```
MILE                                                        T. Takahashi
Internet-Draft                                                      NICT
Intended status: Standards Track                            June 8, 2016
Expires: December 10, 2016
```

JSON representation of IODEF
draft-takahashi-mile-jsoniodef-00

Abstract

RFC5070-bis provides XML-based data representation on incident information, but the use of the IODEF data model is not limited to XML. JSON representation is sometimes preferred since it is easy to handle from certain programming environments. This draft represents the IODEF data model in JSON. Note that this 00 version draft is prepared for the purpose of encouraging discussion on the need for JSON representation.

Status of This Memo

This Internet-Draft will expire on December 10, 2016.

Copyright Notice

Table of Contents

```
   1.  Introduction . . . . . . . . . . . . . . . . . . . . . . . .   3
     1.1.  Requirements Language . . . . . . . . . . . . . . . . . .   4
   2.  The IODEF Information Model in JSON . . . . . . . . . . . . .   4
     2.1.  IODEF-Document Class  . . . . . . . . . . . . . . . . . .   4
     2.2.  Incident Class  . . . . . . . . . . . . . . . . . . . . .   4
     2.3.  Common Attributes . . . . . . . . . . . . . . . . . . . .   5
       2.3.1.  restriction Attribute . . . . . . . . . . . . . . . .   5
       2.3.2.  observable-id Attribute . . . . . . . . . . . . . . .   5
     2.4.  IncidentID Class  . . . . . . . . . . . . . . . . . . . .   5
     2.5.  AlternativeID Class . . . . . . . . . . . . . . . . . . .   6
     2.6.  RelatedActivity Class . . . . . . . . . . . . . . . . . .   6
     2.7.  ThreatActor Class . . . . . . . . . . . . . . . . . . . .   6
     2.8.  Campaign Class  . . . . . . . . . . . . . . . . . . . . .   7
     2.9.  Contact Class . . . . . . . . . . . . . . . . . . . . . .   7
       2.9.1.  RegistryHandle Class  . . . . . . . . . . . . . . . .   7
       2.9.2.  PostalAddress Class . . . . . . . . . . . . . . . . .   8
       2.9.3.  Email Class . . . . . . . . . . . . . . . . . . . . .   8
       2.9.4.  Telephone Class . . . . . . . . . . . . . . . . . . .   8
     2.10. Discovery Class . . . . . . . . . . . . . . . . . . . . .   8
       2.10.1.  DetectionPattern Class . . . . . . . . . . . . . . .   9
     2.11. Method Class  . . . . . . . . . . . . . . . . . . . . . .   9
       2.11.1.  Reference Class  . . . . . . . . . . . . . . . . . .   9
     2.12. Assessment Class  . . . . . . . . . . . . . . . . . . . .   9
       2.12.1.  SystemImpact Class . . . . . . . . . . . . . . . . .  10
       2.12.2.  BusinessImpact Class . . . . . . . . . . . . . . . .  10
       2.12.3.  TimeImpact Class . . . . . . . . . . . . . . . . . .  10
       2.12.4.  MonetaryImpact Class . . . . . . . . . . . . . . . .  10
       2.12.5.  Confidence Class . . . . . . . . . . . . . . . . . .  10
     2.13. History Class . . . . . . . . . . . . . . . . . . . . . .  11
       2.13.1.  HistoryItem Class  . . . . . . . . . . . . . . . . .  11
     2.14. EventData Class . . . . . . . . . . . . . . . . . . . . .  11
     2.15. Expectation Class . . . . . . . . . . . . . . . . . . . .  12
     2.16. System Class  . . . . . . . . . . . . . . . . . . . . . .  12
     2.17. Node Class  . . . . . . . . . . . . . . . . . . . . . . .  13
       2.17.1.  Address Class  . . . . . . . . . . . . . . . . . . .  13
       2.17.2.  NodeRole Class . . . . . . . . . . . . . . . . . . .  13
       2.17.3.  Counter Class  . . . . . . . . . . . . . . . . . . .  13
     2.18. DomainData Class  . . . . . . . . . . . . . . . . . . . .  14
       2.18.1.  Nameserver Class . . . . . . . . . . . . . . . . . .  14
       2.18.2.  DomainContacts Class . . . . . . . . . . . . . . . .  14
     2.19. Service Class . . . . . . . . . . . . . . . . . . . . . .  14
       2.19.1.  ServiceName Class  . . . . . . . . . . . . . . . . .  15
       2.19.2.  ApplicationHeader Class  . . . . . . . . . . . . . .  15
```

