We thank you for your time spent taking this survey.
Your response has been recorded.

10/10 **100.0%**

A(n)_____ is an occurence with the potential to negatively impact the confidentiality, integrity or availability of information stored, processed or transmitted through HAL systems or networks. **1/1**

Event

Adverse Event

Incident

Disaster

A(n)_____ is an adverse event that has transpired, and actively threatens the security of information within HAL systems or networks, but not the overall continuity of HAL operations. **1/1**

Event

Adverse Event

Incident

Disaster

Which of the following is not a valid incident containment strategy or procedure? **1/1**

Disabling compromised user accounts

Reconfiguring a firewall to block the problem traffic

Temporarily disabling the compromised process or service

Taking down the conduit application or server—for example, the e-mail server

Stopping all computers and network devices

All of these are valid incident containment strategies or procedures

None of these are valid incident containment strategies or procedures

All Team IR Liaisons should submit all IR documentation and forms using _____ addressing all communications to _____. **1/1**

- **Email / ciso@halcorp.biz**
- Interoffice Mail / CCCO
- the Service Desk System / CIO
- None of these

If an adverse event is determined to be an incident, the CSIRT assesses the severity and scope of the incident, and _____. **1/1**

- **initiates IR procedures and starts an IR form capturing key information regarding the incident**
- notifies the CIO's office immediately
- immediately isolates all affected systems from the network
- declares a state of emergency and requests IR support from corporate headquarters

If an adverse event is determined to be an incident, the CSIRT assesses the severity and scope of the incident, complete systems recovery and submits the IR from reporting their initial findings within _____ . **1/1**

- 1 hour of incident detection
- 1 hour of system recovery
- **3 hours of incident detection**
- 3 hours of system recovery

The CISRT will only take those steps necessary to regain control of HAL systems and networks, minimizing _____. **1/1**

- the cost of personnel and support services
- **disruption of HAL services and business functions**
- network down time
- the amount of employee overtime

An Incident is deemed resolved, and IR procedures completed when: **1/1**

the incident is contained

control of all systems have been regained

the incident and resulting damage has been documented

all systems and services have been restored to normal

the proper IR forms have been submitted to corporate

all of these are correct

none of these are correct

Incident case numbers should be developed using the following format: **1/1**

date(mmddyy)-branch letter - incremental number

branch letter-date(mmddyy)-incremental number

branch letter-incremental number-date(mmddyy)

None of These

All modifications to HALs systems in response to a documented incident are pre-approved under the provisions of the _____as per the Change Management Policy and Procedures. **1/1**

Emergency Change Class 2

Routine Change Class 1

Unknown Change Class 4