Template - Horizontal port scan initiated

Link to alert

**Description**

The device is initiating connections to various ports on another device. This might be an attempt to discover open ports on the remote device.

**Classification**: Incident

**Alert detail**

User:

Device name:

Application:

Initial detection:

Outbound connection:

Severity:

**Remediation**

A. Validate the alert.

1. Investigate the process that initiated the connections.

2. Check for other suspicious activities in the machine timeline.

3. Locate unfamiliar processes in the process tree. Check files for prevalence, their locations, and digital signatures.

4. Submit relevant files for deep analysis and review file behaviors.

5. Identify unusual system activity with system owners.

B. Scope the incident. Find related machines, network addresses, and files in the incident graph.

C. Contain and mitigate the breach. Stop suspicious processes, isolate affected machines, decommission compromised accounts or reset passwords, block IP addresses and URLs, and install security updates.

***NB: PROVIDE A SCREESNHOT OF THE WORK DONE***