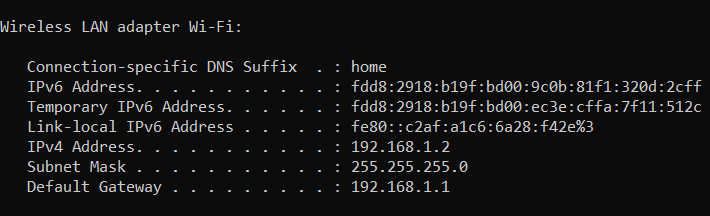
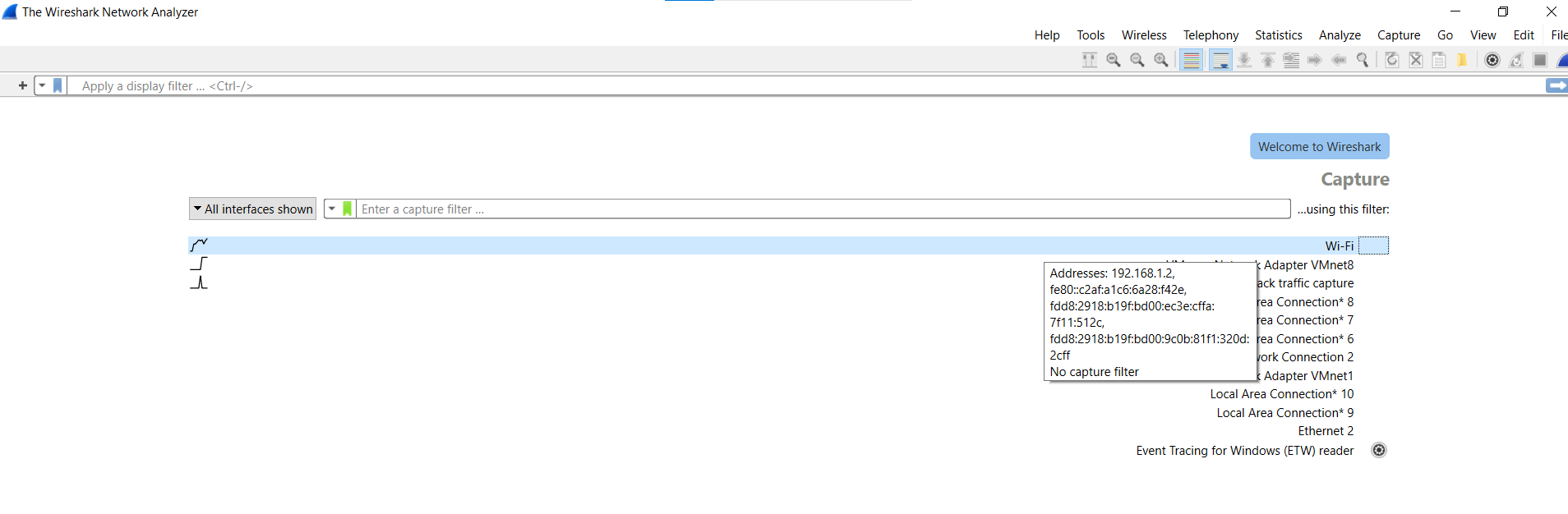
