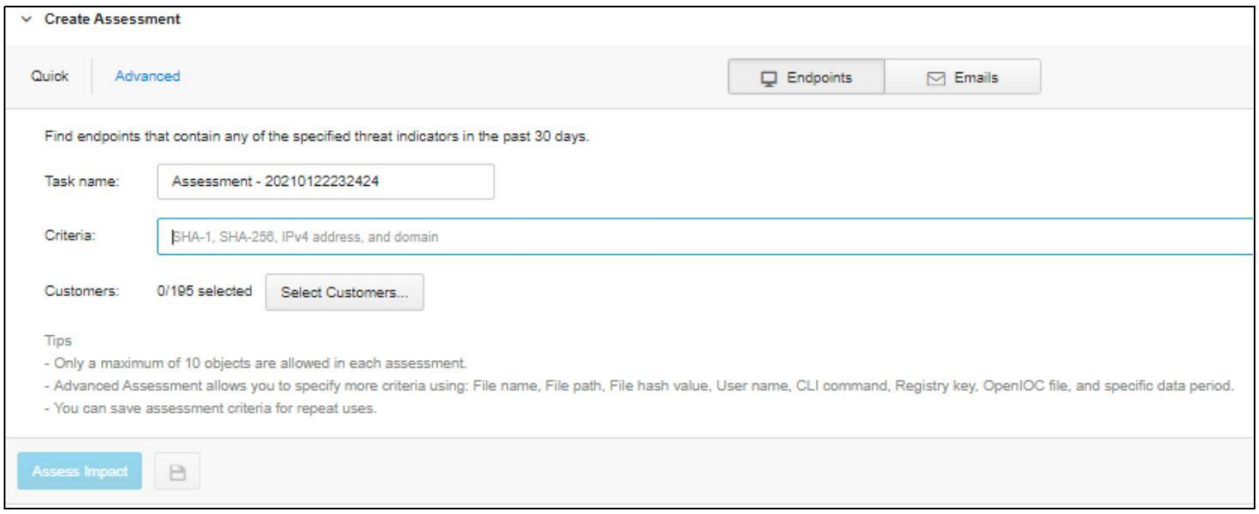
Hướng dẫn sử dụng Đánh giá trong Remote Manager

Đánh giá

Chức năng Detection & Response Assessments là chức năng điều tra chéo khách hàng giúp bạn định vị **Thư điện tử** và **Điểm cuối** dữ liệu khớp với tiêu chí mối đe dọa được bạn chỉ định. Trên tab Assessments, bạn có thể tạo đánh giá mới, quản lí đánh giá hiện có và xem kết quả đánh giá. Có 2 cách tạo đánh giá: tạo nhanh và tạo nâng cao.

