# Incident Ticket Template

*Use the following as a template for generating a ticket to track activity related to a security incident.*

## Detection (network events, host events, external report):

### 

### Initial detection/IoC:

|  |
| --- |
| 2020-06-06 22:00:50 216.154.220.53:80 -> 10.0.0.12:50134 (ET POLICY PE EXE or DLL Windows file download HTTP) |

### 

### Additional indicators (incl. network traffic, host logs):

|  |
| --- |
| 2020-06-06 22:23:03 88.214.26.53:42069 -> 172.31.83.122:5432 (ET SCAN Suspicious inbound to PostgreSQL) |

### 

### False Positives *(Note: in the real world, false positives are not logged in an incident ticket. This section is unique to our project)*

|  |
| --- |
| 2020-06-06 21:57:09 192.168.1.56:36982 -> 34.239.152.87:80  2020-06-06 17:02:09 10.0.0.12:51026 -> 168.63.129.16:53 |

## Containment:

|  |
| --- |
| Contacted Network Operations Center (616-555-4662) and asked the on-call staff to disable the network access to desktop, data center.  Rest the passwords and called the help desk (616-555-4357) to assist with the task. |

## Analysis (other compromised hosts, lateral movement, data exfiltration, etc.):

|  |
| --- |
| Documented the infection path.  Checked for other infected hosts.  Removed network access via the on-call Network Operations Center staff.  Rest all the account passwords.  Investigated unusual activity. |

## Recovery:

|  |
| --- |
| Recover all the lost or compromised files.  Isolate and patch all the infected parts. |

## Post-incident recommendations:

|  |
| --- |
| Train users so that untrusted files are not downloaded.  Update all the un-updated software.  Implement network segmentation.  Reset all the passwords. |