Số và ký hiệu: 1795/TB-VCS-TCHC
Ngày ban hành: 09/10/2021

TẬP ĐOÀN CÔNG NGHIỆP-VIỄN THÔNG QUÂN ĐỘI
**CÔNG TY AN NINH MẠNG VIETTEL**

**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
**Độc lập - Tự do - Hạnh phúc**
*Hà Nội, ngày tháng năm 2021*

# PHỤ LỤC: BẢNG PHÂN BẬC KỸ SƯ, LỘ TRÌNH NGHỀ NGHIỆP VÀ CHI TIẾT VỀ PHÂN BẬC NGHỀ

| | | | | |
|---|---|---|---|---|
| **Tên chức danh** | **Tối ưu ATTT - Content** | | | |
| **Nghề** | **An toàn thông tin (002)** | | | |
| **Các level và bậc HRL** | Junior Content<br>Experienced Content<br>Senior Content<br>Expert Content | | | |
| **Tóm tắt về vị trí công việc** | Mục tiêu chính:<br>- Xây dựng bổ sung rule, usecase phát hiện các kỹ thuật tấn công mới, các yêu cầu giám sát của KH<br>- Tối ưu các rule, usecase không đạt tiêu chuẩn chất lượng<br>- Xây dựng các Automation Playbook để tự động hóa công tác vận hành ATTT | | | |
| **Lộ trình** | **Junior** → | **Experienced** → | **Senior** → | **Expert** |
| **Nội dung** | **Các level** | | | |
| | **Junior Content** | **Experienced Content** | **Senior Content** | **Expert Content** |
| **A. Tiêu chí phân bậc** | | | | |
| **Kiến thức chuyên môn** | **Kiến thức:**<br>- Có kiến thức cơ bản về CNTT ở bậc đại học trở lên hoặc được đánh giá tương đương (Vượt qua bài kiểm tra kiến thức CNTT cơ bản, điểm >= 5)<br>- Có kiến thức cơ bản về ATTT & các phương thức tấn công mạng (có chứng chỉ CEH, Security +) hoặc được đánh giá tương đương (Vượt qua khóa đào tạo CEH, điểm trung bình các bài lab & bài test trắc nghiệm cuối khóa >= 5) | **Kiến thức:**<br>Như level Junior và:<br>- Nắm bắt, am hiểu sâu về các Data Source phổ biến, hiểu rõ mối liên kết giữa các loại Data Source | **Kiến thức:**<br>Như level Experienced và:<br>- Có chứng chỉ nâng cao về hacking technique (OSCP) hoặc được đánh giá tương đương (Tấn công & chiếm quyền điều khiển >= 50 máy tính trên 4 Network Zone trong hệ thống PWK Lab của OSCP, không sử dụng các công cụ dạng Automatic Exploitation (như SQLmap, Metasploit, ...)).<br>- Nắm bắt, am hiểu các chuẩn detection rule phổ biến trên thế giới (Suricata rule, YARA rule, WAF rule)<br>- Kiến thức cơ bản về Machine Learning | **Kiến thức:**<br>Như level Senior |
| **Kỹ năng chuyên môn** | - Sử dụng thành thạo công cụ viết rule trên SIEM Correlation | Như level Junior và:<br>- Sử dụng thành thạo công cụ tạo Playbook của giải pháp SOAR | Như level Experienced và:<br>- Kỹ năng nghiên cứu<br>- Sử dụng thành thạo portal hệ thống KIAN, iML<br>- Kỹ năng nâng cao về hacking technique | **Kỹ năng:**<br>Như level Senior |
| **Kỹ năng mềm** | - Tập trung vào chi tiết và chất lượng | Như level Junior và:<br>- Nhiệt tình và tích cực | Như level Experienced và:<br>- Liên tục học hỏi<br>- Khả năng chủ động | Như level Senior và:<br>- Kỹ năng giao tiếp, lãnh đạo nhóm<br>- Kỹ năng giao tiếp, lãnh đạo nhóm<br>- Kỹ năng Mentor |
| **Khoá học, Chứng chỉ** | **Khoá học:**<br>*Must:*<br>- CEH nội bộ<br>- OSCP nội bộ<br>*Should:*<br>#N/A<br>*Nice:*<br>#N/A<br><br>**Chứng chỉ:**<br>*Must:*<br>Chứng chỉ nội bộ CEH và OSCP<br>*Should:*<br>- CEH, OSCP<br>*Nice:*<br>#N/A | **Khoá học:**<br>*Must:*<br>- CEH nội bộ<br>- OSCP nội bộ<br>*Should:*<br>#N/A<br>*Nice:*<br>#N/A<br><br>**Chứng chỉ:**<br>*Must:*<br>Chứng chỉ nội bộ CEH và OSCP<br>*Should:*<br>- CEH, OSCP<br>*Nice:*<br>#N/A | **Khoá học:**<br>*Must:*<br>- CEH nội bộ<br>- OSCP nội bộ<br>*Should:*<br>#N/A<br>*Nice:*<br>#N/A<br><br>**Chứng chỉ:**<br>*Must:*<br>Chứng chỉ nội bộ CEH và OSCP<br>*Should:*<br>- CEH, OSCP<br>*Nice:*<br>#N/A | **Khoá học:**<br>*Must:*<br>- CEH nội bộ<br>- OSCP nội bộ<br>*Should:*<br>#N/A<br>*Nice:*<br>#N/A<br><br>**Chứng chỉ:**<br>*Must:*<br>Chứng chỉ nội bộ CEH và OSCP<br>*Should:*<br>- CEH, OSCP<br>*Nice:*<br>#N/A |
| **Kinh nghiệm** | Không yêu cầu kinh nghiệm | - Có kinh nghiệm làm công tác Content trên 1 năm. | - Có kinh nghiệm làm công tác Content trên 3 năm | - Có kinh nghiệm làm công tác Content trên 5 năm<br>- Dẫn dắt, lead team Content Analyst thực hiện tốt các nhiệm vụ trong 3 năm liên tiếp, được team đánh giá tốt, kết quả tốt được BGĐ ghi nhận<br>- Chủ trì ít nhất 2 dự án/nghiên cứu chuyên sâu về Detection |

