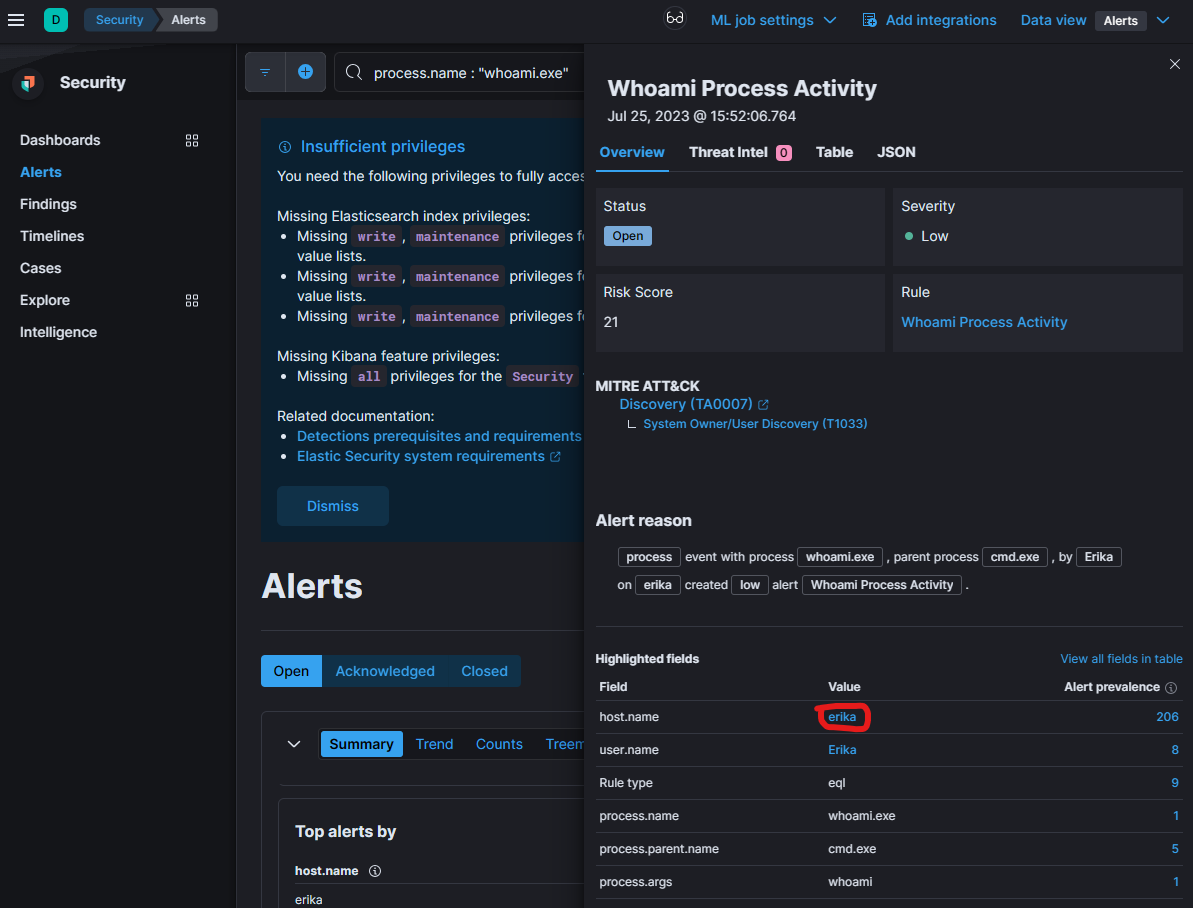
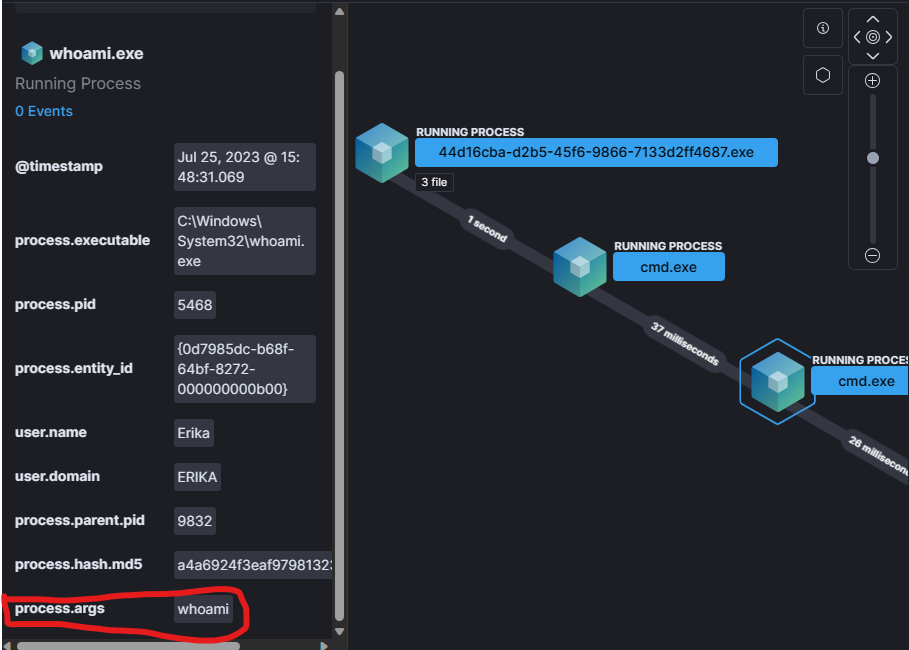
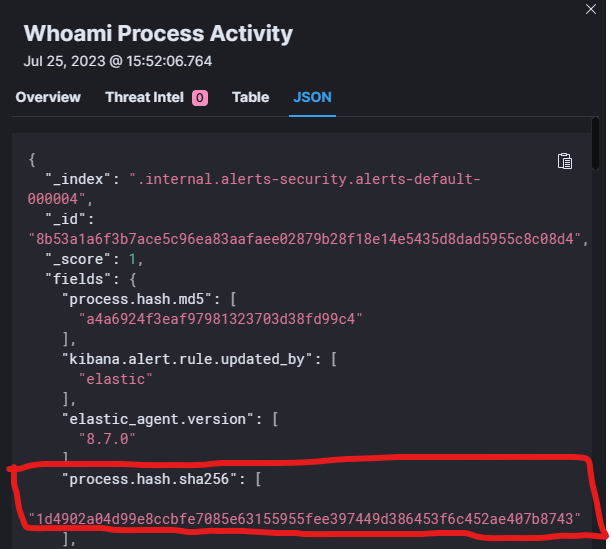
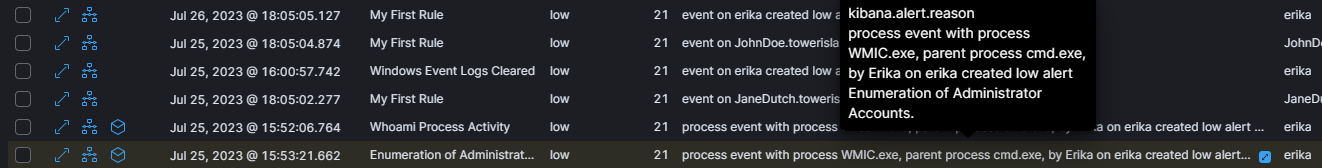
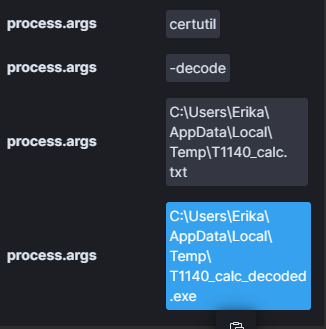
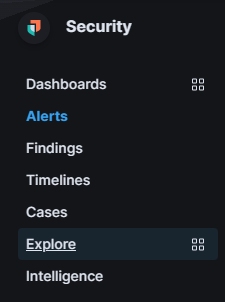
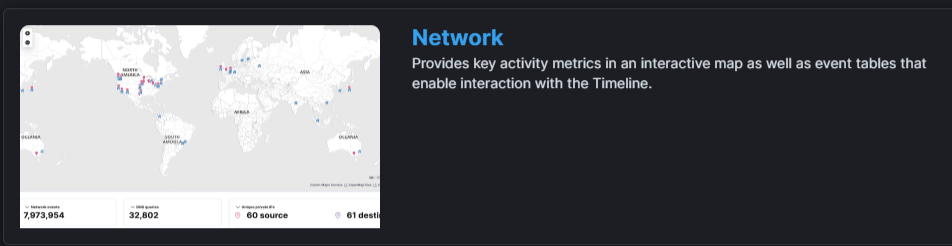
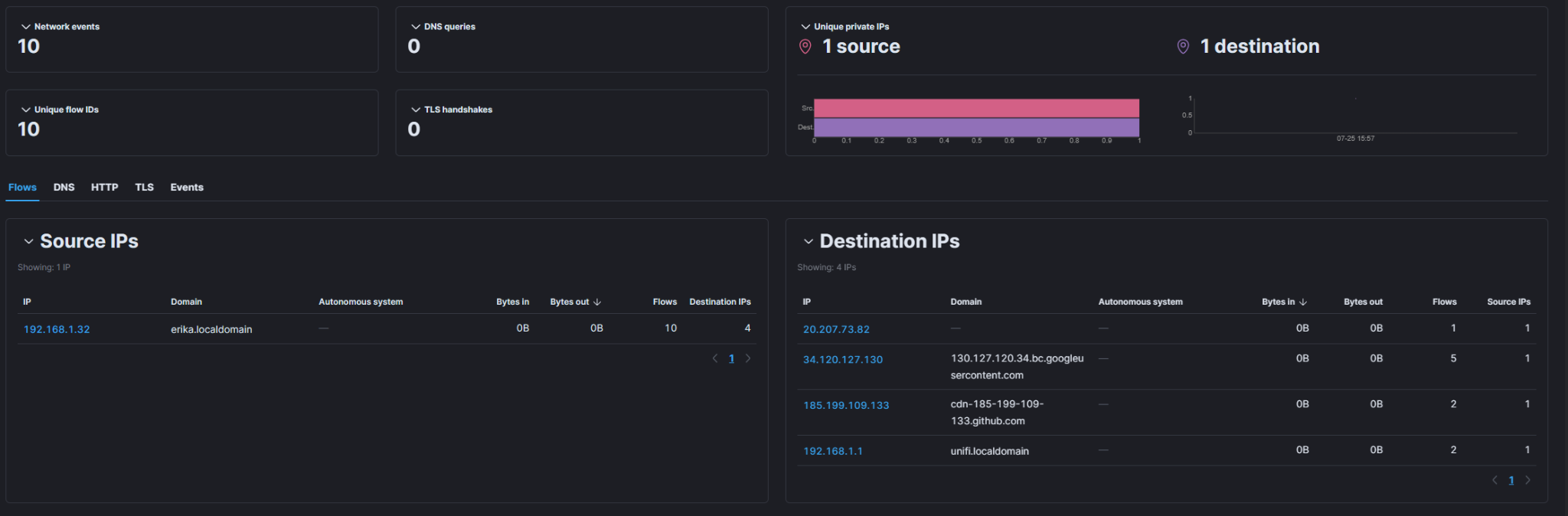
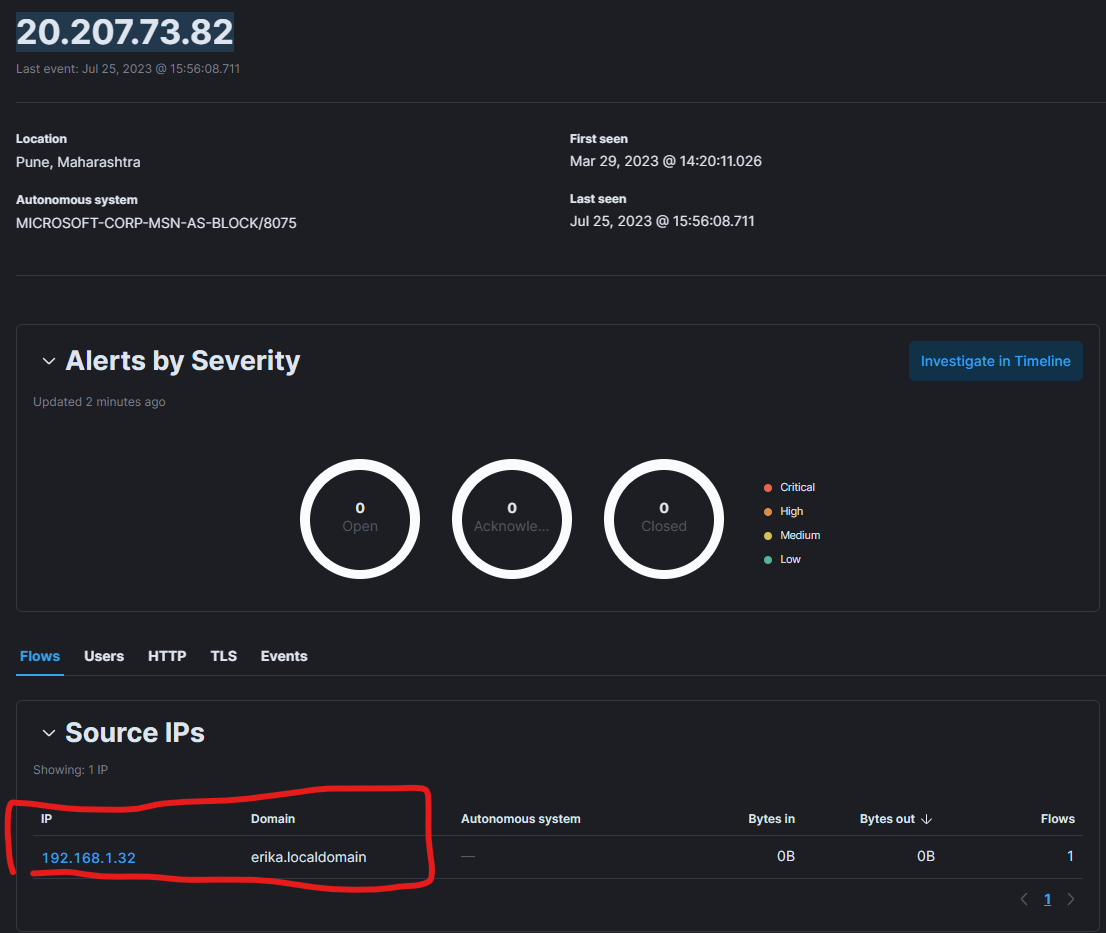
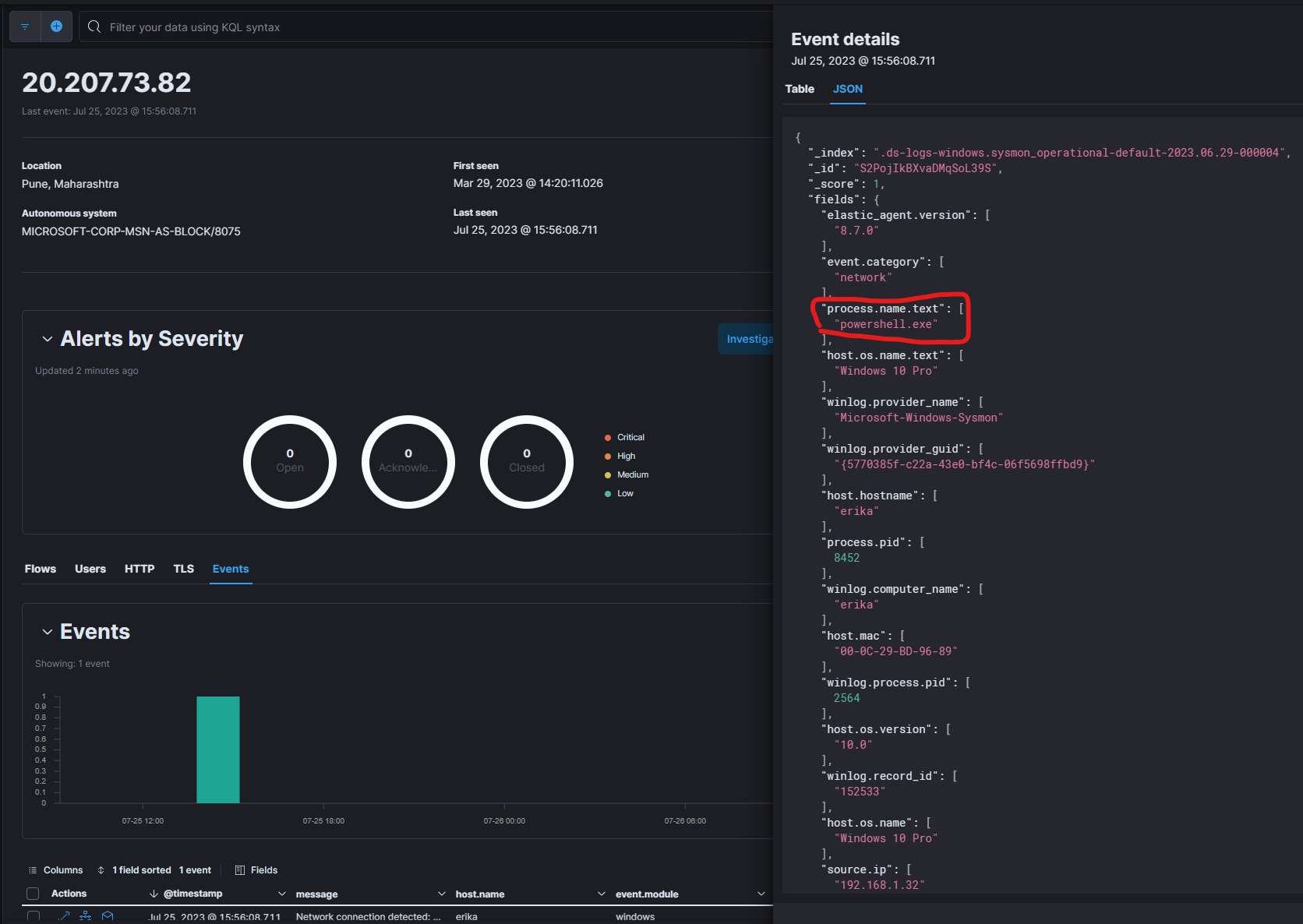
horizontal line

**Plus971 Cybersecurity**

Investigative Report Using Elastic

**26th July 2023**

1. **During this time period an Alert was generated named “Whoami Process Activity”:** 
   1. **What is the name of the system on which this activity was performed?** 
      1. Navigated to the alerts tab in the alerts tab in the security section.
      2. Set the date filter to “Last 24 hours”
      3. process.name : "whoami.exe" 