2.20. EmailData Class 15
2.21. Record Class 15
2.21.1. RecordPattern Class 16
2.22. WindowsRegistryKeysModified Class 16
2.22.1. Key Class 16
2.23. CertificateData Class 17
2.23.1. Certificate Class 17
2.24. FileData Class 17
2.24.1. File Class 18
2.25. HashData Class 18
2.25.1. Hash Class 18
2.25.2. FuzzyHash Class 18
2.26. SignatureData Class 19
2.27. Indicator Class 19
2.27.1. IndicatorID Class 19
2.27.2. AlternativeIndicatorID Class 20
2.27.3. Observable Class 20
2.27.4. IndicatorExpression Class 20
2.27.5. ObservableReference Class 20
2.27.6. IndicatorReference Class 21
2.27.7. AttackPhase Class 21
3. Notable differences from RFC5070-bis (to be deleted) 21
4. Examples 21
4.1. Minimal Example 21
4.2. Indicators from a Campaign 22
5. The IODEF Data Model (JSON Schema) 24
6. Acknowledgements 57
7. IANA Considerations 57
8. Security Considerations 58
9. References 58
9.1. Normative References 58
9.2. Informative References 58
Author’s Address 58

1. Introduction

RFC5070-bis defines an data model for sharing incident information. It facilitates automated exchange of information among parties over networks. The data model can be implemented in a form of XML, but it is not always suitable for implementation. JSON-based representation is often useful.

Therefore, in this document, we provide a means to represent IODEF data model in JSON.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. The IODEF Information Model in JSON

The data model of IODEF is defined in RFC5070-bis, and this section represent the elements of the data model in JSON.

2.1. IODEF-Document Class

The IODEF-Document class is the top level class in the IODEF data model. All IODEF documents are an instance of this class. This class provides seven parameters: version, lang, format-id, private-enum-name, private-enum-id, Incident, and AdditionalData.

The example below represents how to describe this class in JSON.

```
"IODEF-Document": {
  "version": "1.0",
  "lang": "en",
  "format-id": "RFC5070",
  "Incident": [
     <<< omitted >>>
  ]
}
```

Figure 1: IODEF-Document Class in JSON

2.2. Incident Class

The Incident class describes commonly exchanged information when reporting or sharing derived analysis from security incidents.

The example below represents how to describe this class in JSON.

```
"Incident": {
  "purpose": "reporting",
  "lang": "en",
  "restriction": "green",
  "IncidentID": {<<< omitted >>>},
  "RelatedActivity": [<<< omitted >>>],
  "GenerationTime": "2015-10-02T11:18:00-05:00",
  "Description": ["Incident class description field"],
  "Assessment": [<<< omitted >>>],
  "Methods": [<<< omitted >>>],
  "Contact": [<<< omitted >>>]
  "EventData": [<<< omitted >>>],
  "IndicatorList": [<<< omitted >>>] # check whether it can exist once or mo
re
  "History": {<<< omitted >>>},
  "AdditionalData": [<<< omitted >>>],
}
```

Figure 2: Incident Class in JSON

2.3. Common Attributes

There are a number of recurring attributes used in the information model. They are documented in this section.

2.3.1. restriction Attribute

RFC5070-bis defines the restriction Attribute as one of common attributes. It is defined as below:

```
"restriction":{"enum": ["public", "partner", "need-to-know",
"private", "default", "white", "green", "amber", "red", "ext-value"]}
```

2.3.2. observable-id Attribute

RFC5070-bis defines the observable-id attribute as one of common attributes. The value of this attribute is a unique identifier in the scope of the document.It is defined as below:

```
"observable-id": {"type": "string"},
```

Figure 3: observable-id in JSON

2.4. IncidentID Class

The example below represents how to describe this class in JSON.

```
"IncidentID": {
  "id": "nict20150518-0001",
  "name": "NICT_cert",
  "instance": "cyberlab"
}
```

Figure 4: IncidentID Class in JSON

2.5. AlternativeID Class

The example below represents how to describe this class in JSON.

```
"AltervativeID": {
  "restriction": "private",
  "IncidentID": [<<<omitted>>>]
}
```