| | | | | |
|---|---|---|---|---|
| **Nhiệm vụ** | - Xây dựng bổ sung rule phát hiện các kỹ thuật tấn công mới (mức cơ bản: rule bắt theo pattern trên 1 loại data source), các yêu cầu giám sát của KH<br>- Tối ưu các rule (mức cơ bản: rule bắt theo pattern trên 1 loại event) không đạt tiêu chuẩn chất lượng | Như JUNIOR và:<br>- Xây dựng bổ sung rule phát hiện các kỹ thuật tấn công mới (mức phức tạp: rule tương quan giữa các loại data source)<br>- Tối ưu các rule (mức phức tạp: rule tương quan giữa các loại data source) không đạt tiêu chuẩn chất lượng<br>- Xây dựng các Automation Playbook để tự động hóa công tác vận hành ATTT | Như EXPERIENCED và:<br>- Xây dựng bổ sung usecase (KIAN, iML), Suricata rule, YARA rule, WAF rule phát hiện các kỹ thuật tấn công mới, lỗ hổng mới cho VCS_ATT&CK<br>- Tối ưu các usecase (KIAN, iML), Suricata rule, YARA rule, WAF rule không đạt tiêu chuẩn chất lượng<br>- Nghiên cứu công nghệ mới phục vụ bài toán phát hiện tấn công ATTT.<br>- Nghiên cứu phương án phát hiện đối với kỹ thuật, lỗ hổng, công cụ mới của các nhóm tấn công APT | Như SENIOR và:<br>- Dẫn dắt, lead chuyên môn về mảng Content, định hướng các phương pháp mới để tăng khả năng Detection<br>- Xây dựng, tổ chức đào tạo chuyên môn nghiệp vụ nâng cao chất lượng cho nội bộ và khách hàng. |