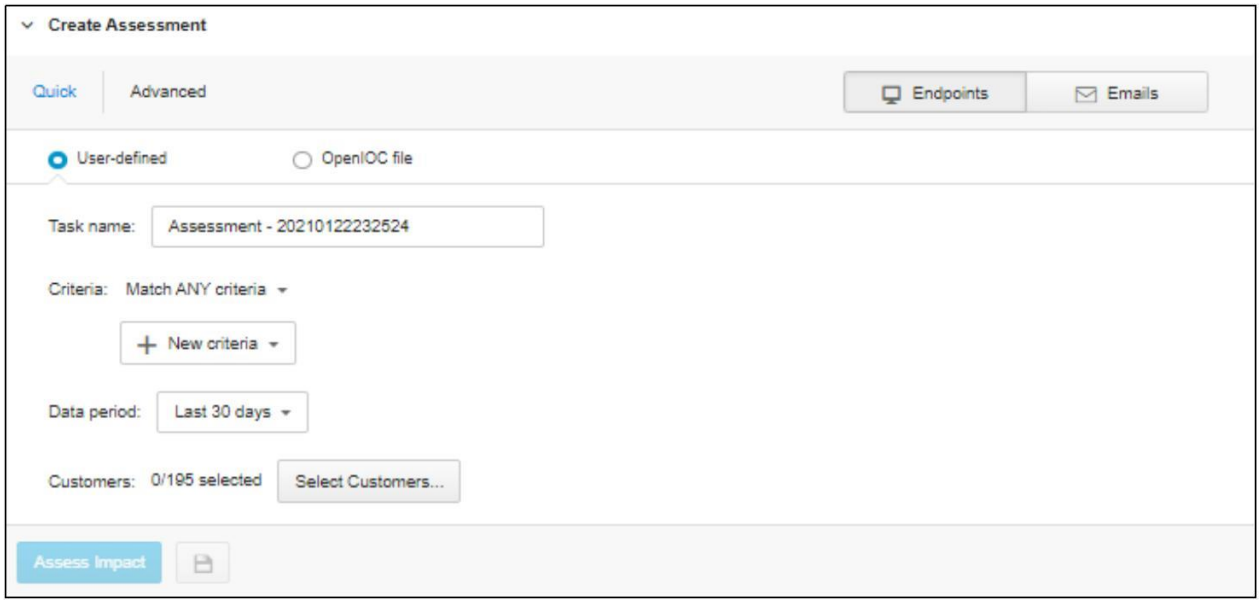
I. Cách tạo Endpoint Assessment

1. **Tạo nhanh Endpoint Assessment** – Đánh giá nhanh điểm cuối có sẵn bốn (4) loại tiêu chí và khoảng thời gian ba mươi (30) ngày trước.



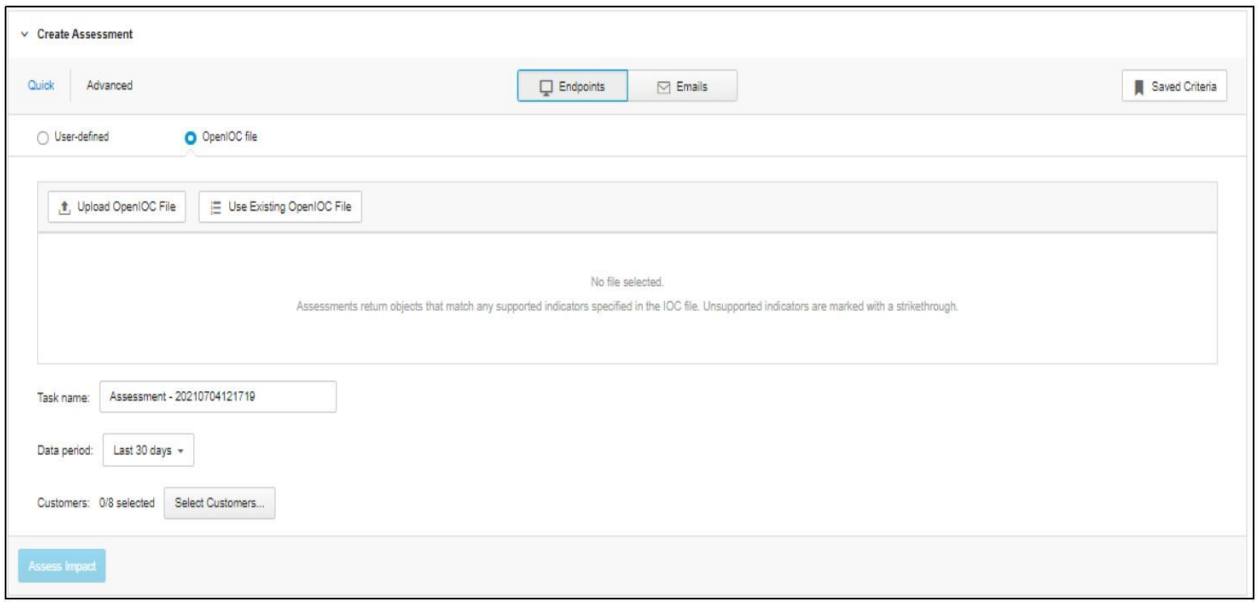
a) Nhấp vào Detection & Response > Assessments.
b) Mở rộng mục Create Assessment, chọn Quick and Endpoints.
c) Nhập tên đầu mục hoặc sử dụng tên tạo ngẫu nhiên.
d) Nhập tối đa mười tiêu chí.
   - Hàm băm SHA-1
   - Hàm băm SHA-256
   - Địa chỉ Ipv4
   - Miền
e) Nhấp vào Select Customers, sau đó chọn khách hàng để đưa vào đánh giá
f) Nhấp vào Assess Impact.

