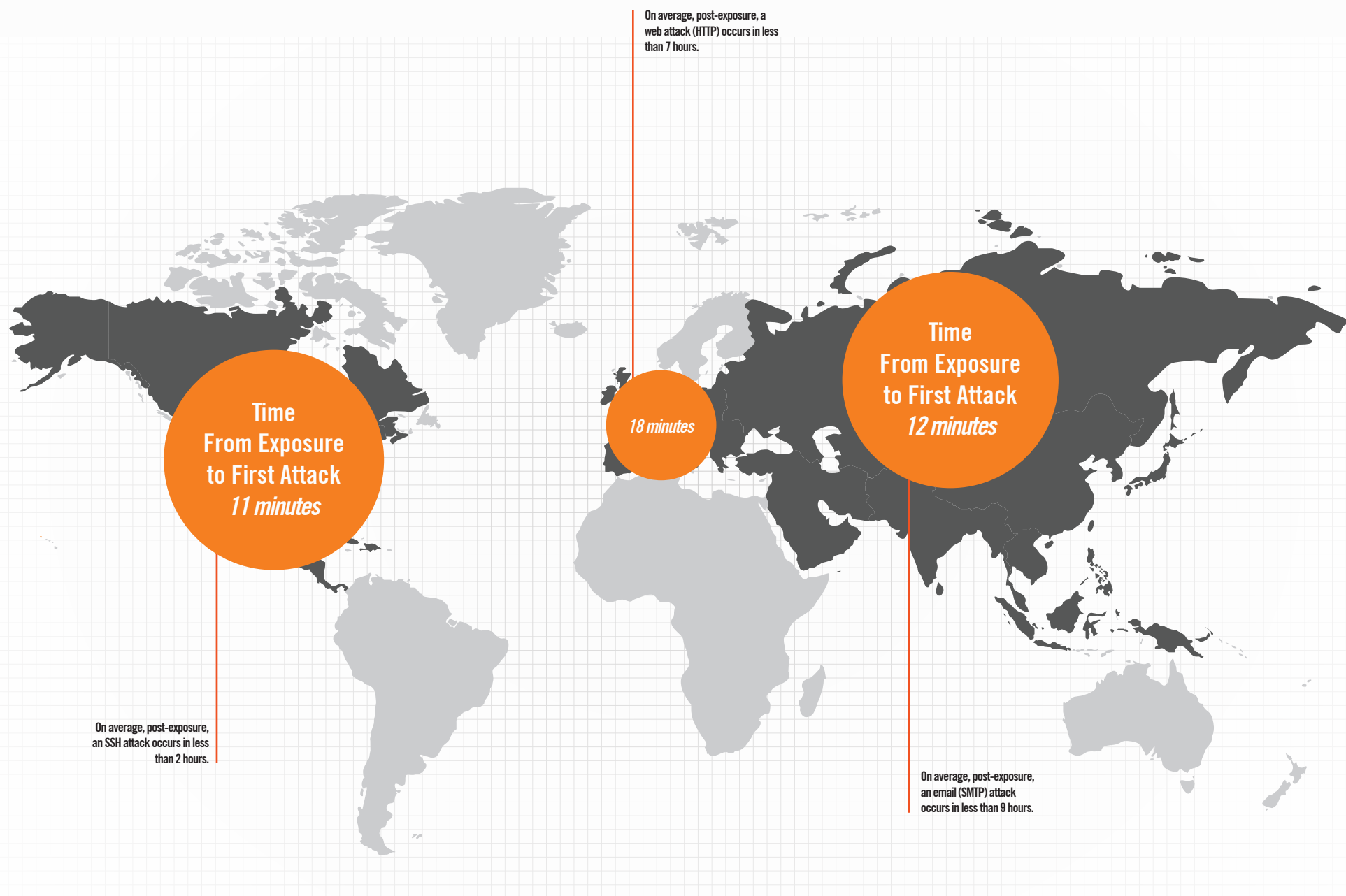






HONEYNET STATS OCTOBER 2015





BROUGHT TO YOU BY THE ALERT LOGIC ACTIVEINTELLIGENCE TEAM







NORTH AMERICA

-  Time From Exposure to Email Attack
7 hours, 44 minutes
-  Time From Exposure to SSH Attack
2 hours, 35 minutes
-  Time From Exposure to Web Attack
4 hours, 38 minutes
-  Time From Exposure to Remote Desktop Attack
1 hour, 05 minutes

EUROPE

-  Time From Exposure to Email Attack
4 hours, 07 minutes
-  Time From Exposure to SSH Attack
1 hour, 48 minutes
-  Time From Exposure to Web Attack
4 hours, 21 minutes
-  Time From exposure to Remote Desktop Attack
1 hour, 27 minutes

ASIA

-  Time From Exposure to Email Attack
5 hours, 36 minutes
-  Time From Exposure to SSH Attack
1 hour, 33 minutes
-  Time From Exposure to Web Attack
9 hours, 13 minutes
-  Time From exposure to Remote Desktop Attack
2 hours, 41 minutes

This map demonstrates how quickly cybercriminals seek out attack vectors within your systems. Within 24 hours of exposure to the Internet, it is likely that your systems have already been scanned and selected for further investigation by cybercrime groups. Mitigate your risk for attack by applying security best practices that include continuous monitoring of your networks and systems.

The Alert Logic ActiveIntelligence group operates a number of proactive initiatives to gather information on the threat landscape, one of which is a baiting operation utilizing our global honeynet network. The times listed in the table above represent average lengths of time from exposure to attack for the four most common types of attacks.