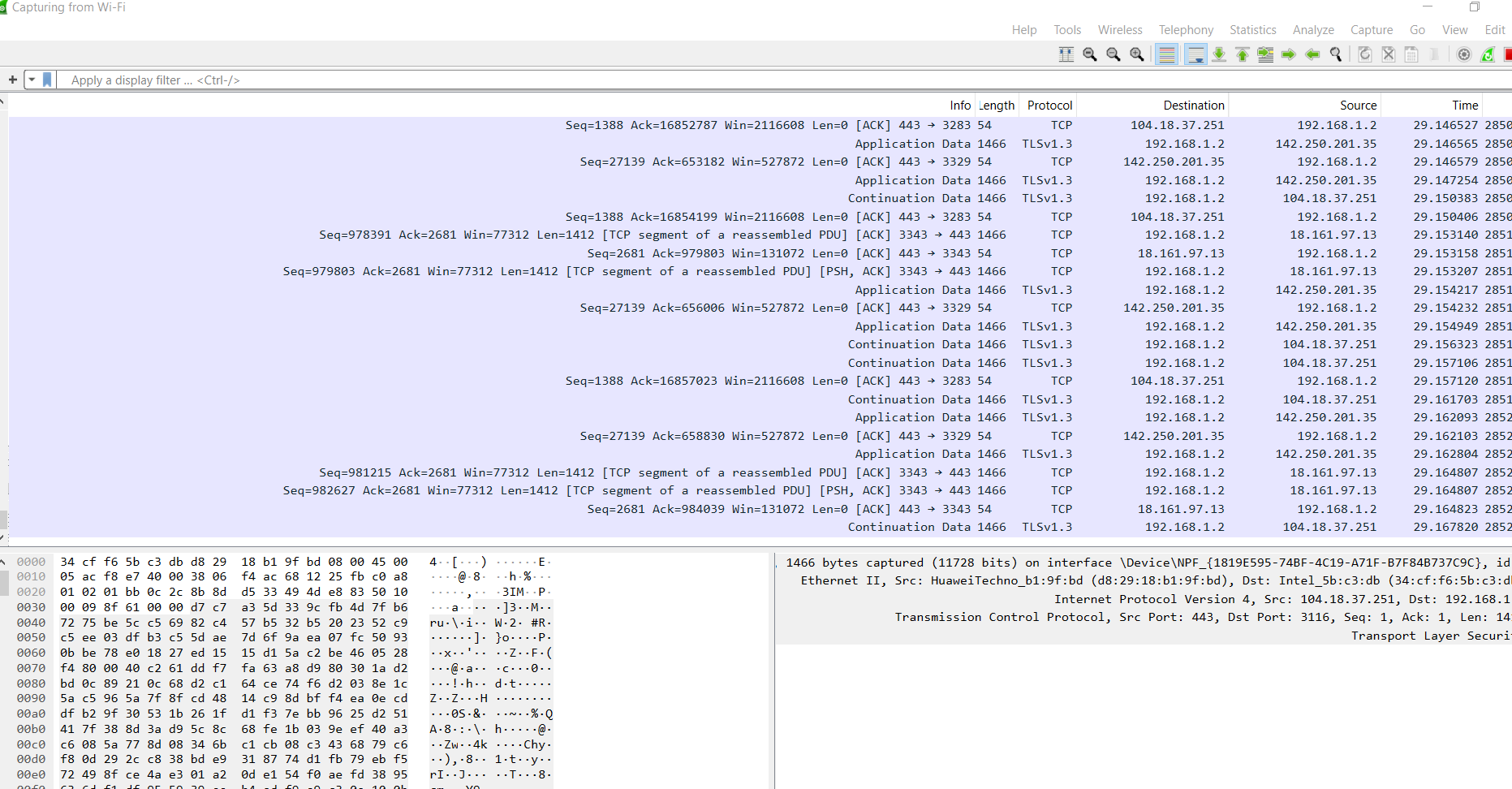
**Wireshark analysis report**