Figure 5: AlternativeID Class in JSON

2.6. RelatedActivity Class

The example below represents how to describe this class in JSON.

```
"RelatedActivity": {
  "restriction": "private",
  "ThreatActor": [
    {
      "ThreatActorID": "TA-12-AGGRESSIVE-BUTTERFLY",
      "Description": "Aggressive Butterfly"
    }
  ],
  "Campaign": [
    {
      "CampaignID": "C-2015-59405",
      "Description": "Orange Giraffe"
    }
  ]
}
```

Figure 6: RelatedActivity Class in JSON

2.7. ThreatActor Class

The example below represents how to describe this class in JSON.

```
"ThreatActor": {
  "ThreatActorID": "TA-12-AGGRESSIVE-BUTTERFLY",
  "Description": "Aggressive Butterfly"
}
```

Figure 7: ThreatActor Class in JSON

2.8. Campaign Class

The example below represents how to describe this class in JSON.

```
"Campaign": {
  "CampaignID": "C-2015-59405",
  "Description": "Orange Giraffe"
}
```

Figure 8: Campaign Class in JSON

2.9. Contact Class

The example below represents how to describe this class in JSON.

```
"Contact": {
  "type": "organization",
  "role": "creator",
  "ContactName": "CSIRT for example.com",
  "email": {
    "emailTo": "contact@csirt.example.com"
  }
}
```

Figure 9: Contact Class in JSON

2.9.1. RegistryHandle Class

The example below represents how to describe this class in JSON.

```
"RegistryHandle": {
  "RegistryHandleName": "MyAPNIC",
  "registry": "apnic",
}
```

Figure 10: RegistryHandle Class in JSON

2.9.2. PostalAddress Class

The example below represents how to describe this class in JSON.

```
       "PostalAddress": {
         "type": "mailing",
         "PAddress": "184-8795",
         "Description": "4-2-1 Nukui-Kitamachi Koganei Tokyo, Japan"
       },
```

Figure 11: PostalAddress Class in JSON

2.9.3. Email Class

The example below represents how to describe this class in JSON.

```
                 "Email": {
                   "emailTo": "contact@csirt.example.com"
                 },
```

Figure 12: Email Class in JSON

2.9.4. Telephone Class

The example below represents how to describe this class in JSON.

```
                    "Telephone": {
                      "TelephoneNumber": "+81423275862"
                    },
```

Figure 13: Telephone Class in JSON

2.10. Discovery Class

The example below represents how to describe this class in JSON.

```
                   "Discovery": {
                     "DetectionPattern": {
                       "Application": {
                         "Description": "Microsoft Win"
                       }
                     }
                   }
```

Figure 14: Discovery Class in JSON

2.10.1. DetectionPattern Class

The example below represents how to describe this class in JSON.

```
                    "DetectionPattern": {
                      "Application": {
                        "Description": "Microsoft Win"
                      }
                    }
```

Figure 15: DetectionPattern Class in JSON

2.11. Method Class

The example below represents how to describe this class in JSON.

```
                           "Method": {
                             "Vulnerability": {}
                           }
```

Figure 16: Method Class in JSON

2.11.1. Reference Class

The example below represents how to describe this class in JSON.

```
                      "Reference":{
                        "URL":"http://www.nict.go.jp"
                      }
```

Figure 17: Reference Class in JSON

2.12. Assessment Class

The example below represents how to describe this class in JSON.

```
                     "Assessment": {
                       "BusinessImpact": {
                         "type": "breach-proprietary"
                       }
                     }
```

Figure 18: Assessment Class in JSON

2.12.1. SystemImpact Class

The example below represents how to describe this class in JSON.

```
"SystemImpact":{
  "severity":"low",
  "type":"unknown"
},
```

Figure 19: SystemImpact Class in JSON

2.12.2. BusinessImpact Class

The example below represents how to describe this class in JSON.

```
"BusinessImpact": {
  "type": "breach-proprietary"
}
```

Figure 20: BusinessImpact Class in JSON

2.12.3. TimeImpact Class

The example below represents how to describe this class in JSON.

```
"TimeImpact":{
  "value":"5 hours",
  "metric":"elapsed"
}
```

Figure 21: TimeImpact Class in JSON

2.12.4. MonetaryImpact Class

The example below represents how to describe this class in JSON.

```
"MonetaryImpact":{}
```

Figure 22: MonetaryImpact Class in JSON

2.12.5. Confidence Class

The example below represents how to describe this class in JSON.

```
                            "Confidence": {
                              "rating": "medium"
                            }
```

Figure 23: Confidence Class in JSON

2.13. History Class

The example below represents how to describe this class in JSON.

```
               "History": {
                 "HistoryItem": {
                   "DateTime": "2015-10-15T11:18:00-05:00",
                   "action": "investigate"
                 }
               },
```