2. **Tạo Advanced Endpoint Assessment (User-Defined)** – Đánh giá điểm cuối nâng cao có sẵn chín (9) loại tiêu chí và khoảng thời gian xác định cấu hình tối đa lên đến ba mươi (30) ngày trước. Bạn có thể thủ công định dạng đánh giá hoặc tải tệp OpenIOC lên.



a) Nhấp vào Detection & Response > Assessments.
b) Mở rộng mục Create Assessment, nhấn chọn Advanced and Endpoints.
c) Để định dạng tiêu chí thủ công, chọn User-defined.
d) Nhập tên đầu mục hoặc sử dụng tên tạo ngẫu nhiên.
e) Nhập tối đa mười tiêu chí.
    - FQDN / địa chỉ IP / Tên máy chủ
    - Tên người dùng
    - Tên tệp
    - Gía trị hàm băm của tập
    - Tập tin của thư mục
    - Mã đăng kí
    - Tên giá trị đăng kí
    - Dữ liệu giá trị đăng kí
    - Lệnh CLI
f) Chọn khoảng thời gian của dữ liệu
    - 24 giờ qua
    - 7 ngày qua
    - 30 ngày qua
g) Nhấp vào Select Customers, sau đó chọn khách hàng để đưa vào đánh giá
h) Nhấp vào Assess Impact.

3. **Tạo Advanced Endpoint Assessment (OpenIOC file)** - Đánh giá điểm cuối nâng cao (tệp OpenIOC) cho phép bạn tải lên tệp OpenIOC bao gồm giá trị được xác định trước và khoảng thời gian xác định cấu hình tối đa lên đến ba mươi (30) ngày trước.



a) Nhấp vào Detection & Response > Assessments.

b) Mở rộng phần Create Assessment, chọn Advanced and Endpoints. Chuyển nút radio sang OpenIOC File

c) Tải lên tệp OpenIOC File mới hoặc sử dụng tệp có sẵn đã được tải lên từ trước.

d) Chọn khoảng thời gian dữ liệu

- 24 giờ qua
- 7 ngày qua
- 30 ngày trước

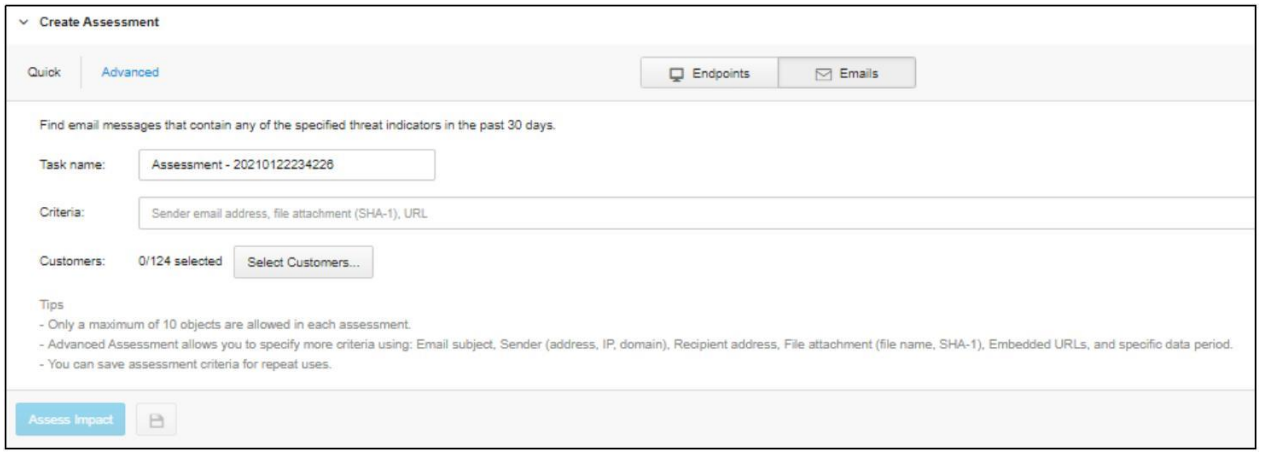
e) Nhấp vào Select Customers, sau đó chọn khách hàng để đưa vào đánh giá

f) Nhấp vào Assess Impact.

Lưu ý: *Đánh giá sẽ trả về đối tượng nào khớp với bất kỳ chỉ số hỗ trợ được chỉ định trong tệp IOC*