First check your interface that you are going to make the analysis on it



Open **wireshark** and and choose the interface based on your network connection



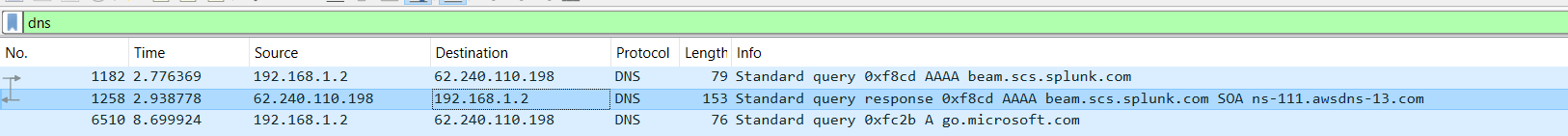


Here is all your network packets you can start or stop capturing packets on the red button

You can use filtering if you are looking for a specific activity on the network

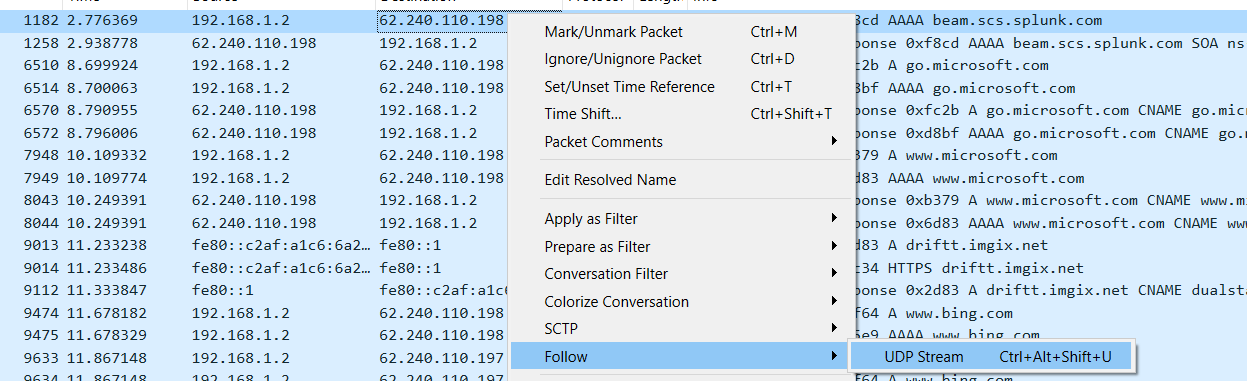
Using ip or protocols or servers whatever the filter you want

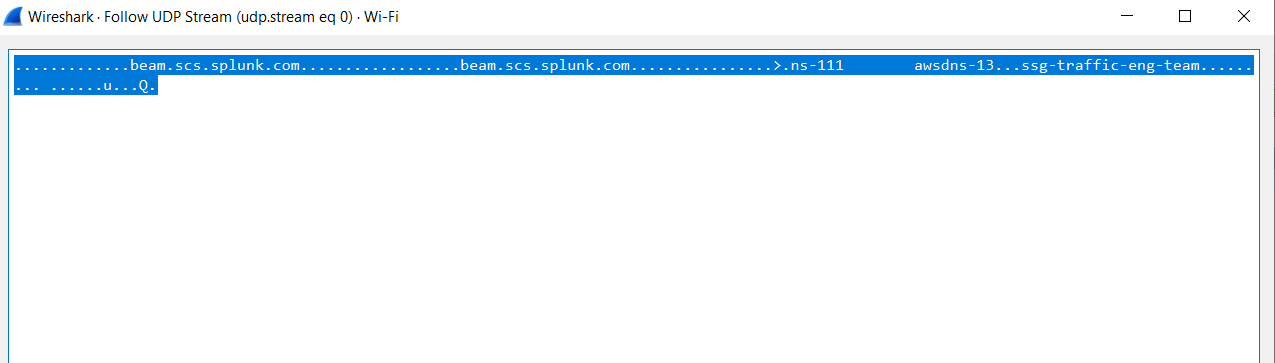
Example open splunk on my browser how do I know the packet and open it will use DNS filtering for this anything on my browser we prefer to search using DNS protocol



First one is the query that I searched for splunk.com

Then the response from splunk using DNS query respond everything happens on the internet wireshark has it





 beam.scs.splunk.com: This is a fully qualified domain name (FQDN) indicating a specific server or service within the splunk.com domain.

 ns-111.aws-dns-13: This appears to be a DNS server, likely part of AWS's DNS infrastructure.

ssg-traffic-eng-team: This could be a tag or identifier for a specific team or service group, possibly within the organization using this infrastructure

**Identify Suspicious Activities**

**Unusual Traffic Patterns:** High volume of traffic

**Unrecognized IP Addresses:** Traffic from or to IP addresses not commonly used within your network.

**Strange Protocols or Ports:** Unusual protocols or non-standard port usage.

 **Repeated Connection Attempts:** Numerous failed login attempts or repeated connections to specific services.(brute-force-attack)