Figure 24: History Class in JSON

2.13.1. HistoryItem Class

The example below represents how to describe this class in JSON.

```
                "HistoryItem": {
                  "DateTime": "2015-10-15T11:18:00-05:00",
                  "action": "investigate"
                }
```

Figure 25: HistoryItem Class in JSON

2.14. EventData Class

The example below represents how to describe this class in JSON.

```
                 "EventData": {
                   "ReportTime": "2016-06-01 18:05:33",
                   "System": {
                     "category": "source",
                     "Node": {
                       "Address": {
                         "category": "ipv4-addr",
                         "AddressValue": "192.228.139.118"
                       },
                       "Location": "OrgID=7"
                     },
                     "Service": {
                       "ip-protocol": 6,
                       "Port": 49183
                     }
                 },
```

Figure 26: EventData Class in JSON

2.15. Expectation Class

The example below represents how to describe this class in JSON.

```
                         "Expectation": {
                           "action": "investigate"
                         },
```

Figure 27: Expectation Class in JSON

2.16. System Class

The example below represents how to describe this class in JSON.

```
                       "System": {
                         "category": "source",
                         "Node": {
                           "Address": {
                             "category": "ipv4-addr",
                             "AddressValue": "192.228.139.118"
                           },
                           "Location": "OrgID=7"
                         },
                         "Service": {
                           "ip-protocol": 6,
                           "Port": 49183
                         }
```

Figure 28: System Class in JSON

2.17. Node Class

The example below represents how to describe this class in JSON.

```
                         "Node": {
                           "Address": {
                             "category": "ipv4-addr",
                             "AddressValue": "192.228.139.118"
                           },
```

Figure 29: Node Class in JSON

2.17.1. Address Class

The example below represents how to describe this class in JSON.

```
                           "Address": {
                             "category": "ipv4-addr",
                             "AddressValue": "192.228.139.118"
                           },
```

Figure 30: Address Class in JSON

2.17.2. NodeRole Class

The example below represents how to describe this class in JSON.

```
                                "NodeRole": {
                                  "category": "client"
                                },
```

Figure 31: NodeRole Class in JSON

2.17.3. Counter Class

The example below represents how to describe this class in JSON.

```
                                 "Counter": {
                                   "value": "3",
                                   "type": "count",
                                   "unit": "packet"
                                 }
```

Figure 32: Counter Class in JSON

2.18. DomainData Class

The example below represents how to describe this class in JSON.

```
"DomainData": {
  "system-status": "innocent-hacked",
  "domain-status": "assignedAndInactive",
  "Name": "temp1.nict.go.jp"
},
```

Figure 33: DomainData Class in JSON

2.18.1. Nameserver Class

The example below represents how to describe this class in JSON.

```
"NameServers": {
  "Server": "vgw.nict.go.jp",
  "Address": {
    "AddressValue": "133.243.18.5",
    "category": "ipv4-addr"
  }
}
```

Figure 34: Nameserver Class in JSON

2.18.2. DomainContacts Class

The example below represents how to describe this class in JSON.

```
"DomainContacts": {
  "Contact": {
    "role": "user",
    "type": "organization"
  }
}
```

Figure 35: DomainContacts Class in JSON

2.19. Service Class

The example below represents how to describe this class in JSON.

```
            "Service": {
              "ServiceName": {
                "Description": "It seems to be a scan from an infected machi
ne."
              },
              "ip-protocol": 6,
              "Port": 49183
            }
```

Figure 36: Service Class in JSON

2.19.1. ServiceName Class

The example below represents how to describe this class in JSON.

```
              "ServiceName": {
                "Description": "It seems to be a scan from an infected machi
ne."
              },
```

Figure 37: ServiceName Class in JSON

2.19.2. ApplicationHeader Class

The example below represents how to describe this class in JSON.

```
                                  "ApplicationHeader": {}
```

Figure 38: ApplicationHeader Class in JSON

2.20. EmailData Class

The example below represents how to describe this class in JSON.

```
                                      "EmailData":{}
```

Figure 39: EmailData Class in JSON

2.21. Record Class

The example below represents how to describe this class in JSON.

```
                          "Record": {
                            "RecordPattern": {
                              "type": "regex",
                              "value": "[0-9][A-Z]"
                            },
                            "RecordItem": {}
                          },
```

