Cyber Security Incident Response Plan

Table 1 - Control Satisfaction

Standard	NIST Category	Controls Satisfied	Audit Controls
NIST 800-53rev4	-	-	-

Table 2 - Major Document History

Date	Comment	Who
12/19/2019	Initial Doc	Tharp

Response Plan Overview

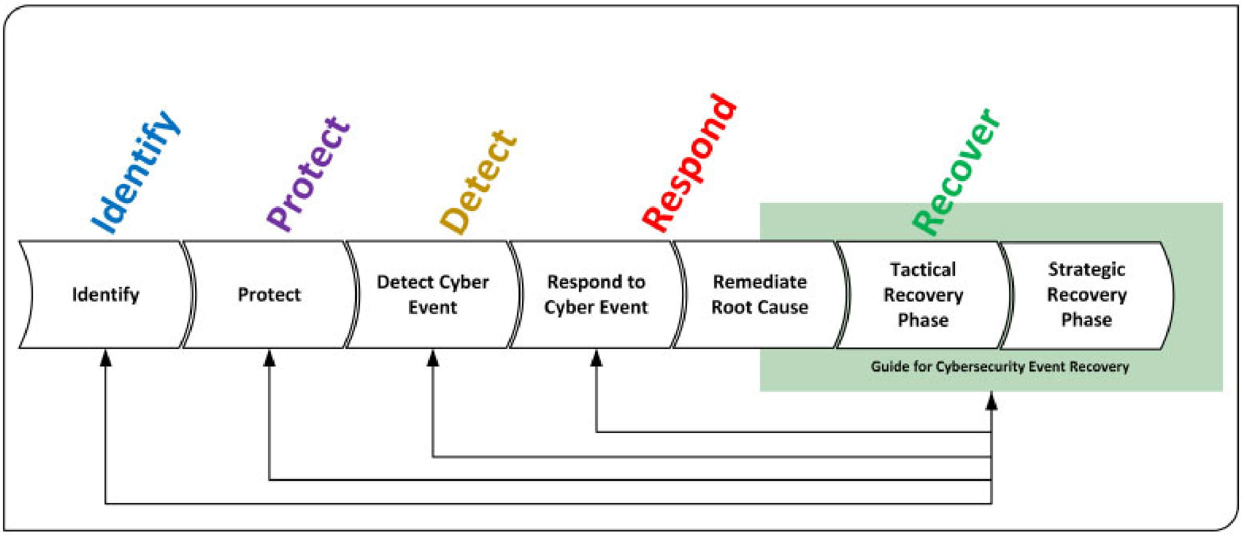

Figure 3-1: NIST SP 800-184 Guide for Cybersecurity Event Recovery Relationship with the NIST CSF

Response Plan Compromised Instance or exposed Access Keys

1. Change the root password and passwords for all IAM users
2. Add / Validate MFA for all Admin users and console access users
3. Create new EC2 key pairs and update instances (delete compromised keys)
4. Relaunch the instance and create new AMI to relaunch if needed; edit ssh/authorized keys file
5. Rotate and delete IAM access keys
6. Delete unrecognized or unauthorized resources
    - Instances
    - IAM Users
    - Spot Bids
7. Contact AWS Support

    - Respond to abuse notifications

Often times the worst attacks occur after the first vulnerability appears to have been remediated. Be Vigilant!!!