ACME Incident Response Plan

Produced by: Marvin the Martian SOC

Commissioned by: WIley E. Coyote

Date: 11/05/2022

Incident Response Overview

Preparation, detection, containment, investigation, remediation, and recovery are the six phases that make up the fundamental event process. NIST SP 800-61 provides a definition of these phases. The whole incident response process followed by the ISO (Information Security Officer) comprises detection, containment, investigation, remediation, and recovery. From a governance standpoint, this plan serves as the main road map for the preparation stage; local policies and practices will enable the ISO to be prepared to handle any crisis. Reassessing whether the preparation or techniques employed in each step are appropriate and changing them if necessary are part of the recovery process.

Preparation

The ISO can respond to an incident with the help of preparations such as policies, tools, processes, good governance, and communication strategies. Preparation also suggests that the impacted parties have put in place the safeguards required to recover and go on with business after an incident is recognized. Continuous improvement of this stage should be based on post-mortem examinations of earlier instances.

Detection

Discovery of the event via security tools or communication of a suspected incident by an internal or external party are both examples of detection. The declaration of the incident, its

initial classification, and any initial notifications mandated by contract or law are all included in this stage.

Containment

The triage stage known as containment is when the afflicted host or system is located, isolated, or otherwise mitigated. It is also during this stage that the affected parties are informed, and the investigative status is determined. Seizure and evidence handling, escalation, and communication sub-procedures are all included in this phase.

Investigation

During the investigation stage, ISO staff members determine the incident's severity, scope, risk, and root cause.

Remediation

Remediation is the process of restoring compromised systems after an incident, informing affected parties, communicating with them, and doing an analysis to verify the threat has been eliminated. All regulatory needs are decided upon by key stakeholders, as are all internal and external communications. The post-mortem will be finished now, regardless of any official findings, as it might impact the investigation and interpretation of the occurrence.

Recovery

Recovery includes gathering data, analyzing the incident for procedural and policy effects, and incorporating "lessons learned" into future training and response efforts.