|  |  |
| --- | --- |
| TẬP ĐOÀN CÔNG NGHIỆP - VIỄN THÔNG QUÂN ĐỘI  **CÔNG TY TNHH MTV AN NINH MẠNG VIETTEL**  Số: /BC-VCS | **CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM**  **Độc lập - Tự do - Hạnh phúc**  *Hà Nội, ngày tháng năm 2025* |

|  |
| --- |
| **BÁO CÁO**  **Các vấn đề An toàn thông tin trong quá trình cung cấp dịch vụ của Công ty TNHH MTV An ninh mạng Viettel cho {{name\_company}} (từ ngày {{from}} đến hết ngày {{to}})** |

Kính gửi: {{name\_company}}

Căn cứ thỏa thuận về việc Công ty TNHH MTV An ninh mạng Viettel (VCS) cung cấp Dịch vụ An toàn thông tin cho {{name\_company}}({{sc\_name\_company}}), VCS kính gửi báo cáo tổng hợp định kỳ các vấn đề An toàn thông tin (ATTT) trong quá trình cung cấp dịch vụ, kết quả cụ thể như sau:

1. **Thông tin sự cố**

* *{{incident}}*

1. **Thông tin cảnh báo**

- Trên hệ thống giám sát ATTT tại *VPTWĐ* ghi nhận {{ total\_num\_alerts}} cảnh báo vào các hệ thống máy chủ, máy tính người dùng. VCS đã thực hiện phân loại, đánh giá các cảnh báo và tạo 4 ticket gán cho *VPTWĐ* xác minh hành vi, nghiệp vụ.

* Thống kê số lượng cảnh báo theo giải pháp:

| **STT** | **Giải pháp** | **Số lượng cảnh báo** |
| --- | --- | --- |
|  | CyM Agent | {{num\_alerts\_siem}} |
|  | Network Security Mornitoring | {{num\_alert\_NSM}} |
|  | Endpoint Detection & Response | {{num\_alert\_EDR}} |

* Thống kê cảnh báo theo hình thức tấn công như sau:

1. **Thông tin vận hành**

| **Nhóm vận hành** | **Chỉ tiêu SLA** | **KPI** |
| --- | --- | --- |
| Tier 1 - VCS | 90% | 100% (135 / {{ total\_num\_alerts}}) |
| Tier 2 - {{tenant}} | 90% | 100% (3 / {{ total\_num\_tickets}}) |
| Tier 3 - VCS | 90% | 100% (2 / {{ total\_num\_cases}}) |

* {{kpi\_comparison\_and\_comments}}

1. **Về việc triển khai đầy đủ các giải pháp ATTT**

Dưới đây là thông tin hoạt động của các giải pháp giám sát ATTT của VCS đang triển khai cho {{tenant}}:

| **STT** | **Giải pháp** | **Độ phủ** | **Hiện trạng** |
| --- | --- | --- | --- |
|  | Network Security Monitoring (NSM) | 02/02 sensor:  Vptwdang  vptwdanghlc | Các sensor đang hoạt động giám sát bình thường |
|  | Endpoint Detection & Response | 157 agent đã được cài đặt EDR | - Ghi nhận 157 agent online trong vòng 30 ngày. |
|  | CyM Agent | 140 agent đã được cài đặt | - 111 agent đều đang có trạng thái ON, thực hiện giám sát ATTT bình thường.  - 29 agent đang ở trạng thái OFF. |

*(Chi tiết danh sách CyM Agent Offline xem tại Phụ lục 01)*

Mọi thắc mắc các vấn đề liên quan, vui lòng liên hệ email: [vcs.care@viettel.com.vn](mailto:vcs.care@viettel.com.vn), điện thoại: 0971.360.360./.

Trân trọng!

|  |  |
| --- | --- |
| ***Nơi nhận:***  - Như trên;  - BGĐ (để b/c);  - Lưu: VT, TTGS. Hiên 07. | **TUQ. GIÁM ĐỐC**  **PHÓ GIÁM ĐỐC** |

