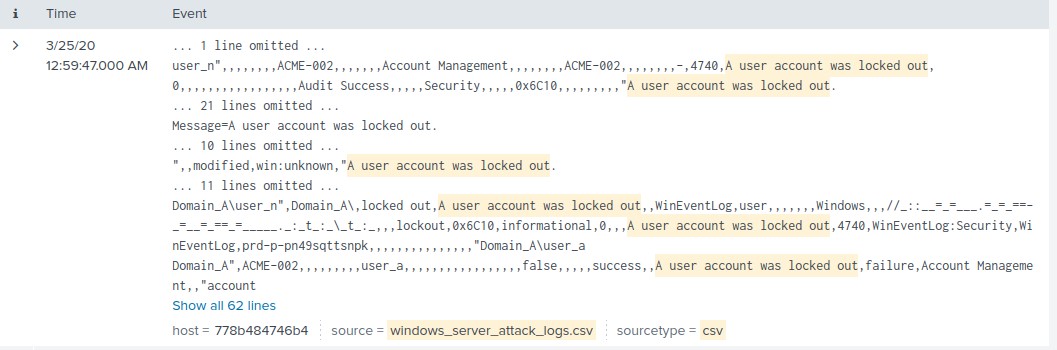
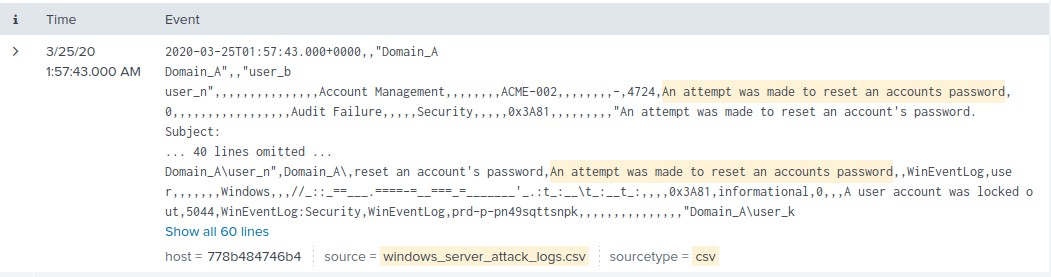
## **Unit 19 SEIM Homework: Protecting VSI from Future Attacks**

### **Part 1: VSI Windows Server Attack**

1. **An attack was done on VSI’s Windows Server on March 25, 2020**
2. **User’s accounts had become compromised, and both Users A and K were impacted.**
3. **Both the SOC team and VSI notified**

**User A: “A user account was locked out” between 1 AM and 2 AM**

****

**User K: “An attempt was made to reset an account’s password” between 9 AM and 10 AM**

**Mitigation of Server attacks against VSI shall be recommended as follows:**

* **All accounts will now be set to a limited number of login attempts no more than 5**
* **Both SOC team and VSI should be notified imminently if 2 lockouts occur within the same 24 hours**
* **The use of “MFI” (Multi-Factor Identification) shall be set up to all users immediately**
* **Password resets will not be more than 2 per 24 hours and will be locked if done so with both SOC and VSI being notified when it happens**

**VSI has insider information that JobeCorp attempted to target users by sending “Bad Logins” to lock out every user. To mitigate against this vulnerability, the SOC team recommends the following mitigation as follows:**

* **Both SOC team and VSI shall be notified immediately of High Severity attacks of Mass “Bad Logins”**
* **All users should be locked out as soon as a set limit of “2 Bad Logins” for more than a set limit threshold of 15 % of users being locked out**
* **IP addresses that are caught shall be put on a Black List immediately**

