Standard Categories for Incident Response Teams

Definitions V2.1

February 2018

Introduction

This document outlines categories that Incident Response Teams can use to track the types of work that they are involved in. Although it can be used 'stand-alone' it is also used in conjunction with the document;

Standard Categories for Incident Response Teams (Joint Metrics)

Steering Committee

The purpose of the steering committee will be to initially define the incident categories, perform web searches for similar systems and to oversee changes. Initially the SC will meet as and when necessary, until version 1 of the 'standard definitions for incident categories' document has been agreed. After this time, it is proposed that they meet quarterly to assess any changes to the categories or their definitions.

At the time of writing, the SC comprises of;

Patrick Green – University of St Andrews
Jordan M. Schroeder - UCSS InfoSec

Definitions

For the purposes of the document,

Incident: a security event which requires action from the internal security team. This does not include events which do not become incidents. Events can also be logged, as an addition.

Event: An alert or log from a system that indicates that an attempted attack has happened (for example a firewall log entry log for an SSH brute force attack).

Each incident is split into 2 designations;

Major: the main category, which the metrics are devised from. This is a large grained approach, which allows for simple graphing and comparison of trends across different entities.

Minor: these are subtypes of the major category and are loosely defined here as examples to allow entities to identify which Major designation fits. Local entities are encouraged to build finer grained metrics based on minor designations, so that they can add reporting value to their constituents.

This document outlines the standard incident response categories. Each category is outlined in a standard format,

Major Designation
Definition
Example minor designations

Where a device had multiple incidents (for example more than one case of malicious code) only one entry into the correct category should be made. This aims to prevent data becoming skewed, when a machine has multiple infections.

For situations where a single incident may infect multiple machines, each one should be counted separately (for example, where a worm infects many machines). This will give an indication of how large the outbreak is.

Logging

When logging incidents, the following template can be used;

Major Designation: number of incidents (number of events)
Minor designation: number of incidents (number of events)

Where the number of minor designations should not be more than the total number of the major designation (there is a possibility that it is fewer, if not all minor designations are separated out). For example;

Unauthorised access: 3 (7)
SSH brute force: 2 (6)
SQL injection: 1 (1)

For 3 unauthorised access incidents, 2 were through SSH passwords being broken through brute force and 1 SQL injection. In total, there were 6 brute force attempts and 1 SQL injection attempt.

Categories

Below are the proposed definitions for the categories.

External Investigation

An external investigation covers those incidents which require the services of the security team following a request from an external authority such as law enforcement or intelligence services. Such incidents will likely involve log file analysis, disk or email forensics and/or network forensics.

This category is specifically for those incidents where the results of the investigation are to be passed on to aid the investigation of the requesting authority (e.g. in the case of a criminal offence being committed). It does not include incidents for which the security team has been alerted to by, for example, another security team. Those should be logged under the category that the investigation concludes as the root cause. This category is distinct from "Internal Investigation" though may well result in such an incident as well.

Minor designations
Please provide information on the following IP address
Please provide log files for the following user

Malicious Code

This category covers those incidents where some action is required of the security team following a machine being 'infected' by malware.

This category is specifically for incidents where the root cause of the compromise is deliberately created code which has automatically exploited

vulnerability on the system in question. This will include viruses, trojans, worms, and botnets as well as code embedded in web pages or email attachments (up to and including user persuaded to download something they shouldn't). It is distinct from "Unauthorised Access" incidents where an attacker has gained entry to a system by some means and then downloaded malicious software onto the machine.

Minor designations
Ransomware
PUP
Zeus

Internal investigation
This category is used to cover any situation in which the Acceptable Use Policy of an organisation is breached by a user that is bound by that AUP. Breaches do not have to be intentional, so the category can be used to record mistakes as well as wilful breaches.

Here, we also include incidents such as Internal Investigations, where log file analysis, disk forensics, email forensics and / or network forensics are used to support internal departments such as HR / Legal during their investigations. It also covers incidents such as lost or stolen devices.

