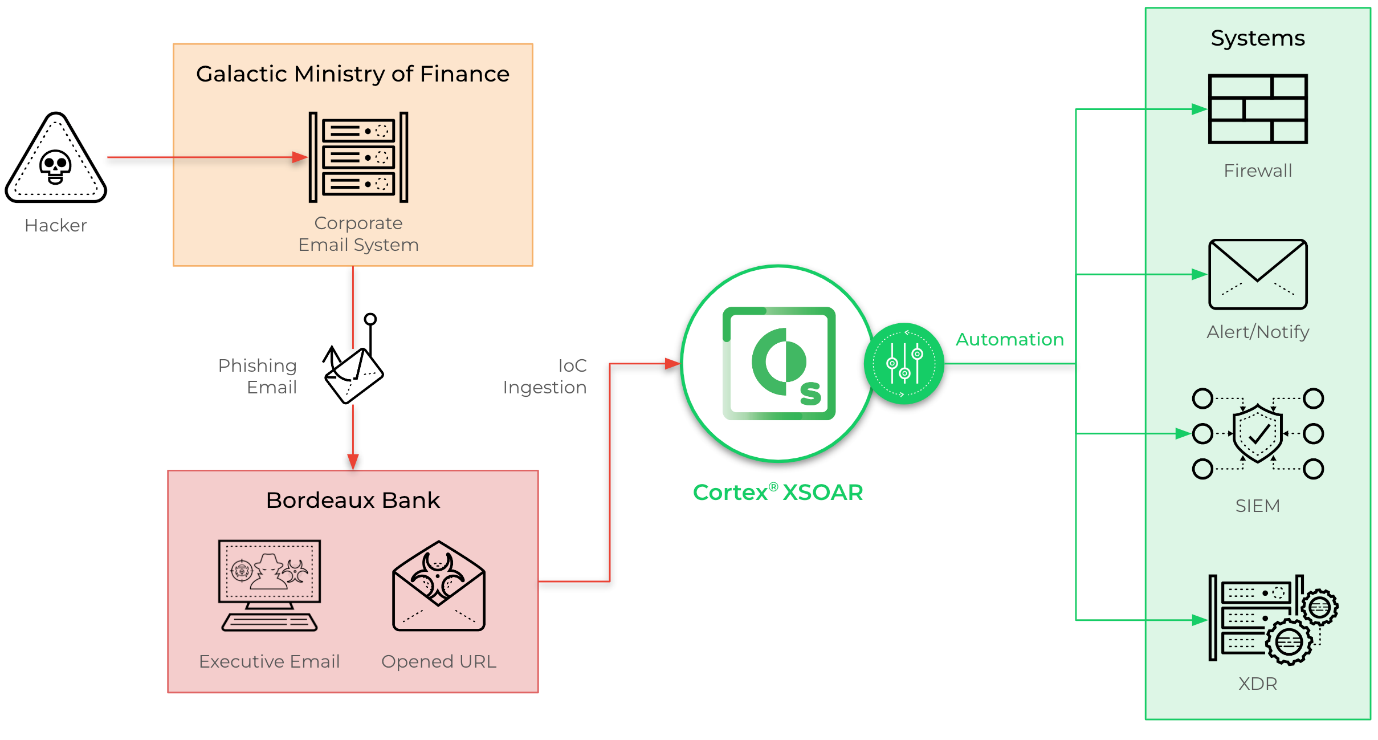
**Automating Response to Phishing with Cortex XSOAR**

**Overview**

In this lab, use Cortex XSOAR (XSOAR) to automate incident response to phishing attacks.

The lab uses a real spear phishing attack against a fictional bank, Galactic Ministry of Finance, by infiltrating the bank's e-mail server. After infiltration, the attacker sends phishing e-mails to executives at a partnering bank, Bordeaux Bank, during peak business hours.



The XSOAR instance in this lab has been pre-configured to use specific alerts, incidents, and playbooks. We recommend taking the time to review the out-of-box integrations available through the XSOAR Marketplace.

Palo Alto Networks has partnered with Google Cloud to host this lab. As part of the lab you will be given access to a Cortex XSOAR threat intel management instance.

What you'll learn

In this lab, you will perform the following tasks:

* Investigating incidents using Cortex XSOAR.
* Understanding Cortex XSOAR War Rooms.
* Creating an incident Response Plan with Cortex XSOAR.

In this task, take a moment to review the limitations of current solutions in effectively addressing phishing attacks.

1. **What is phishing?**

Phishing is a type of social engineering that primarily occurs through email. Attackers create fraudulent emails that mimic legitimate communication in order to deceive recipients.

1. **What are some current limitations with today's systems in addressing phishing emails?**

Responding to phishing emails can be a time-consuming and complex task. These tasks often require multiple tools and involve manual actions that are error prone.

1. **How does Cortex XSOAR address these limitations?**

Cortex XSOAR effectively addresses challenges associated with phishing emails through its comprehensive automation and orchestration capabilities.  
By combining automation, orchestration, and integrations, Cortex XSOAR significantly enhances the efficiency, accuracy, and speed of responding to phishing emails, effectively mitigating the associated challenges.

In this lab you learned to use Cortex XSOAR to respond to phishing incidents. You also learned how to generate reports, navigate War Room, and complete Work Plans and playbooks.