WGU Fowl Owls
CCDC Team

Network Incident Response

Incident Number

Date

Analyst Name

Reporter Name

Reporter Name

Phone Number

E-mail

Team Number

Incident Information

Date of Incident

Time of Incident

Machine/MAC address

Source IP

Destination IP

Subnet with CIDR

TYPE OF INCIDENT:

- ☐ Outage
- ☐ Malware
- ☐ Shellcode
- ☐ Other: _____
- ☐ Unauthorized Access
- ☐ Data Breach
- ☐ Remote Execution
- ☐ DDOS
- ☐ Exploit
- ☐ Recon

400 S 700 E #300
Salt Lake City, UT 84107

801-274-3280

wgumobile@wgu.edu

WGU Fowl Owls
CCDC Team

Summary of what happened

400 S 700 E #300
Salt Lake City, UT 84107

801-274-3280

wgumobile@wgu.edu

WGU Fowl Owls
CCDC Team

Systems Involved

First Detection

PORT / Protocols

IP Address

OS

Alternative Identification

How was it Detected?

How did we remediate?

400 S 700 E #300
Salt Lake City, UT 84107

801-274-3280

wgumobile@wgu.edu