The Security Playbook

This Security Playbook contains descriptions of the network event data and other helpful information you will need. Take your time to understand what is in the Security Playbook and refer to it often to help you.

Read this playbook carefully and refer to it often.

Scenario

You are a junior cyber security analyst at XYZ Company -- a tech firm in the United States that provides business intelligence, sales management, and human resources management systems to its customers. Users connect to your services through personal computers, mobile devices, and hosted services (e.g., external websites). Much of the data XYZ Company keeps inside its network is sensitive to both its customers and employees.

You perform initial triage on incoming network events that your company's Intrusion Detection System (IDS) has deemed an alert. The network events assigned to you all deal with the notion of *impossible travel* – when a user accesses the network from two different geographical locations within a relatively short amount of time.

However, the IDS often yields false alarms, and many alerts are nothing to worry about. Your job is to examine the network events to decide if:

a. The alert correctly identifies an attack against the company and thus needs to be *escalated* to senior security personnel; or
b. The alert is is a false alarm and the harmless network activity can be ignored.

In general, the senior security personnel are very busy, so simply escalating everything is not an option. Conversely, ignoring all of the alerts is a bad idea. You have to use your best judgment.

Network Event Data

The IDS summarizes the "impossible travel" events as infomation about two locations:

City of Authorization
There will be two of these fields, one for each geographic location that the IDS detected an authorization from.

Number of Successful Logins
The number of *successful* logins from each location in the past 24 hours. A successful login is one where a correct username+password combination was entered.

Number of Failed Logins
The number of failed login from each location in the past 24 hours. A failed login is when an incorrect password was used for an account.

Source Provider
The type of Internet Provider the authorizations came from at each location.

Telecom	traditional Internet Source Providers (ISPs), e.g., Spectrum and U-verse
Mobile/cellular	Wireless carriers, e.g., Verizon Wireless, AT&T, or Sprint
Hosting/server	Companies that provide hosted services, e.g., Virtual Private Networks (VPNs), web hosting, and server space

Time Between Authorizations
This is the field that typically triggers the alarm. The IDS correlates an authorization from each location and determines that they happened too quickly.

VPN Confidence
The conclusion that you, the analyst/participant, came to that this event involves a user utilizing a Virtual Private Network (VPN).

How to evaluate an event

- You may assume that one of the locations represents legitimate access.
- Look at the city of authorizations. XYZ Company is located in the USA, and has relatively few users from outside the US. Location should not be a deciding factor as users travel legitimately and hosted services may connect from other countries. Nonetheless, certain locations may warrant a more critical evaluation.
- Evaluate the time between authorizations. Authorizations from different locations in a short time could be an indication of account compromise. Refer to the chart below for typical travel times between locations.
- Analyze the *ratio* of successful logins to failed logins from each location. More failed logins than successful logins could be an indication of password guessing, but people do often forget their passwords.
- Evaluate the source providers that the authorizations are coming from. There is nothing inherently safe or malicious about any type of source provider, but knowing can help you determine if other information makes sense.
- The number attributed to "VPN Confidence" should be treated as the conclusion that you, the analyst/participant, came to that this event involves a user utilizing a VPN.

Things to keep in mind

- The IDS is not accurate. It frequently alerts on network events that are normal. It could be that many or all of the alerts are false alarms!
- Users visiting countries with restrictive governments will often use a VPN to get past that nation's firewall.
- It is not unusual for a mobile device to ping in the country the mobile device is registered in when the user is traveling abroad.

Concern Level for each location

Based on the past history of network events, and where XYZ Company's customers typically are, the senior security personnel have put together the following "concern level" chart for various locations. Location is not a deciding factor, but some locations warrant closer inspection.

High	Moscow	Beijing				
Medium	London	Paris	Berlin	Tokyo		
Low	New York	Seattle	Los Angeles	Miami	Vancouver	Toronto

Hours of travel time between locations

The travel times listed in the table below are guidelines, not absolutes.

		New York	Seattle	Los Angeles	Miami	Vancouver	Toronto	London	Paris	Berlin	Tokyo	Moscow	Beijing
USA	**New York**	0	6	5.75	3	5.67	1.5	6.75	6.9	8	13.5	9.2	13.5
	Seattle	6	0	2.7	5.85	3	4.5	9.25	9.55	11.95	9.55	14.55	11.4
	Los Angeles	5.75	2.7	0	5.15	2.75	4.5	10.25	10.5	12.67	11.15	11.25	12.67
	Miami	3	5.85	5.15	0	8.25	3	8.33	8.85	11.5	16.33	11.25	17.5
Canada	**Vancouver**	5.67	3	2.75	8.25	0	4.33	9.25	9.5	11.85	10	14.5	10.67
	Toronto	1.5	4.5	4.5	3	4.33	0	6.95	7.15	7.85	13	11.5	13.45
England	**London**	6.75	9.25	10.25	8.33	9.25	6.95	0	2.5	1.67	11.5	3.67	9.67
France	**Paris**	6.9	9.55	10.5	8.85	9.5	7.15	2.5	0	1.67	11.75	3.35	10.05
Germany	**Berlin**	8	11.95	12.67	11.5	11.85	7.85	1.67	1.67	0	11.85	2.45	9.15
Japan	**Tokyo**	13.5	9.55	11.15	16.33	10	13	11.5	11.75	11.85	0	9.85	3.15
Russia	**Moscow**	9.2	14.55	11.25	11.25	14.5	11.5	3.67	3.35	2.45	9.85	0	7.5
China	**Beijing**	13.5	11.4	12.67	17.5	10.67	13.45	9.67	10.05	9.15	3.15	7.5	0