BarracudaCampus

IR01020 – Insights and Reporting with Incident Response
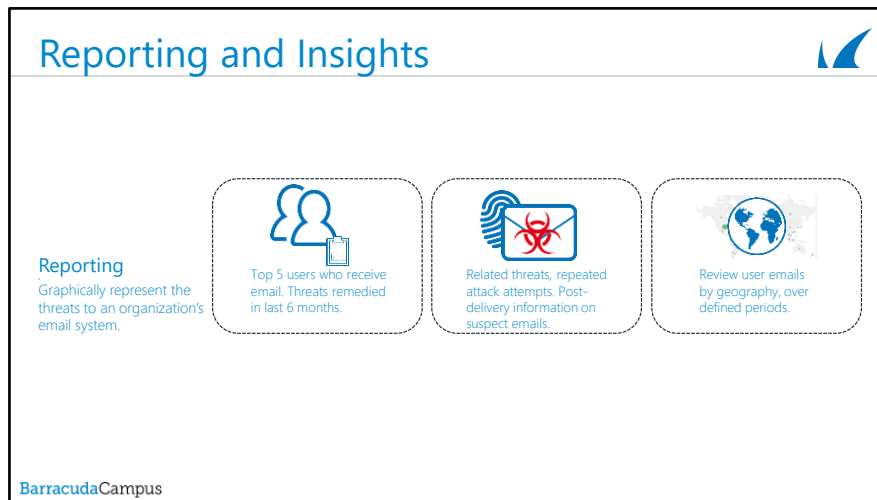
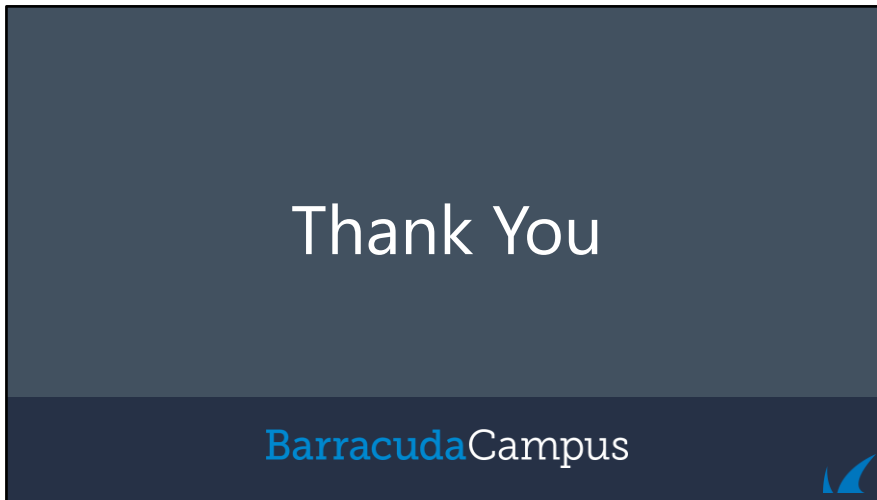Reporting and tracking threats

Training Video Transcript

Training Video Transcript

In any organization, information regarding threats needs to be managed. Conclusions need to be carefully drawn. Insights can be used to glean more information about user email, to detect phishing and spearphishing that may otherwise go undetected. Insights in Incident Response graphically represents many of the threats to an organization's email systems.

A set of default reports provides a further guide regarding the different layers of resilience within the organization. The two reports: top 5 users who report malicious emails, versus top 5 users who receive malicious emails, can be compared. In some cases, users who either under report, or over report confirmed threats can be recommended for further training. Logs and reports provide an accessible store of previous threats and incidents, which can be analyzed to further to gauge responses and provide forensic information.

There are two types of identified potential threats which are continually tracked in Incident Response. Related threats are those threats identified as versions of previously flagged threats. These are mainly based on what users have reported. Meanwhile, post-delivery threats employ the wider intelligence gained by Barracuda Networks from various sources to detect any malicious email threats which are currently circulating. These two types are the basis for alerts. Operators and administrators can prepare a specific set of default responses in each case.

We can see where email has been received from. This helps administrators build up a picture of where incoming mail is being directed towards recipients within an organization. It can show countries, and regions, where it is highly unlikely that email might originate, given the organization and its activities. Activity within different time frames can be highlighted using filtering, from 1 hour to the last 7 days. If you find a location that seems suspicious, you can click on it and view the emails to verify whether it is a source of malicious emails. If it is, you can create an incident directly.

Thank You

Barracuda**Campus**

Training Video Transcript