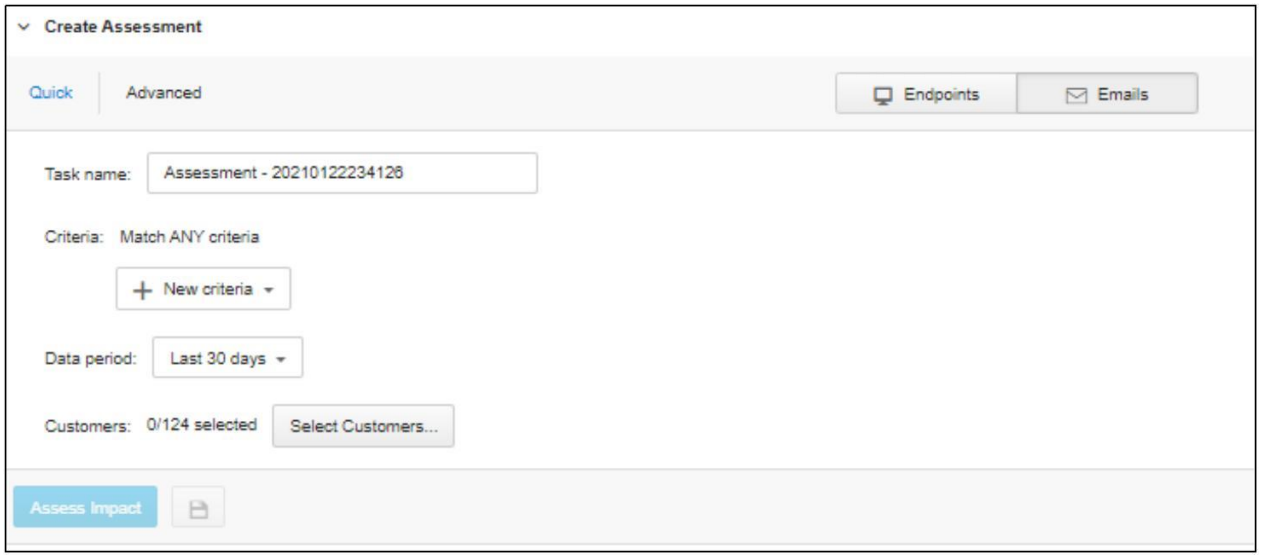
II. Cách tạo Email Assessment

1. **Tạo nhanh Quick Email Assessment** - Thư đánh giá nhanh có sẵn ba (3) loại tiêu chí và khoảng thời gian ba mươi (30) ngày trước.



a) Nhấp chọn Detection & Response > Assessments.
b) Mở rộng phần Create Assessment, chọn Quick and Emails.
c) Nhập tên đầu mục hoặc sử dụng tên tạo ngẫu nhiên
d) Nhập tối đa mười tiêu chí.
   - Địa chỉ email của người gửi
   - Gía trị hàm băm SHA-1 (đối với tệp đính kèm)
   - URL được nhúng
e) Nhấp vào Select Customers, sau đó chọn khách hàng để đưa vào đánh giá
f) Nhấp vào Assess Impact.

2. **Tạo thư Advanced Email Assessment** – Thư đánh giá nâng cao có sẵn tám (8) loại tiêu chí và khoảng thời gian xác định cấu hình tối đa lên đến ba mươi (30) ngày trước.



a) Nhấp vào Detection & Response > Assessments.
b) Mở rộng mục Create Assessment, chọn Advanced and Emails.
c) Nhập tên đầu mục hoặc sử dụng tên tạo ngẫu nhiên
d) Định dạng cấu hình tối đa mười tiêu chí đánh giá
   - Địa chỉ email của người gửi
   - IP hoặc miền của máy chủ email người gửi
   - Địa chỉ email người nhận
   - Chủ đề tin nhắn
   - Tên tệp đính kèm
   - Gía trị hàm băm SHA-1 của tệp đính kèm
   - Tệp mở rộng
   - URL được nhúng
e) Chọn khoảng thời gian dữ liệu
   - 7 ngày qua
   - 14 ngày qua
   - 30 ngày qua
f) Nhấp vào Select Customers, sau đó chọn khách hàng để đưa vào đánh giá
g) Nhấp vào Assess Impact.

III. Xem kết quả đánh giá

Trên tab Detection & Response Assessments, phần Danh sách Assessment List cho phép bạn thực hiện các tác vụ sau.

i. Xem chi tiết đánh giá - vào liên kết trong cột Task Name để xem chi tiết bao gồm tình trạng hiện tại, giai đoạn, khách hàng được chọn, khách hàng bị ảnh hưởng và các tiêu chí đánh giá.

A. Tin nhắn trùng khớp
   - Tin nhắn bị khoanh vùng hoặc
   - Xuất dữ liệu
   - Xem người nhận tin nhắn
   - Quản lý các URL được nhúng
   - Quản lý các tệp đính kèm

B. Điểm cuối trùng khớp
   - Xuất dữ liệu
   - Xem chi tiết của điểm cuối được xác định trùng khớp

ii. Xem khách hàng bị ảnh hưởng – Nhấp vào số lượng trong cột Affected Customers để xem danh sách khách hàng có thư tin nhắn email hoặc dữ liệu điểm cuối

iii. Xóa đánh giá – Chọn bất kì con số hoặc đánh giá đã hoàn tất và nhấp vào Delete.