Junior Security Analyst IntroHelp

Link: https://tryhackme.com/room/jrsecanalystintrouxo

-Đế Tọa-

I. Over view

Trong vai trò Junior Security Analyst, bạn sẽ là Triage Specialist. Bạn sẽ dành nhiều thời gian để phân loại hoặc theo dõi nhật ký sự kiện và cảnh báo.

Trách nhiệm của Junior Security Analyst hoặcTier 1 SOC Analyst bao gồm:

- Giám sát và điều tra các cảnh báo (hầu hết thời gian, đó là môi trường hoạt động SOC

  24x7)
- Cấu hình và quản lý các công cụ bảo mật
- Phát triển và triển khai các chữ ký IDS (Hệ thống phát hiện xâm nhập) cơ bản
- Tham gia các nhóm công tác SOC, các cuộc họp
- Tạo yêu cầu và báo cáo sự cố bảo mật lên Cấp 2 và Trưởng nhóm nếu cần

Yêu cầu bằng cấp (phổ biến nhất):

- 0-2 năm kinh nghiệm về Hoạt động An ninh

- Hiểu biết cơ bản về Mạng (Mô hình OSI (Mô hình kết nối hệ thống mở) hoặc mô hình TCP/IP (Giao thức điều khiển truyền/Mô hình giao thức Internet)), Hệ điều hành (Windows, Linux), Ứng dụng web. Để tìm hiểu thêm về các mô hình OSI và TCP/IP.
- Kỹ năng viết kịch bản/lập trình là một lợi thế

Chứng chỉ mong muốn:

- Bảo mật CompTIA+

Khi bạn tiến bộ và nâng cao kỹ năng của mình với tư cách là Junior Security Analyst, cuối cùng bạn sẽ chuyển lên Tier 2 và Tier 3.

Tổng quan về Mô hình ba tầng của Trung tâm điều hành an ninh (SOC):

II. What is SOC

Chức năng cốt lõi của SOC (Trung tâm điều hành an ninh) là điều tra, giám sát, ngăn chặn và ứng phó với các mối đe dọa trong lĩnh vực mạng 24/7 hoặc suốt ngày đêm. Theo định nghĩa của McAfee về SOC , " Các nhóm vận hành bảo mật chịu trách nhiệm giám sát và bảo vệ nhiều tài sản, chẳng hạn như sở hữu trí tuệ, dữ liệu nhân sự, hệ thống kinh doanh và tính toàn vẹn của thương hiệu. Là thành phần triển khai của khuôn khổ an ninh mạng tổng thể của tổ chức, các hoạt động bảo mật các nhóm đóng

vai trò là điểm cộng tác trung tâm trong các nỗ lực phối hợp nhằm giám sát, đánh giá và bảo vệ chống lại các cuộc tấn công mạng". Số lượng người làm việc trong SOC có thể khác nhau tùy thuộc vào quy mô của tổ chức.

Trách nhiệm của SOC bao gồm những gì?

Chuẩn bị và phòng ngừa

Với tư cách là SOC tier 1, bạn nên cập nhật thông tin về các mối đe dọa an ninh mạng hiện tại (Twitter và Feedly có thể là những nguồn tài nguyên tuyệt vời để cập nhật tin tức liên quan đến An ninh mạng). Điều quan trọng là phát hiện và truy lùng các mối đe dọa, xây dựng lộ trình bảo mật để bảo vệ tổ chức và sẵn sàng cho tình huống xấu nhất.

Các phương pháp phòng ngừa bao gồm thu thập dữ liệu tình báo về các mối đe dọa mới nhất, các tác nhân đe dọa và TTP của chúng (Chiến thuật, Kỹ thuật và Quy trình) . Nó cũng bao gồm các quy trình bảo trì như cập nhật chữ ký tường lửa, vá các lỗ hổng trong hệ thống hiện có, các ứng dụng danh sách chặn và danh sách an toàn, địa chỉ email và IP.

Để hiểu rõ hơn về TTP, bạn nên xem xét một trong các cảnh báo của CISA (Cơ quan an ninh mạng & cơ sở hạ tầng) về APT40 (Mối đe dọa liên tục nâng cao của Trung Quốc). Hãy tham khảo liên kết sau để biết thêm thông tin, https://us-cert.cisa.gov/ncas/alerts/aa21-200a .

Giám sát và điều tra

Nhóm SOC chủ động sử dụng các công cụ SIEM (Quản lý sự kiện và thông tin bảo mật) và EDR (Phát hiện và phản hồi điểm cuối) để giám sát các hoạt động mạng đáng ngờ và độc hại. Với tư cách là Nhà phân tích bảo mật, bạn sẽ học cách ưu tiên các cảnh báo dựa trên cấp độ của chúng: Thấp, Trung bình, Cao và Quan trọng. Tất nhiên, có thể dễ dàng đoán được rằng bạn sẽ cần phải bắt đầu từ cấp cao nhất (Quan trọng) và tiến dần xuống phía dưới - Cảnh báo cấp thấp. Việc trang bị sẵn các công cụ giám sát bảo mật được cấu hình đúng cách sẽ mang đến cho bạn cơ hội tốt nhất để giảm thiểu mối đe dọa.

Các nhà phân tích bảo mật cấp dưới đóng một vai trò quan trọng trong thủ tục điều tra. Họ thực hiện phân loại các cảnh báo đang diễn ra bằng cách khám phá và hiểu cách hoạt động của một cuộc tấn công nhất định và ngăn chặn những điều xấu xảy ra nếu có thể. Trong quá trình điều tra, điều quan trọng là phải đặt ra câu hỏi "Như thế nào? Khi nào và tại sao?". Các nhà phân tích bảo mật tìm ra câu trả lời bằng cách đi sâu vào nhật ký dữ liệu và cảnh báo kết hợp với việc sử dụng các công cụ nguồn mở mà chúng ta sẽ có cơ hội khám phá sau trong lộ trình này.

Response

Sau khi điều tra, nhóm SOC sẽ điều phối và thực hiện hành động đối với các máy chủ bị xâm nhập, bao gồm việc cách ly các máy chủ khỏi mạng, chấm dứt các quy trình độc hại, xóa tệp, v.v.

III. A day In the life of a Junior (Associate) Security Analyst

Question and Answer

What was the malicious IP address in the alerts?

221.181.185.159

To whom did you escalate the event associated with the malicious IP address?

Will Griffin

After blocking the malicious IP address on the firewall, what message did the malicious actor leave for you?

THM{UNTIL-WE-MEET-AGAIN}