**Data Exfiltration:** Large volumes of data being sent to external addresses.

 **Malware Communication:** Communication with known malicious IPs/domains

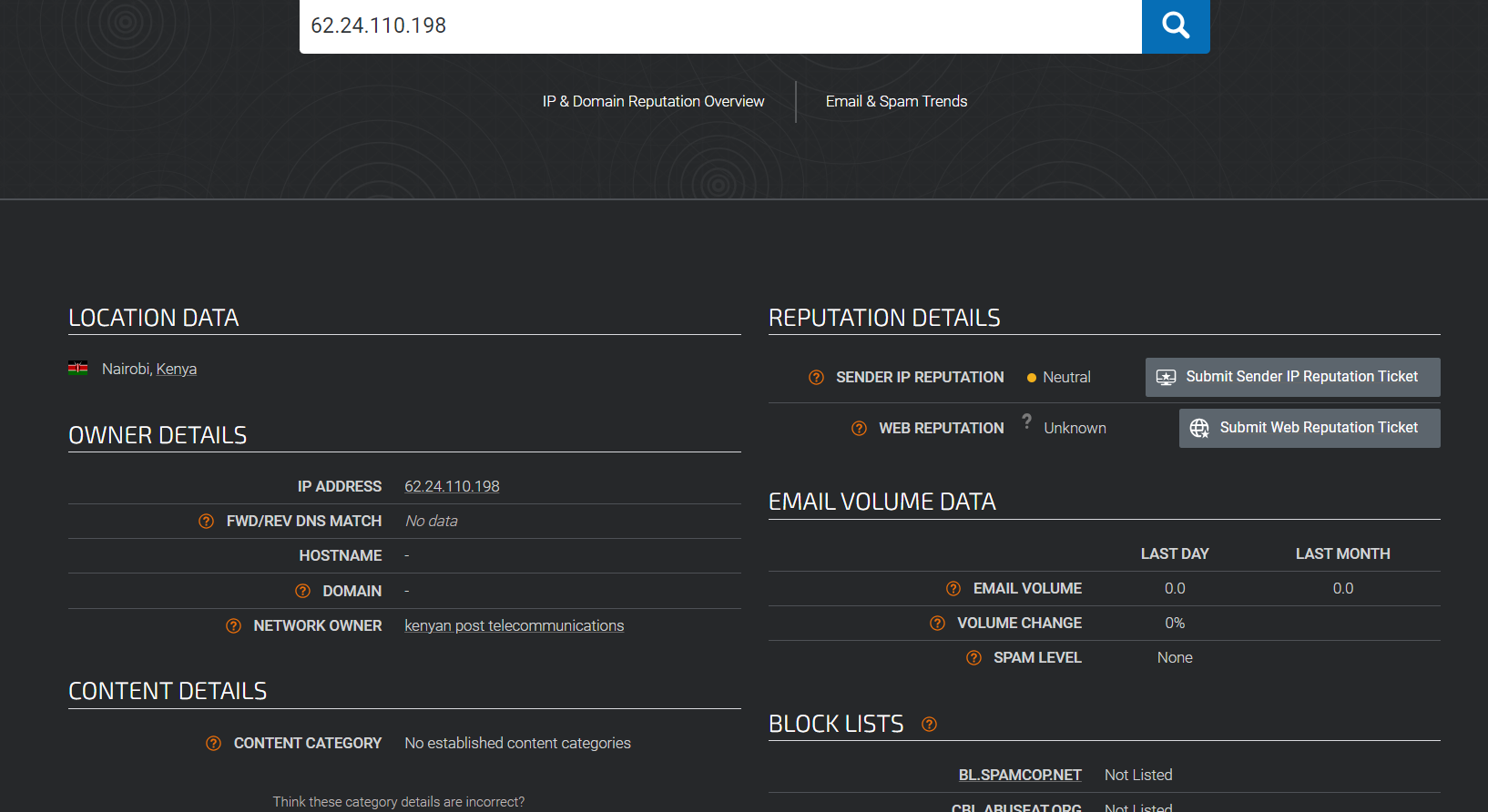
**Solutions to these problems**

**Network Monitoring and Alerts:** Implement continuous network monitoring and set up alerts for unusual traffic patterns using tools like Splunk