Figure 40: Record Class in JSON

2.21.1. RecordPattern Class

The example below represents how to describe this class in JSON.

```
                            "RecordPattern": {
                              "type": "regex",
                              "value": "[0-9][A-Z]"
                            },
```

Figure 41: RecordPattern Class in JSON

2.22. WindowsRegistryKeysModified Class

The example below represents how to describe this class in JSON.

```
                    "WindowsRegistryKeysModified": {
                      "Key": {
                        "KeyValue": "xxxxxxxxxxxxxxxxxxxxxxxx",
                        "KeyName":"HKEY_LOCAL_MACHINExxxxxxx",
                      }
                    }
```

Figure 42: WindowsRegistryKeysModified Class in JSON

2.22.1. Key Class

The example below represents how to describe this class in JSON.

```
                      "Key": {
                        "KeyValue": "xxxxxxxxxxxxxxxxxxxxxxxx",
                        "KeyName":"HKEY_LOCAL_MACHINExxxxxxx",
                      }
```

Figure 43: Key Class in JSON

2.23. CertificateData Class

The example below represents how to describe this class in JSON.

```
            "CertificateData": {
              "Certificate": {
                "X509Data": {
                  "X509IssuerSerial": {
                    "X509IssuerName": "CN=TAMURA Kent, OU=TRL, O=IBM, L=Yama
to-shi, ST=Kanagawa, C=JP",
                    "X509SerialNumber": "12345678"
                  },
                  "X509SKI": "31d97bd7"
                }
              }
            }
```

Figure 44: CertificateData Class in JSON

2.23.1. Certificate Class

The example below represents how to describe this class in JSON.

```
              "Certificate": {
                "X509Data": {
                  "X509IssuerSerial": {
                    "X509IssuerName": "CN=TAMURA Kent, OU=TRL, O=IBM, L=Yama
to-shi, ST=Kanagawa, C=JP",
                    "X509SerialNumber": "12345678"
                  },
                  "X509SKI": "31d97bd7"
                }
              }
```

Figure 45: Certificate Class in JSON

2.24. FileData Class

The example below represents how to describe this class in JSON.

```
                              "FileData": {
                                "File": {
                                  "FileName": "dummy.exe"
                                }
                              },
```

Figure 46: FileData Class in JSON

2.24.1. File Class

The example below represents how to describe this class in JSON.

```
                                "File": {
                                  "FileName": "dummy.exe"
                                }
```

Figure 47: File Class in JSON

2.25. HashData Class

The example below represents how to describe this class in JSON.

```
                "HashData": {
                  "scope": "file-contents",
                  "Hash": {
                    "DigestMethod": "http://www.w3.org/2000/09/xmldsig#sha1"
,
                    "DigestValue": "xxxxxxxxxxx"
                  }
                }
```

Figure 48: HashData Class in JSON

2.25.1. Hash Class

The example below represents how to describe this class in JSON.

```
                  "Hash": {
                    "DigestMethod": "http://www.w3.org/2000/09/xmldsig#sha1"
,
                    "DigestValue": "xxxxxxxxxxx"
                  }
```

Figure 49: Hash Class in JSON

2.25.2. FuzzyHash Class

The example below represents how to describe this class in JSON.

```
                                   "FuzzyHash": {
                                     "FuzzyHashValue": {}
                                   }
```

Figure 50: FuzzyHash Class in JSON

2.26. SignatureData Class

The example below represents how to describe this class in JSON.

```
                                 "SignatureData": {
                                   "Signature": "xxxxxxxx"
                                 }
```

Figure 51: SignatureData Class in JSON

2.27. Indicator Class

The example below represents how to describe this class in JSON.

```
                     "Indicator": {
                       "IndicatorID": {
                         "id": "G90823490",
                         "name": "csirt.example.com",
                         "version": "1"
                       },
                       "Description": "C2 domains",
                       "StartTime": "2014-12-02T11:18:00-05:00",
                       "Observable": {
                         "BulkObservable": {
                           "type": "fqdn"
                         },
                         "BulkObservableList": [
                           "kj290023j09r34.example.com",
                           "09ijk23jfj0k8.example.net",
                           "klknjwfjiowjefr923.example.org",
                           "oimireik79msd.example.org"
                         ]
                       }
                     }
```

Figure 52: Indicator Class in JSON

2.27.1. IndicatorID Class

The example below represents how to describe this class in JSON.

```
                            "IndicatorID": {
                              "id": "G90823490",
                              "name": "csirt.example.com",
                              "version": "1"
                            },
```

