|  |
| --- |
| **BÁO CÁO KẾT QUẢ CỦA ĐỘI PHÒNG THỦ TRONG DIỄN TẬP THỰC CHIẾN BẢO ĐẢM AN TOÀN THÔNG TIN TỈNH ĐIỆN BIÊN NĂM 2022** |

**THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO**

* Tên tổ chức/cá nhân báo cáo (\*)
* Địa chỉ: (\*)
* Điện thoại (\*) Email (\*)

**NGƯỜI LIÊN HỆ**

* Họ và tên (\*) Chức vụ:
* Điện thoại (\*) Email (\*)

|  |  |
| --- | --- |
| Thời gian thực hiện diễn tập (\*) | |
| Thời gian bắt đầu: ….giờ…..phút …ngày…tháng….năm … | Thời gian kết thúc: …..giờ…..phút …ngày…tháng….năm … |

**KẾT QUẢ PHÒNG THỦ**

<kết quả phòng thủ được thể hiện rõ ràng, chi tiết gồm: chú thích, hình ảnh, bằng chứng>

* Đội giám sát vận hành hệ thống

Mô tả chi tiết cách thức phát hiện tấn công kèm theo các ảnh chụp mô tả như:

* Ảnh chụp giao diện website bị thay đổi.
* Ảnh chụp logs cảnh báo trên hệ thống giám sát SIEM.
* Đội rà soát ứng cứu sự cố

Mô tả chi tiết các bước rà soát, ứng cứu sự cố kèm theo các ảnh chụp mô tả như:

* Thông tin sơ bộ mã độc ( thời gian tạo, dung lượng), ảnh file mã độc
* Ảnh keyrun mã độc, ảnh mã độc đang chạy trên hệ thống.
* Ảnh file webshell trên hệ thống
* Ảnh file keylog trên hệ thống

**KIẾN NGHỊ, ĐỀ XUẤT HỖ TRỢ**

|  |
| --- |
| Mô tả về đề xuất, kiến nghị |
| *Đề nghị cung cấp tóm lược về các kiến nghị và đề xuất hỗ trợ trong tổ chức thực hiện phòng thủ* |

**THỜI GIAN THỰC HIỆN BÁO**\*:/…/…/… (ngày/tháng/năm)

**NGƯỜI ĐẠI DIỆN ĐỘI PHÒNG THỦ**

*(Ký tên, đóng dấu)*