SPIKE **S**tructure **P**recise **I**ncident **K**nowledge **E**xtract

1 Incident Identifying Personnel

Name	
Position	

2 Time Incident Detected: _________:_________ Local time

3 Type of Incident Detected

Denial of service		Unauthorized User / use		Unplanned Downtime	
Malicious code		account compromise		Other (Fill 3E below)	

3E Other: [ ]

4 Indicators of Incident (log, alert, pcap, IDS flags, etc)

Device Location	
File location	
Indicator	

5 Systems effected

Physical device	
Service	

PROCEED TO SOE FOR IR CONTINUATION. FILL BLOCKS 6 THROUGH 9 AFTER RESOLUTION

6 Measures Implemented

Containment	
Eradication	
Recovery	

7 Responder(s) Identification

Name	Position

Incident Follow-up

8 Lessons Learned

9 Future Preventative Measures

Sequence of Events after Discovery (can be multiple pages)

:	
:	
:	
:	
:	
:	
:	
:	
:	
:	
:	
:	
:	
:	
:	
:	