# 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  Malware fnpufu.exe  Host: osric.org |

### 

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

|  |
| --- |
| 2020-06-09 190.6.193.152 :80 =>10.0.0.12:50143 (HTTP/1.1)  <http://190.6.193.15:8080/w00nl9tnkeyeyjN0> |

### 

### 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 21:57:09 192.168.1.65:36982 => 34.239.152.87:80  2020-06-06 21:57:09 172.31.90.209:35997=> 172.31.0.2:53 |

## Containment:

|  |
| --- |
| ●  Contact the Network Operations Center (616-555-4662) and ask the on-call staff to disable network access to the wall jack (desktop) or network switch (data center).  ●  Reset the account passwords for any system users, including local and administrative accounts. Help Desk (616-555-4357) can assist with this. |

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

|  |
| --- |
| 1. Check network logs    * ●  Document the path to infection, if known    * ●  Check for other infected hosts (similar network traffic)    * ●  Document any signs of lateral movement    * ●  Document and signs of data exfiltration   Check the antimalware logs, if available. |

## Recovery:

|  |
| --- |
| 1. rebuild the system and restore data from a known good backup before restoring network access. |

## Post-incident recommendations:

|  |
| --- |
| 1. Document all investigation and follow-up steps in the ticketing system. |