Pittsburgh Public Schools

Expect great things.

Pittsburgh Public Schools

Standard Operating Procedure

IT Investigation Norms

Office of Information and Technology

OIT-006

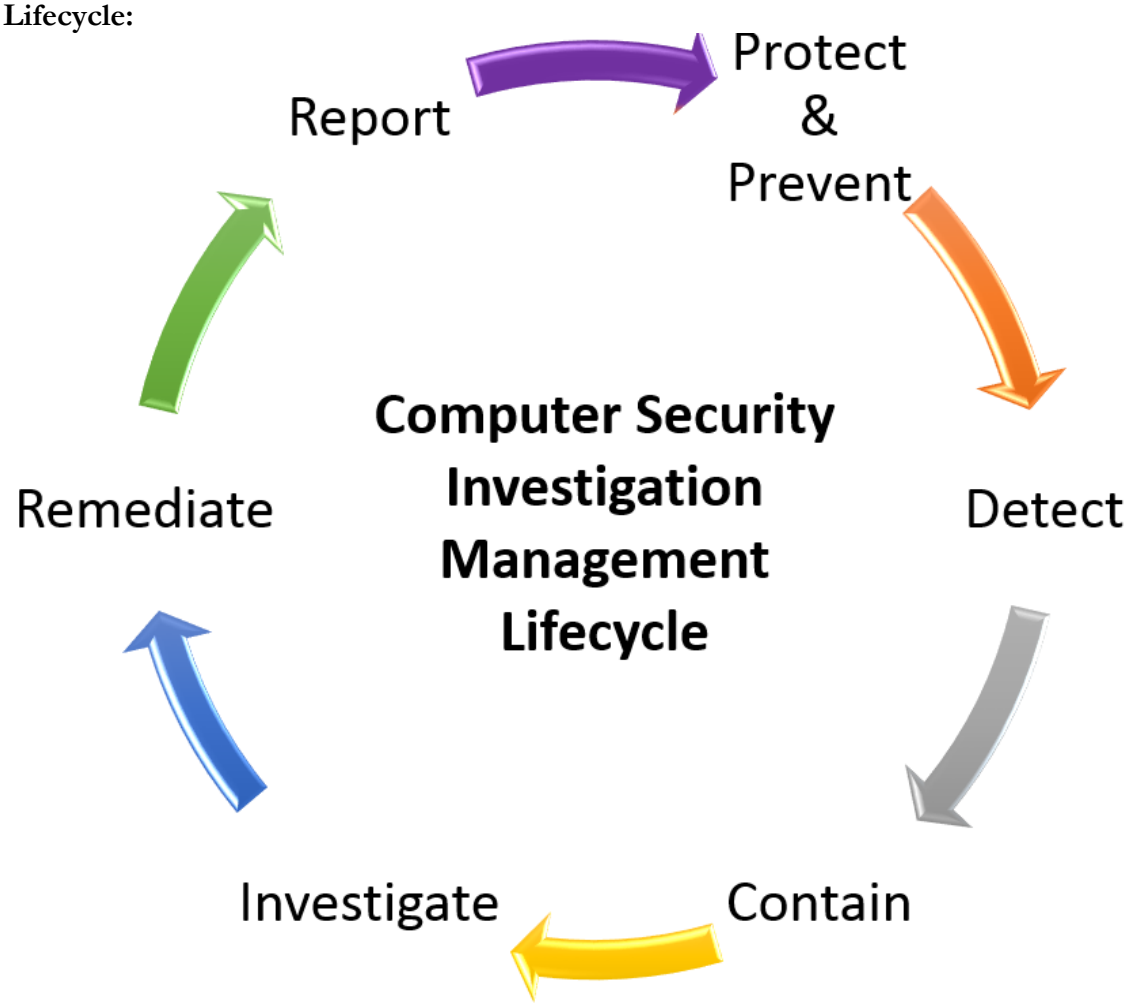
Pittsburgh Public Schools | 341 S Bellefield Ave Pittsburgh PA 15213
Support: 412-529-HELP (4357) | support@pghschools.org

IT Security Investigation

Overview:
This document describes the overall lifecycle for responding to information security events at the Pittsburgh Public Schools. It defines the roles and responsibilities of District personnel, characterization/classification of incidents, relationships to other forms, policies and procedures, and reporting requirements. The goal of the Security Investigation Lifecycle Management Guidelines is to detect and react to computer security incidents, determine their scope and risk, respond appropriately to the event, communicate the results and risk to all appropriate individuals as well mitigate the likelihood of the incident from reoccurring.