**PHỤ LỤC 01**

**DANH SÁCH CYM AGENT OFFLINE**

| **STT** | **Hostname** | **IP DCN** | **IPs** | **OS platform** | **Last ping** |
| --- | --- | --- | --- | --- | --- |
|  | Reputa-VPTWD-Elasticsearch8 | 10.208.137.141 | 10.208.137.141 | ubuntu | 10/3/2025 7:45 |
|  | soc-vptwd-dlp-1 | 10.208.137.159 | 10.208.137.159 | Microsoft Windows Server 2019 Standard | 16:06:25 23/04/2025 |
|  | svr-sso01 | 10.221.173.130 | 10.221.173.130 | ubuntu | 16:19:21 28/04/2025 |
|  | svr-sso02 | 10.221.173.131 | 10.221.173.131 | ubuntu | 3/1/2025 11:11 |
|  | ADC | 10.10.0.70 | 10.0.87.12, 171.254.93.214, 10.129.1.117 | Microsoft Windows Server 2022 Standard | 21:36:10 17/04/2025 |
|  | APP1 | 10.10.0.71 | 10.0.87.4, 171.254.93.140, 10.129.1.109 | Microsoft Windows Server 2022 Standard | 21:45:12 17/04/2025 |
|  | APP2 | 10.10.0.71 | 10.0.87.5, 171.254.95.239, 10.129.1.110 | Microsoft Windows Server 2022 Standard | 21:44:59 17/04/2025 |
|  | DB1 | 10.10.0.71 | 10.0.87.132, 10.0.87.136, 10.129.1.118, 169.254.2.38 | Microsoft Windows Server 2022 Standard | 21:51:26 17/04/2025 |
|  | DB2 | 10.10.0.71 | 10.0.87.133, 10.0.87.134, 10.0.87.135, 10.129.1.119, 169.254.1.108 | Microsoft Windows Server 2022 Standard | 21:53:31 17/04/2025 |
|  | LIVESTREAM | 10.10.0.71 | 10.0.87.8, 171.254.94.102, 10.129.1.113 | Microsoft Windows Server 2022 Standard | 21:54:18 17/04/2025 |
|  | PDC | 10.10.0.71 | 10.0.87.11, 171.254.95.182, 10.129.1.116 | Microsoft Windows Server 2022 Standard | 21:40:52 17/04/2025 |
|  | SEARCH | 10.10.0.70 | 10.0.87.7, 171.254.95.244, 10.129.1.112 | Microsoft Windows Server 2022 Standard | 21:58:35 17/04/2025 |
|  | TH | 10.10.0.71 | 10.0.87.6, 171.254.93.180, 10.129.1.111 | Microsoft Windows Server 2022 Standard | 22:00:11 17/04/2025 |
|  | VEEAM | 10.10.0.71 | 10.0.87.10, 171.254.94.189, 10.129.1.115 | Microsoft Windows Server 2022 Standard | 22:02:23 17/04/2025 |
|  | a21ff1bb-32d7-4701-9aee-abec2af9ef99 | 10.10.0.71 | 10.0.82.16, 10.129.9.186 | ubuntu | 21:01:41 28/04/2025 |
|  | ab9e495e-95e4-48eb-baed-c8baa1314f5c | 10.10.0.70 | 10.0.82.33, 10.129.9.203 | ubuntu | 22:02:30 28/04/2025 |
|  | adab08b8-d2e3-4e7c-b024-6f1a6af010e1 | 10.10.0.71 | 10.0.82.38, 10.129.9.208 | ubuntu | 22:04:10 28/04/2025 |
|  | af83395d-ff5a-4ae3-bdc4-de06d6a38f55 | 10.10.0.70 | 10.0.82.30, 10.129.9.200 | ubuntu | 22:01:29 28/04/2025 |
|  | b68a4ad5-1557-4d17-a5a6-1500e9eccf3e | 10.10.0.71 | 10.0.82.21, 10.129.9.191 | ubuntu | 21:04:08 28/04/2025 |
|  | bc834314-82c2-4adc-b702-286b79719927 | 10.10.0.71 | 10.0.82.12, 10.129.9.182 | ubuntu | 21:00:23 28/04/2025 |
|  | c28596f8-09f6-4d4f-9abf-4018f1f4e92c | 10.10.0.70 | 10.0.82.18, 10.129.9.188 | ubuntu | 21:02:36 28/04/2025 |
|  | c8f97136-bc79-40a1-a078-39b395caae7e | 10.10.0.70 | 10.0.82.11, 10.129.9.181 | ubuntu | 21:00:11 28/04/2025 |
|  | d13dc8dd-a4a4-48e5-af02-1731d6bb36ad | 10.10.0.70 | 10.0.82.20, 10.129.9.190 | ubuntu | 21:03:48 28/04/2025 |
|  | d3291382-80d0-4acc-8d8f-6d5da6f36911 | 10.10.0.70 | 10.0.82.41, 10.129.9.211, 10.0.2.50 | ubuntu | 18:20:09 28/04/2025 |
|  | d9321443-d093-4ffe-a2a2-88e216278591 | 10.10.0.70 | 10.0.82.26, 10.129.9.196 | ubuntu | 21:59:39 28/04/2025 |
|  | da7a469d-fcef-4fb6-b8fa-d373d26025f0 | 10.10.0.71 | 10.0.82.40, 10.129.9.210 | ubuntu | 22:04:27 28/04/2025 |
|  | rac1 | 10.10.0.70 | 117.5.149.1, 10.0.79.133, 10.129.9.84, 10.0.9.3, 192.168.122.1 | oracle | 3/4/2025 14:16 |
|  | rac2 | 10.10.0.70 | 117.5.148.59, 10.0.79.134, 10.129.9.85, 10.0.9.4, 192.168.122.1 | oracle | 3/4/2025 11:46 |
|  | simax | 10.10.0.71 | 171.254.94.241, 10.0.87.9, 10.129.1.114 | centos | 9/4/2025 13:40 |