطلاعات و گروه‌های شبکه دریافت می‌کند و به گزارش‌های مدیریتی و قابل استفاده در اختیار مدیریت و کاربران عمومی و کاربران فعال در سه لایه اصلی مرکز عملیات امنیت قرار می‌دهد؛ کاربران فعال در سه سطح مرکز عملیات امنیت با توجه به اطلاعات دریافتی از پورتال، علاوه بر پاسخ‌گویی به درخواست‌های مشاوره و حل مشکلات اولیه، دیدگاه خود در مانیتور کردن وقایع را نیز اصلاح می‌کنند.