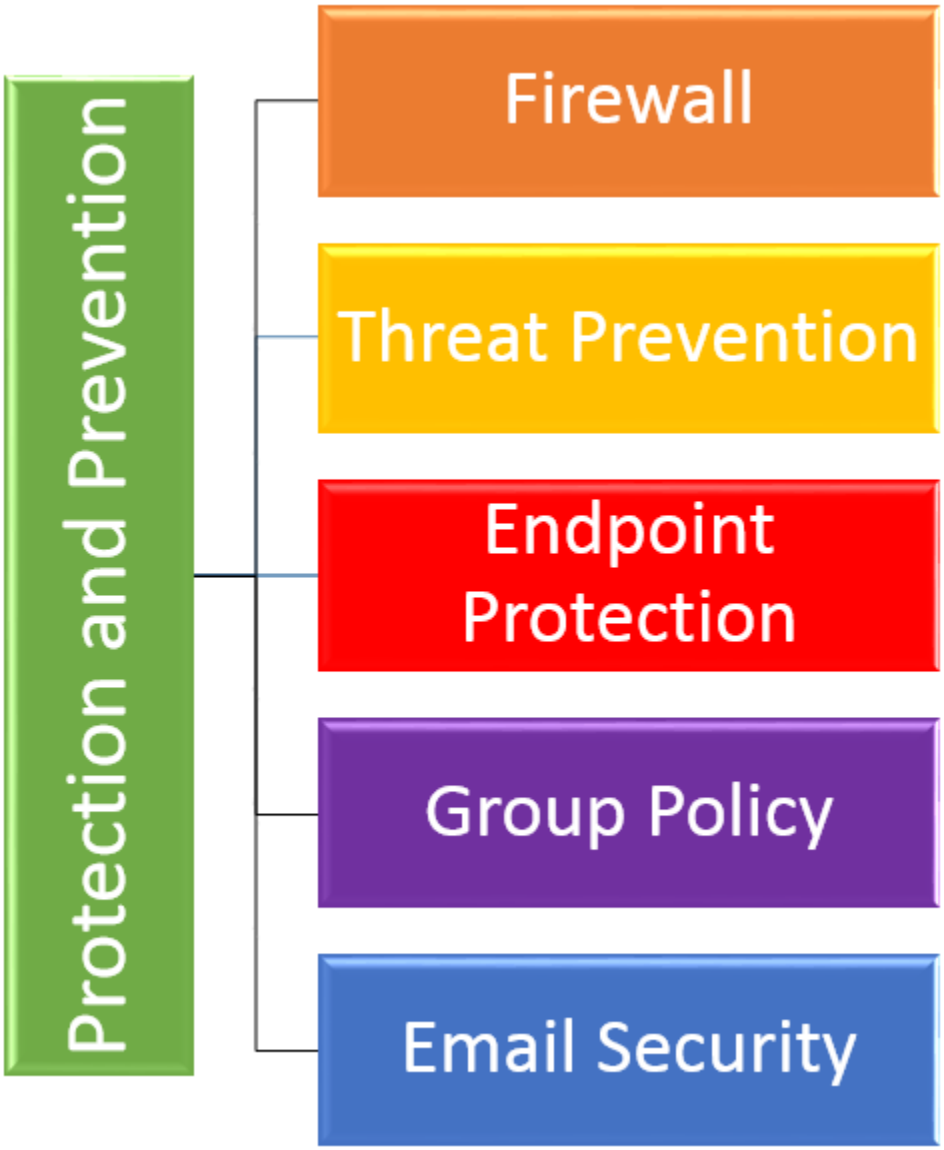
Definitions
Event - An event is abnormal activity to the normal standard operation of IT infrastructure, systems, or services. Not all events become incidents.
Incident – An incident is an event, that when assessed by network security personnel, violates one of more District policies, standards or otherwise threatens the confidentiality, integrity, or availability of District resources.
Network security personnel will assign each incident a Risk Score utilizing the Risk Score Matrix as a general guide. The Risk score assigned can have many variables and the assigned Risk Score is at the discretion of network security personnel. The Risk Score is utilized for prioritization of internal resources only. The Risk Score may change during the course of an investigation.
Law Enforcement - Law Enforcement includes the School Police, Pittsburgh Police, as well as federal and state law enforcement agencies, and U.S. government agencies.
Designated District personnel – Requests for computer security investigation of staff can be initiated by the Office of School Safety and the Office of Human Resources, or their designated parties. Request from other parties will be informed that one of the aforementioned departments must be contacted to start the process officially. Requests for computer security investigation of students can be initiated by the principal of the school that the student attends or by the Office of School Safety. Requests for both staff and students can be initiated at any point in time by network security personnel based upon security management tools and/or routine security monitoring.