This category is distinct from any investigations internal to the security team in order to understand the root cause of another incident. This category should also be used where misconfiguration leads to an investigation (for example a machine configured as an open DNS resolver). Another use for this category is for incidents that require significant investigation by the security team, but at completion no security or policy breach has been found.

Minor designations
What websites did this user look at?
This server is vulnerable to this attack, please can you fix it

Copyright infringement
This category covers any incident from an entity which outlines a breach of copyright. This would most commonly be film, music or software but may also include items such as journals, reference books etc. This category also includes IPR infringement, so trademark complaints etc.

Minor designations
The following IP has been uploading our intellectual property, please desist

Denial of Service
The denial of service category outlines any incident where an attempt is made to deny service (this category also covers distributed denial of service). It is likely that these will be external attacks rather than internally generated, as internal attacks will have a different root cause. The attack may not result in an actual denial of service, but this category

should record the attempt, where a member of the security team has undertaken some work into root cause analysis.

Minor designations
We are being attacked by the following IP in a DoS
We are seeing the following IPs being used in a DDoS, can you shut them down

Unauthorised access

This category covers any incident in which an attacker has been able to acquire an unauthorised level of access to a machine, service or information asset, and the person in question knows that the access is unauthorised at the time.

Common incidents will include use of compromised accounts (e.g. brute forced SSH accounts), exploitation of software vulnerabilities to execute code or access accounts, buffer overflows, code injection attacks (e.g. SQL injection) and unauthorised elevation of privileges. Usually there will be some element of human interaction involved in the initial exploit. This category is distinct from "Malicious Code" where the root cause of the compromise is fully automated, self-replicating code such as a worm, and exploiting vulnerabilities in common software.

Minor designations
I've found an unknown user account on a server
There are strange SQL statements in this log file

APT

This category is used for attacks which are specifically targeted against an organisation or individual and use multiple methods of attack to break into a network, evade detection and harvest data over a period of time. APTs will typically cover more than one category of attack such as Malicious Code, Unauthorised Access and Internal Investigation. The common theme would be that a single actor can be attributed to the same attack, it is targeted specifically and is over a substantial period of time. It is likely that it may take time to identify incidents in this category, with several incidents being categorised differently and closed down before being recognised as an APT. Such attacks generally have an end result of extracting data, rather than targeting the computing assets of the entity.

Minor designation
We have had a number of user accounts compromised
This phishing email was sent just to one person, who then got infected with a Trojan

Social

This category covers any incident in which an attacker has been able to acquire a user's account details, potentially or actually giving them access to the persons service or information assets.
Common incidents will include use of emails or SMS messages, when a user has actually entered in their account details. This category is not used

for when a phishing attack has been started, but no details have been lost.

Minor designations
Phishing
Vishing
Smishing

Vulnerability Notification
The Vulnerability Notification category is not strictly an incident. It is more a measure of service. This category is a simple count of the number of notifications that the security team has sent out to their constituency, during the reporting period.

Minor designations
OS notification
Networking notification
Application notification

Block applied
The Block Applied category is used to cover occasions where the security team applies a block to an external resource. This could, for example, be an RPZ entry or a firewall block. This category is not used for blocks to internal resources.

This is outside of any automated process (for example a block list) which is downloaded and applied. The Block Applied category is used either in response to an attack or as a preventative measure (from intelligence).

Minor designations
Firewall block
RPZ block
Proxy block

Threat/Extortion/Blackmail
This category covers communication with a member of the entity which tries to gain money or services through leverage. This can be threats, force or through revealing compromising information.

Minor designations
DDoS threat
Data exfiltration and ransom

Currently uncategorised
This category covers those incidents which have not yet been given one of the standard categories. This may occur when either the incident occurs at the time when the metrics are being collated (e.g. last day of the month) or as a place holder until root cause can be determined.

Minor designations
N/A