### **Part 2: Apache Webserver Attack:**

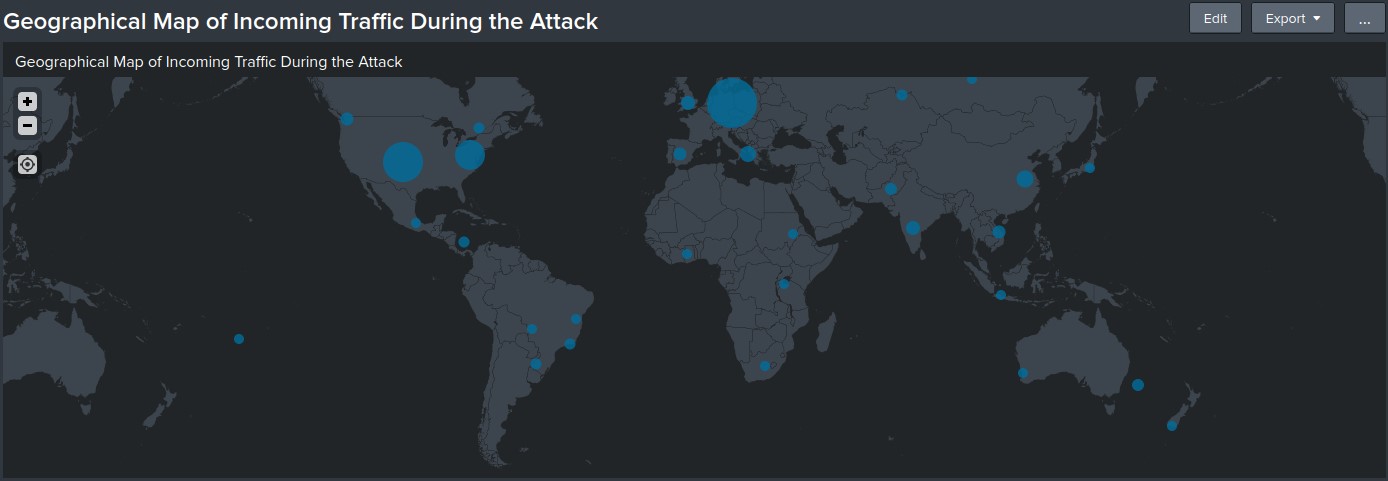
1. **VSI Apache Webserver is Attacked on March 25, 2020, between 6 PM and 9 PM**
2. **The attack was found to be from Kyiv, Ukraine**
3. **Both the SOC team and VSI notified**

**Mitigation of Server attacks against VSI shall be recommended:**

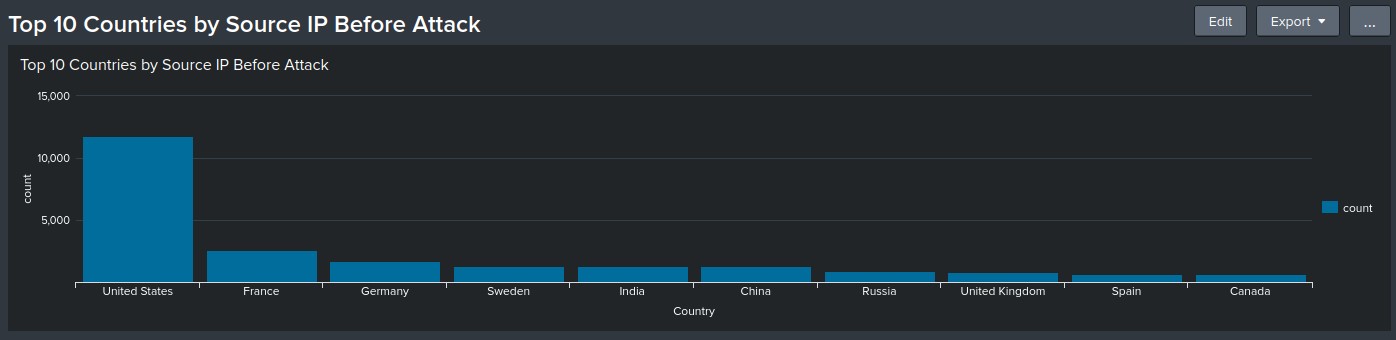
* **“Block all incoming HTTP traffic where the source IP comes from Kyiv, Ukraine”**

**VSI receives very little traffic during normal business hours from Kyiv, Ukraine. The most traffic internationally during attacks comes from Ukraine. It just makes the most sense to block Ukraine from VSI, because they put in the most work for any attacks made internationally. VSI would not show any loss for their day-to-day operations if they block Ukraine.**

**Below are the Screenshot Examples:**

**Geographical Map of Incoming Traffic During the AttackTop 10 Countries by Source IP Before Attack**

**Top 10 Countries by Source IP Before Attack**

****

#### **Top 10 Countries by Source IP During Attack**

**VSI has insider information that JobeCorp will launch the same webserver attack, but use a different IP address each time in order to avoid being stopped by the above firewall rule.**

**To mitigate against future attacks, the SOC team recommends the following firewall rules be implemented:**

* **Block any IP address which generates three or more consecutive POST requests to the login page (/VSI\_Account\_logon.php)**
* **Block any IP address which generates three or more consecutive POST requests identified by the user agent string Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)**