Lifecycle:



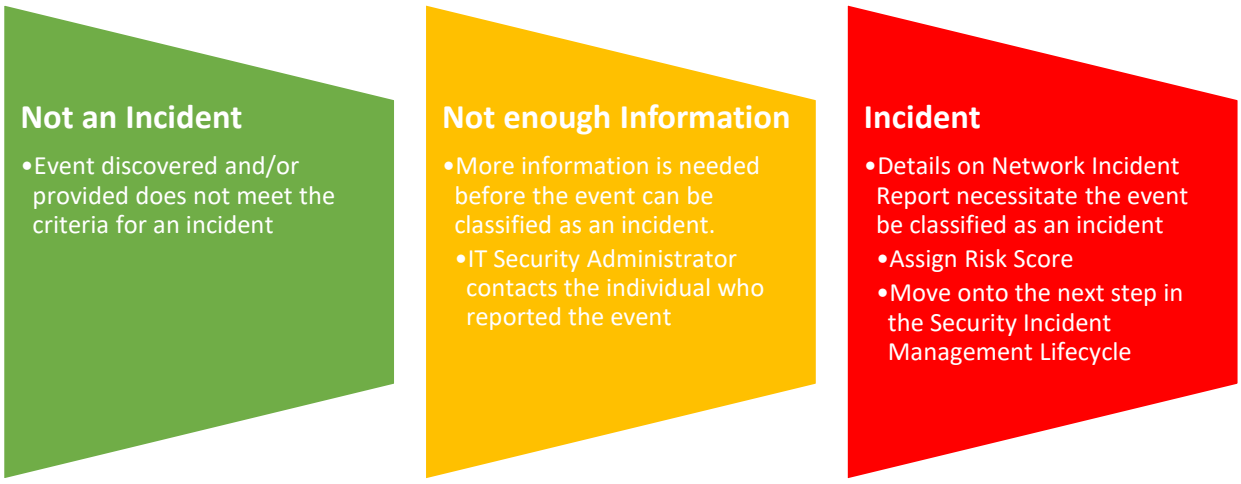
Protection and Prevention:
Primary Responsible Party: IT Security Administrator
Secondary Responsible Party: Network Security Assistant
Protection and Prevention tasks are proactive activities undertaken on a consistent basis by Network Security personnel. These activities include (but are not limited to): monitoring and tracking traffic, utilizing an enterprise-class application centric firewall, filtering internet bound traffic, and utilizing

enterprise class endpoint protection to help prevent and protect the Pittsburgh Public Schools Infrastructure and resources



Detection
Primary Responsible Party: IT Security Administrator, Director of Infrastructure and IT Services
Secondary Responsible Party: Network Security Assistant
Detection is the initial discovery of an event. Discovery of an event can be via automated security management tools, routine security monitoring, notification via designated District personnel, or

notification via external entities (Internet Service Provider, Law Enforcement, etc). Detection involves gathering as much critical information regarding the event as possible.
If information regarding an event is coming via District personnel or external entities, the Network Event Report form should be filled out with as much information as possible and sent to the Director of Infrastructure and IT Services. The more information that is provided, the easier it is for network security personnel to determine if the event is an actual incident and can help classify the incident appropriately. The Director of Infrastructure and IT Service will inform the IT Security Administrator of the event and provide the completed Network Incident Report. If the IT Security Administrator is unavailable, the Network Security Assistant and/or Network Administrator should be notified. If the information is coming from security management tools and/or routine security monitoring, network security personnel will fill out Network Incident Report.
After reviewing initial information, an initial Risk Score will be assigned. (Figure 1). If the event is classified as an Incident, network security personnel will assign a Risk Score utilizing the Risk Score Matrix as a general guide. The Risk score assigned can have many variables and the assigned Risk Score is at the discretion of network security personnel. The Risk Score is utilized for prioritization of internal resources only.
Figure 1.

