SafeOC If you SEE something, SAY something

AN NINH MẠNG VÀ CÁC MỐI ĐE DỌA TRỰC TUYẾN

T“Cuộc chiến chống khủng bố” là cuộc chiến không ngừng nghỉ. Trong những năm gần đây, những kẻ khủng bố đã chuyển sang sử dụng nhiềuvũ khí đặc biệt, chẳng hạn như tấn công mạng.

Tấn công mạng có thể đề cập đến một số hành vi khác nhau liên quan đến các kiểu truy cập trái phép, truy cập cơ sở dữ liệu, thay đổi tệp tin và các hành động khác thường, việc đó có thể dẫn đến một cuộc tấn công hoặc truy cập trái phép dữ liệu.

Truy cập SafeOC.com để biết thêm thông tin về nội dung và cách báo cáo.

theo chúng tôi: @SafeOC @SafeOrangeCounty @Safe_OC

SafeOC If you SEE something, SAY something

Dưới đây là một số ví dụ phổ biến nhất về hoạt động đáng ngờ:

HOẠT ĐỘNG CƠ SỞ DỮ LIỆU:

Hoạt động cơ sở dữ liệu bất thường có thể do các cuộc tấn công bên trong hoặc bên ngoài gây ra và các dấu hiệu quan trọng cần theo dõi bao gồm các thay đổi về người dùng, quyền quản trị và sự phát triển dữ liệu nội dung bất thường.

TẤN CÔNG MẠNG:

Làm gián đoạn hoặc làm tổn hại hệ thống công nghệ thông tin của một tổ chức.

LẠM DỤNG TÀI KHOẢN:

Việc lạm dụng các tài khoản đặc quyền là một trong những dấu hiệu phổ biến nhất của cuộc tấn công từ nội bộ và các dấu hiệu cần theo dõi là các dữ liệu kiểm toán bị sửa đổi, chia sẻ quyền truy cập tài khoản và truy cập thông tin nhạy cảm không cần thiết.

THAY ĐỔI TẬP TIN:

Thay đổi cài đặt đối với tập tin – bao gồm thay thế, sửa đổi, thêm và xóa tập tin – là một dấu hiệu vi phạm dữ liệu cơ bản, vì nó cho thấy ai đó đã xâm nhập vào hệ thống mạng lưới của bạn và đang cố gắng ngăn chặn việc bị phát hiện.

Truy cập SafeOC.com để biết thêm thông tin về nội dung và cách báo cáo.

theo chúng tôi: @SafeOC @SafeOrangeCounty @Safe_OC