      4. Using the KQL search bar the following query was run: process.name : "whoami.exe"
      5. Only 1 alert is found and the hostname can be seen in its details.
   2. **What was the command executed, resulting in this alert being generated? Explain what this command is used for.**
      1. By clicking on the box icon on the alert we open the analyzer.
      2. And by clicking on a node we can see more details about the process such as arguments used
      3. And here we can see the command “whoami” is used in cmd.exe
   3. **There is a sha256 hash provided in the alert, what file does this hash belong to?**
      1. Closing the analyzer we can see another button to view more details about the alert.
      2. And switching to the JSON tab we can see the processes SHA256 hash 
      3. Which is “1d4902a04d99e8ccbfe7085e63155955fee397449d386453f6c452ae407b8743”
2. **During this time period an attempt was made to Enumerate Administrator Accounts, how was this achieved? (process name, commands etc. used to perform the attempt)**
   1. Removing the previous KQL syntax the only filter that was applied is the 24h filter
   2. I then changed the rows per page to 100
   3. And read the reasons for all the alerts until I found the following description on the 3rd page.
   4. Viewing the details of the alert lead me to the answers:
      1. process.name : WMIC.exe
      2. process.args: wmic useraccount get /ALL
3. **During this time period some suspicious CertUtil Commands were executed:**
   1. **What is CertUtil?**
      1. A command line program used to display certification authority.