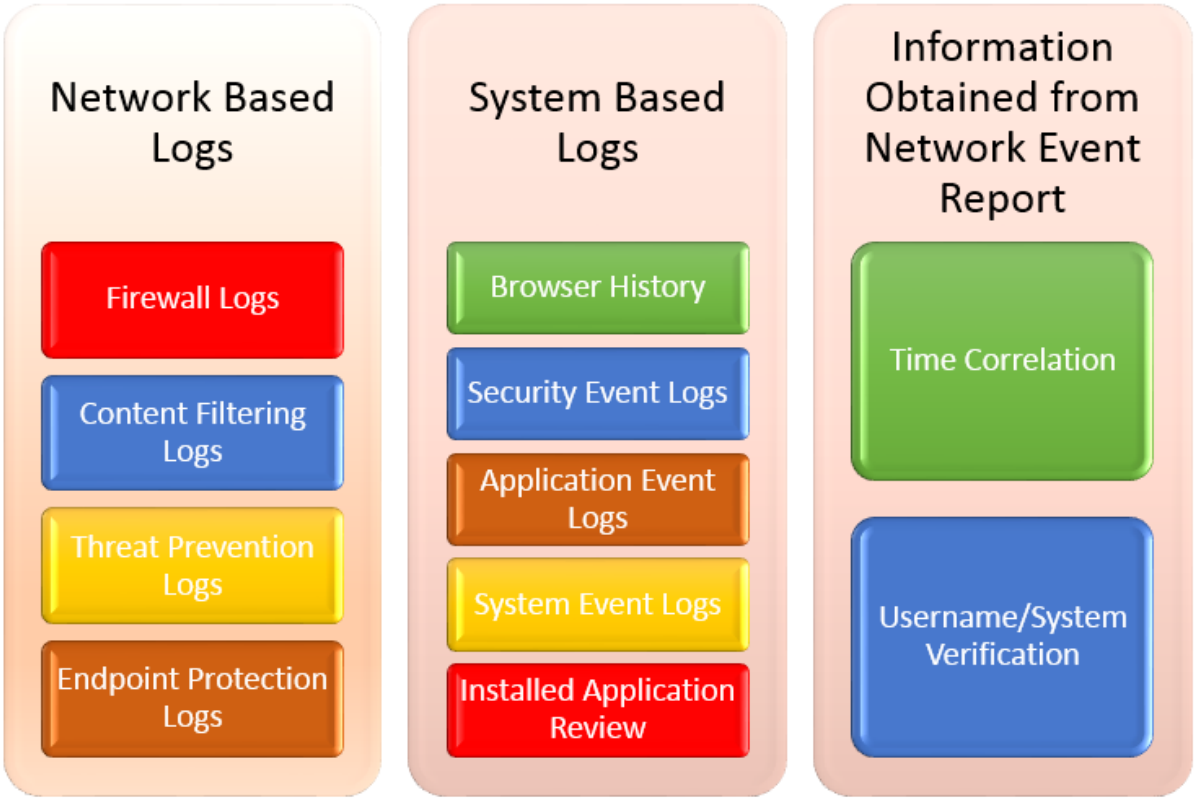


Containment
Primary Responsible Party: IT Security Administrator, Director of End User Services
Secondary Responsible Party: Network Security Assistant
Containment is the triage phase where the affected host or system is isolated and confiscated. Network security personnel will notify the Director of End User Services via the following mechanism based upon the Risk Score if a device needs confiscated and/or physically removed

from a site. Network security personnel will make best effort to provide as much detail as possible to assist the Field Service Technician with locating the device. Field service Technician will create a duplicate image of the device at the request of Network Security personnel. This is based upon the Field Service Technician coverage schedule of 6:00am until 6:00pm Monday through Friday.