Figure 53: IndicatorID Class in JSON

2.27.2. AlternativeIndicatorID Class

The example below represents how to describe this class in JSON.

```
"AlternativeIndicatorID": {
  "IndicatorReference": {
    "uid-ref": "xxxxx"
  }
},
```

Figure 54: AlternativeIndicatorID Class in JSON

2.27.3. Observable Class

The example below represents how to describe this class in JSON.

```
"Observable": {
  "BulkObservable": {
    "type": "fqdn"
  },
  "BulkObservableList": [
    "kj290023j09r34.example.com",
    "09ijk23jfj0k8.example.net",
    "klknjwfjiowjefr923.example.org",
    "oimireik79msd.example.org"
  ]
}
```

Figure 55: Observable Class in JSON

2.27.4. IndicatorExpression Class

The example below represents how to describe this class in JSON.

```
"IndicatorExpression": {}
```

Figure 56: IndicatorExpression Class in JSON

2.27.5. ObservableReference Class

The example below represents how to describe this class in JSON.

```
"ObservableReference": {
  "uid-ref": "xxxxx"
},
```

Figure 57: ObservableReference Class in JSON

2.27.6. IndicatorReference Class

The example below represents how to describe this class in JSON.

```
                                 "IndicatorReference": {
                                   "uid-ref": "xxxxx"
                                 }
```

Figure 58: IndicatorReference Class in JSON

2.27.7. AttackPhase Class

The example below represents how to describe this class in JSON.

```
            "AttackPhase": {
              "Description": "Currently, the infected host is scanning arbit
rary hosts to find next targets."
            }
```

Figure 59: AttackPhase Class in JSON

3. Notable differences from RFC5070-bis (to be deleted)

- Flow class is deleted, and EventData class now has the instance of System class.

- Record class is deleted, and the link to the Record class are directly connected to RecordData class, which is then renamed to Record class.

4. Examples

This section provides example of IODEF documents. These examples do not represent the full capabilities of the data model or the the only way to encode particular information.

4.1. Minimal Example

A document containing only the mandatory elements and attributes.

```
           {
             "version": "2.0",
             "lang": "en",
             "Incident": [
               {
                 "purpose": "reporting",
                 "restriction": "private",
                 "IncidentID": {
                   "id": 492382,
                   "name": "csirt.example.com"
                 },
                 "GenerationTime": "2015-07-18T09:00:00-05:00",
                 "Contact": [
                   {
                     "type": "organization",
                     "role": "creator",
                     "email": {
                       "emailTo": "contact@csirt.example.com"
                     }
                   }
                 ]
               }
             ]
           }
```

Figure 60: JSON representation example 1

4.2. Indicators from a Campaign

An example of C2 domains from a given campaign.

```
{
  "version": "2.0",
  "lang": "en",
  "Incidents": [
    {
      "purpose": "watch",
      "restriction": "green",
      "IncidentID": {
        "id": "897923",
        "name": "csirt.example.com"
      },
      "RelatedActivity": [
        {
          "ThreatActor": [
            {
              "ThreatActorID": "TA-12-AGGRESSIVE-BUTTERFLY",
              "Description": "Aggressive Butterfly"
            }
          ],
          "Campaign": [
            {
              "CampaignID": "C-2015-59405",
              "Description": "Orange Giraffe"
            }
          ]
        }
      ],
      "GenerationTime": "2015-10-02T11:18:00-05:00",
      "Description": [
        "Summarizes the Indicators of Compromise for the Orange Giraffe camp
aign of the Aggressive Butterfly crime gang."
      ],
      "Assessment": [
        {
          "BusinessImpact": {
            "type": "breach-proprietary"
          }
        }
      ],
      "Contacts": [
        {
          "type": "organization",
          "role": "creator",
          "ContactName": "CSIRT for example.com",
          "Email": {
            "emailTo": "contact@csirt.example.com"
          }
        }
      ],
      "IndicatorList": [
        {
          "IndicatorID": {
            "id": "G90823490",
            "name": "csirt.example.com",
            "version": "1"
          },
          "Description": "C2 domains",
          "StartTime": "2014-12-02T11:18:00-05:00",
          "Observable": {
            "BulkObservable": {
              "type": "fqdn"
            },
            "BulkObservableList": [
              "kj290023j09r34.example.com",
              "09ijk23jfj0k8.example.net",
              "klknjwfjiowjefr923.example.org",
              "oimireik79msd.example.org"
            ]
          }
        }
      ]
    }
  ]
}
```

