# 1Incident 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 21:59:17 172.31.90.209:35997 🡪 172.31.0.2:53  2020-06-06 22:00:50 216.154.220.53:80 -> 10.0.0.12:50134 |

### 

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

|  |
| --- |
| 2020-06-06 22:00:50 173.194.162.74:443- 🡪192.168.1.56:46286(Trojan malware) |

### 

### 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 21:58:20 192.168.1.56:36992 -> 34.239.152.87:80  2020-06-06 21:59:17 172.31.90.209:35997 -> 172.31.0.2:53 |

## Containment:

|  |
| --- |
| At 10:00, I detected an unauthorized access/data breach. Once I confirmed this, I contacted the Network Operations Center and asked the on-call staff to disable network access to the wall jack or the network switch. |

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

|  |
| --- |
| Using the logs and other tools, I determined that there was a malicious url on the network and expanded my scope of investigation. |

## Recovery:

|  |
| --- |
| Reset user credentials, including admin credentials and local credentials, on the host.  The host should be rebuilt and restored from a well-known good image before it is returned to the network. |

## Post-incident recommendations:

|  |
| --- |
| The playbook does not say how the user credentials, admin credentials, and local credentials should be reset.  The playbook does not stay how the host should be rebuilt. |