Investigation

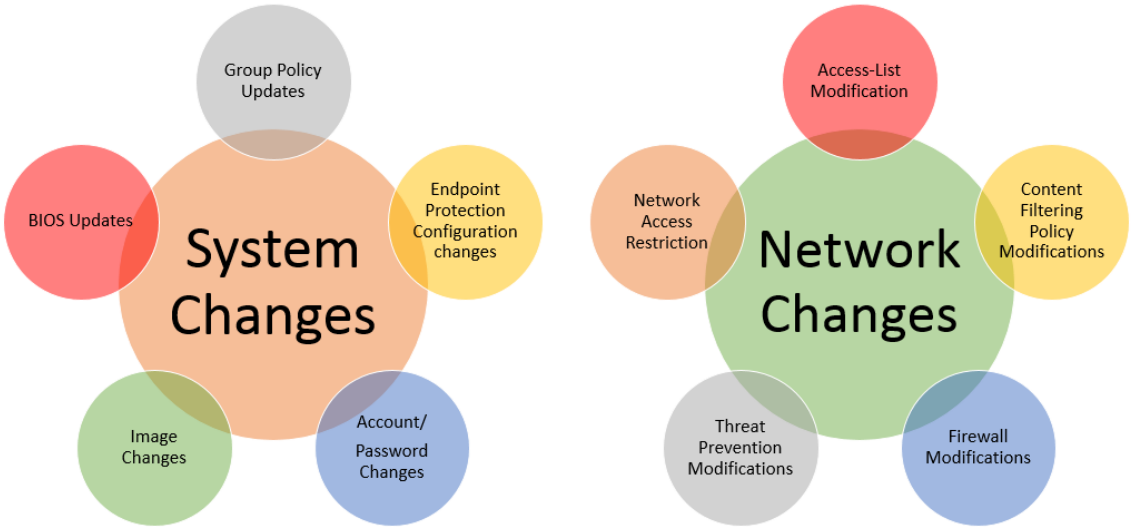
Primary Responsible Party: IT Security Administrator
Secondary Responsible Party: Network Security Assistant
Investigation is the phase where Network security personnel utilizes network based logs, system-based logs, and other information to attempt to determine whether or not the incident actually occurred as well as determine a root cause of the incident (if applicable).



List is not comprehensible and an investigation may include more logs and/or tools then mentioned above.

Remediation
Primary Responsible Party: IT Security Administrator
Secondary Responsible Party: Network Security Assistant

Remediation is sometimes necessary depending on the type of incident that occurred. Remediation task could include making central system changes, network level changes, or site based system changes depending upon the type of investigation that occurred. All remediation mentioned may not need to be performed based upon the outcome of the investigation.
All District devices, if the incident is founded, are required to be reimaged before being returned.



List is not comprehensible as remediation may include more changes then mentioned above.

Report
Primary Responsible Party: IT Security Administrator
Secondary Responsible Party: Network Security Assistant
Reporting is when the evidence is summarized into a tangible document to forward to the necessary resources. Reports will follow a standard template. All reports are stored in a secure location. Screenshots of evidence will be maintained as well.

Sample Incident Report

Pittsburgh Public Schools
Expect great things.

Acceptable Use Policy Violation

Device Information

Device Name: lt-306-spare684
MAC Address: 10-4A-7D-2C-35-3A

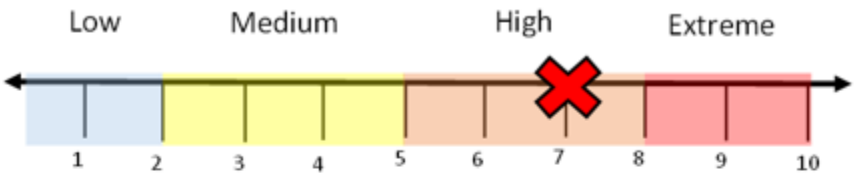
User Information

Username: ststudentuser
Name: Student User
ID Number: 00XXXXXXX

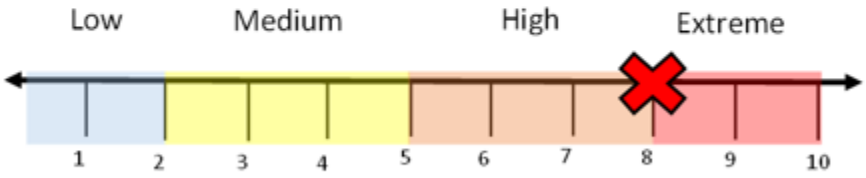
Violations

During routine security monitoring, the student in question was identified as violating the District's Acceptable Use Policy. The student listed below violated the following sections of the Acceptable Use Policy:

Logging on with a username and password other than their own User Account
Student logged into the device with the local system administrator account.



Infiltrating computer system security
Student has multiple hacking tools and visited multiple websites (with evidence of paying for the aforementioned services) that are used for the purpose of conducting illegal denial of service attacks. The student was utilizing network sniffers while actively connect to the District's network infrastructure.



