# 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 |

### 

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

|  |
| --- |
| 2020-05-31 13 :14 :43 192.168.0.7:55321 ->203.0.113.12:81 (HTTP request on non-standard port) |

### 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 21:59:17 172.31.90.209:35997-> 172.31.0.2:53 |

## Containment:

|  |
| --- |
| 2020-06-07 08:00:00 I contacted the Network Operations Center (616-555-4662). I spoke with Jack Newton about a malware attack and asked for conn.log and pcap files for further analysis. |

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

|  |
| --- |
| 2020-06-07 08:15:00 I called the Help Desk (616-555-4357) to document that 172.31.0.2 may be infected by a malware. It is also possible that other hosts may be infected as well on 10.0.0.12 when performing a GET request from 216.154.220.53 |

## Recovery:

|  |
| --- |
| 2020-06-07 08:30:00 I contacted the Network Operations Center (616-55-4662) and spoke with Jack Newton to disable the network access to the wall jack (desktop) or the network switch (data center).  2020-06-07 08:35:00 I contacted the Help Desk (616-555-4357) and talked with Cynthia Ab to reset the account passwords for any users as well as for local and administrative accounts. |

## Post-incident recommendations:

|  |
| --- |
| I recommended to reinstall operation systems and restoring a backup from a good save point. I also recommended to:   * put mitigations in place to prevent future attacks * upgrade vulnerable software * add firewall rules * add additional hosts or network defense * change network architecture   My final recommendations will be to update the playbook and schedule security awareness training for the staff. |