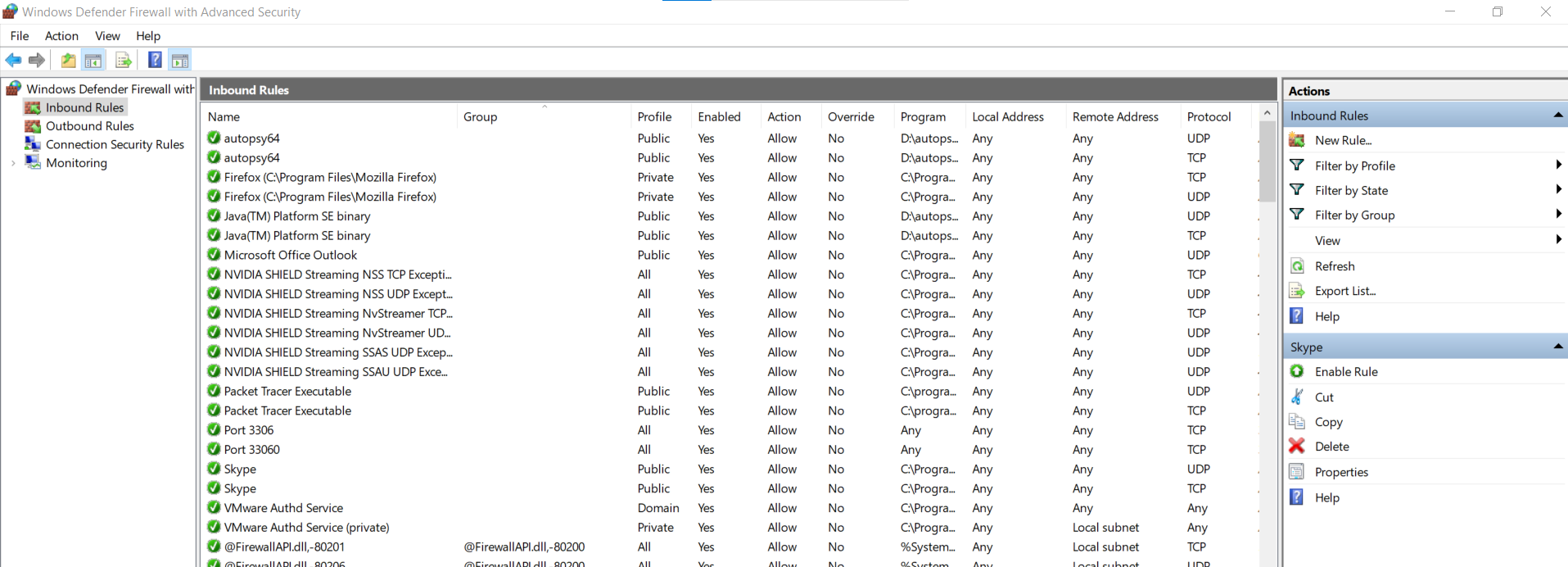
**IP Whitelisting:** Implement IP whitelisting to restrict access to known and trusted IP addresses.

You can check the reputation of the ip using

<https://www.talosintelligence.com/reputation_center>



**Port Management:** Close unnecessary ports and only allow traffic on ports required for business operations.



You Can control all the service allowed and not allowed in your system

**Data Loss Prevention (DLP) Systems:** Deploy DLP systems to monitor and control data transfers, especially to external addresses.

**Access Controls:** Implement strict access controls and ensure that only authorized users can access sensitive data

**DNS Filtering:** Implement DNS filtering to block access to known malicious domains.

**Employee Training:** Conduct regular cybersecurity awareness training for employees to help them recognize and respond to potential threats.