Security Resources assigned to Investigation

Andrea Niedbala-Williams – aniedbalawilliams1@pghboe.net
Steven Tichenor – stichenor1@pghboe.net

General Information

Reporter's Information:

Name: _____ Date Detected: _____

Title: _____

Department: _____

Phone:_____

Email Address:_____

Signature:_____ Date Signed: _____

Event Information

Type of Event:

☐ Inappropriate Web Content ☐ Hacking ☐ Unauthorized Software

☐ Misuse of Systems ☐ Unauthorized Account Access ☐ Other: _____

Event Information:

Location: _____

Name: - _____

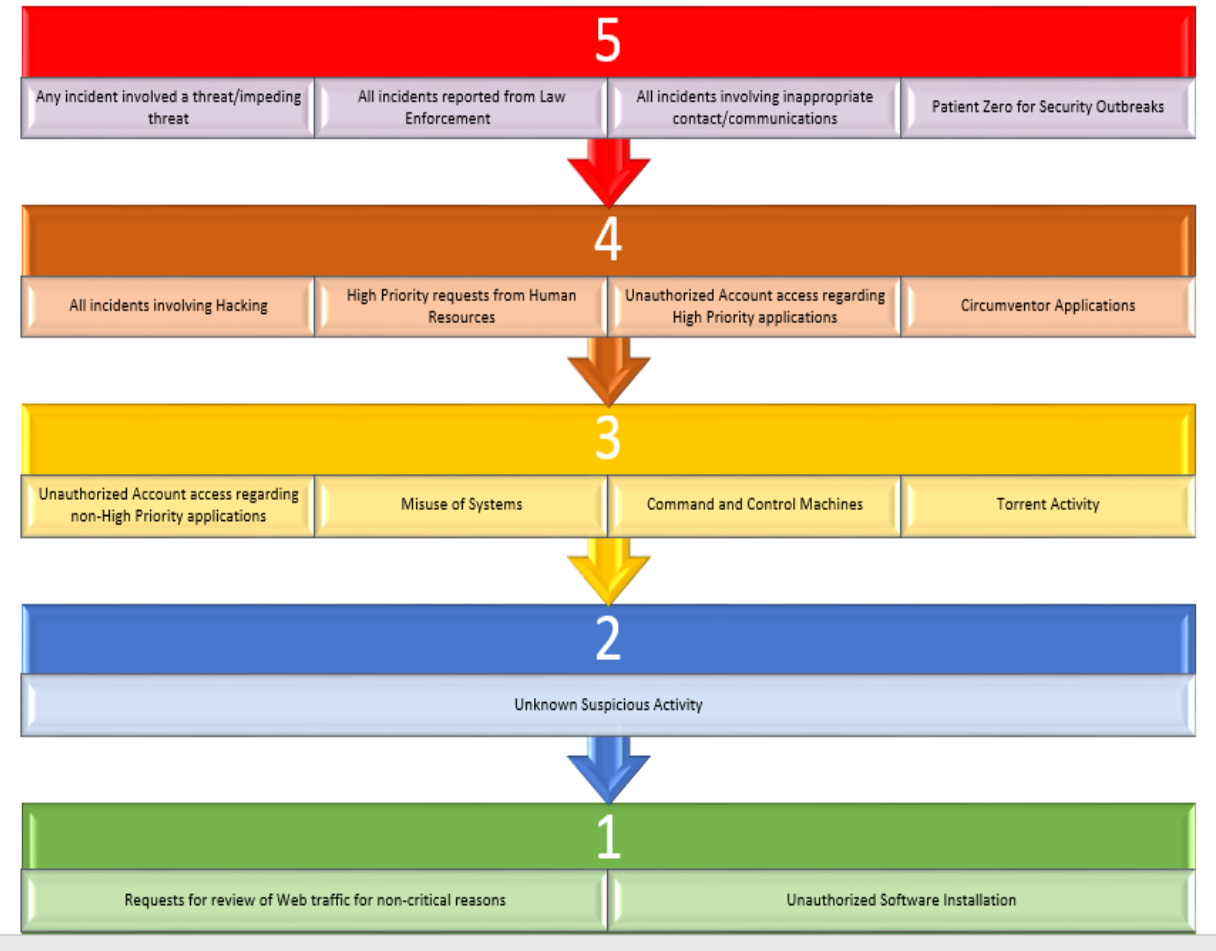
IP Address of Device to be Investigated: _____

Date(s) of Event: _____

Summary of Event: _____

OIT USE ONLY	
Date Received: _____	Initial Risk Score: _____
Event Number: _____	Date of Final Report: _____

Risk Score Matrix



List is not comprehensive and subject to change based upon circumstances of a given incident.