Figure 61: JSON representation example 2

5. The IODEF Data Model (JSON Schema)

```
         {
         {
           "$schema": "http://json-schema.org/draft-04/schema#",
           "definitions": {
             "lang": {
               "enum": [
                 "en",
                 "jp"
               ]
             },
             "restriction": {
               "enum": [
                 "public",
                 "partner",
                 "need-to-know",
                 "private",
                 "default",
                 "white",
                 "green",
                 "amber",
                 "red",
                 "ext-value"
               ]
             },
             "URLtype": {
               "type": "string"
             },
             "IDtype": {
               "type": "string"
             },
             "ExtensionType": {
               "type": "object",
               "properties": {
                 "name": {
                   "type": "string"
                 },
                 "dtype": {
                   "enum": [
                     "boolean",
                     "byte",
                     "bytes",
                     "character",
                     "date-time",
                     "ntpstamp",
                     "integer",
                     "portlist",
                     "real",
                     "string",
                     "file",
                     "path",
                     "frame",
                     "packet",
                     "ipv4-packet",
                     "ipv6-packet",
                     "url",
                     "csv",
                     "winreg",
                     "xml",
                     "ext-value"
                   ]
                 },
                 "ext-dtype": {
                   "type": "string"
                 },
                 "meaning": {
                   "type": "string"
                 },
                 "formatid": {
                   "type": "string"
                 },
                 "restriction": {
                   "$ref": "#/definitions/restriction"
                 },
                 "ext-restriction": {
                   "type": "string"
                 },
                 "observable-id": {
                   "$ref": "#/definitions/IDtype"
                 }
               }
             },
             "SoftwareType": {
               "type": "object",
               "properties": {
                 "SoftwareReference": {
                   "$ref": "#/definitions/SoftwareReference"
                 },
                 "URL": {
                   "$ref": "#/definitions/URLtype"
                 },
                 "Description": {
                   "type": "string"
                 }
               },
               "required": [],
               "additionalProperties": false
             },
             "SoftwareReference": {
               "type": "object",
               "properties": {
                 "value": {
                   "type": "string"
                 },
                 "spec-name": {
                   "type": "string"
                 },
                 "ext-spec-name": {
                   "type": "string"
                 },
                 "dtype": {
                   "type": "string"
                 },
                 "ext-dtype": {
                   "type": "string"
                 }
               },
               "required": [
                 "spec-name"
               ],
               "additionalProperties": false
             },
             "Incident": {
               "title": "Incident",
               "description": "JSON schema for Incident class",
               "type": "object",
               "properties": {
                 "purpose": {
                   "enum": [
                     "traceback",
                     "mitigation",
                     "reporting",
                     "watch",
                     "other",
                     "ext-value"
                   ]
                 },
                 "ext-purpose": {
                   "type": "string"
                 },
                 "status": {
                   "enum": [
                     "blabla"
                   ]
                 },
                 "ext-status": {
                   "type": "string"
                 },
                 "lang": {
                   "$ref": "#/definitions/lang"
                 },
                 "restriction": {
                   "$ref": "#/definitions/restriction"
                 },
                 "ext-restriction": {
                   "type": "string"
                 },
                 "observable-id": {
                   "$ref": "#/definitions/IDtype"
                 },
                 "IncidentID": {
                   "$ref": "#/definitions/IncidentID"
                 },
                 "AlternativeID": {
                   "type": "object"
                 },
                 "RelatedActivity": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/RelatedActivity"
                   }
                 },
                 "DetectTime": {
                   "type": "string"
                 },
                 "StartTime": {
                   "type": "string"
                 },
                 "EndTime": {
                   "type": "string"
                 },
                 "RecoveryTime": {
                   "type": "string"
                 },
                 "ReportTime": {
                   "type": "string"
                 },
                 "GenerationTime": {
                   "type": "string"
                 },
                 "Description": {
                   "type": "array",
                   "items": {
                     "type": "string"
                   }
                 },
                 "Discovery": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/Discovery"
                   }
                 },
                 "Assessment": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/Assessment"
                   }
                 },
                 "Methods": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/Method"
                   }
                 },
                 "Contacts": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/Contact"
                   }
                 },
                 "EventData": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/EventData"
                   }
                 },
                 "IndicatorList": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/Indicator"
                   },
                 },
                 "History": {
                   "$ref": "#/definitions/History"
                 },
                 "AdditionalData": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/ExtensionType"
