

# Wonderland SOC

## Incident Investigation Notes

**Finding name:**

**Analyst assigned:**

Description of System(s)	
Type (Laptop/Desktop/Server/VM/etc.)	
System Operating System	
System Name	
System IP Address	
Other hosts involved: Hostname/IP address	

User information (as applicable)	
User(s) involved in incident	
Other user(s) alias involved	

MITRE ATT&CK info	
Tactic / Technique - ID	

# Wonderland SOC

## Incident Investigation Notes

### Investigation Details

### Additional Artifacts

### Final Analysis

# Wonderland SOC

## Incident Investigation Notes

### SPL Searches