   2. **In this case CertUtil was used to encode a file and then decoded. What is the name of the file that was encoded?**
      1. Using the search bar i searched for “certutil”, which produced 2 alerts
      2. Expanding the first alert via the analyzer yielded:C:\Windows\System32\calc.exe
   3. **What name was the file stored under when it was decoded?**
      1. if we analyze 2nd alert i am led to believe that the decoding was completed and in the arguments of the certutil.exe process we can see 4 arguments provided:
      2. 
         1. The exe’s name “certutil”
         2. The decode flag”-decode”
         3. The file to be decoded “.../T1140\_calc.txt”
         4. And the location of the decoded file “.../T1140\_calc\_decoded.exe”
4. **How many times did the system Erika make an outbound connection to the IP address 20.207.73.82?**
   1. First we go to the explore tab in the security section
   2. 
   3. Then navigate to the network dashboard.
   4. 
   5. After we filter for the last 24 hours we can see 10 flows/network events
   6. 
   7. And in the destination IP we can see the IP address 20.207.73.82, and clicking on it reveals another page.
   8. 
   9. Here we can see erika.localdomain is the only PC to make this connection in the last 24 hours. And the flows show that this connection was only made once.
5. **What executable made the outbound connection to the IP 20.207.73.82?**
   1. Switching to the events tab yields more info on the connection/event and in the json tab we can see that the process that made this request is powershell.exe:
   2. Alternatively in the event details slideout if we type “exe” in the search bar we can see the executables name.