                   }
                 }
               },
               "required": [
                 "IncidentID",
                 "GenerationTime",
                 "Contacts",
                 "purpose"
               ],
               "additionalProperties": false
             },
             "IncidentID": {
               "title": "IncidentID",
               "description": "JSON schema for IncidentID class",
               "type": "object",
               "properties": {
                 "id": {
                   "type": "string"
                 },
                 "name": {
                   "type": "string"
                 },
                 "instance": {
                   "type": "string"
                 },
                 "restriction": {
                   "$ref": "#/definitions/restriction"
                 },
                 "ext-restriction": {
                   "type": "string"
                 }
               },
               "required": [
                 "name"
               ],
               "additionalProperties": false
             },
             "RelatedActivity": {
               "properties": {
                 "restriction": {
                   "$ref": "#/definitions/restriction"
                 },
                 "ext-restriction": {
                   "type": "string"
                 },
                 "IncidentID": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/IncidentID"
                   }
                 },
                 "URL": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/URLtype"
                   }
                 },
                 "ThreatActor": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/ThreatActor"
                   }
                 },
                 "Campaign": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/Campaign"
                   }
                 },
                 "IndicatorID": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/IndicatorID"
                   }
                 },
                 "Confidence": {
                   "$ref": "#/definitions/Confidence"
                 },
                 "Description": {
                   "type": "array",
                   "items": {
                     "type": "string"
                   }
                 },
                 "AdditionalData": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/ExtensionType"
                   }
                 }
               },
               "additionalProperties": false
             },
             "ThreatActor": {
               "properties": {
                 "restriction": {
                   "$ref": "#/definitions/restriction"
                 },
                 "ext-restriction": {
                   "type": "string"
                 },
                 "ThreatActorID": {
                   "type": "string"
                 },
                 "Description": {
                   "type": "string"
                 },
                 "URL": {
                   "$ref": "#/definitions/URLtype"
                 },
                 "AdditionalData": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/ExtensionType"
                   }
                 }
               },
               "additionalProperties": false
             },
             "Campaign": {
               "properties": {
                 "restriction": {
                   "$ref": "#/definitions/restriction"
                 },
                 "ext-restriction": {
                   "type": "string"
                 },
                 "CampaignID": {},
                 "URL": {
                   "$ref": "#/definitions/URLtype"
                 },
                 "Description": {
                   "type": "string"
                 },
                 "AdditionalData": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/ExtensionType"
                   }
                 }
               }
             },
             "Contact": {
               "type": "object",
               "properties": {
                 "role": {},
                 "ext-role": {},
                 "type": {},
                 "ext-type": {},
                 "restriction": {
                   "$ref": "#/definitions/restriction"
                 },
                 "ext-restriction": {
                   "type": "string"
                 },
                 "ContactName": {},
                 "ContactTitle": {},
                 "Description": {
                   "type": "string"
                 },
                 "RegistryHandle": {},
                 "PostalAddress": {},
                 "Email": {},
                 "Telephone": {
                   "$ref": "#/definitions/Telephone"
                 },
                 "Timezone": {},
                 "Contact": {
                   "$ref": "#/definitions/Contact"
                 },
                 "AdditionalData": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/ExtensionType"
                   }
                 }
               },
               "required": [
                 "role",
                 "type"
               ],
               "additionalProperties": false
             },
             "RegistryHandle": {
               "type": "object",
               "properties": {
                 "RegistryHandleName": {},
                 "registry": {},
                 "ext-registry": {}
               },
               "required": [
                 "registry"
               ],
               "additionalProperties": false
             },
             "PostalAddress": {
               "type": "object",
               "properties": {
                 "type": {
                   "type": "string"
                 },
                 "ext-type": {
                   "type": "string"
                 },
                 "PAddress": {
                   "type": "string"
                 },
                 "Description": {
                   "type": "string"
                 }
               },
               "required": [
                 "PAddress"
               ],
               "additionalProperties": false
             },
             "Email": {
               "type": "object",
               "properties": {
                 "type": {},
                 "ext-type": {},
                 "EmailTo": {},
                 "Description": {
                   "type": "string"
                 }
               },
               "required": [
                 "EmailTo"
               ],
               "additionalProperties": false
             },
             "Telephone": {
               "type": "object",
               "properties": {
                 "type": {},
                 "ext-type": {},
                 "TelephoneNumber": {},
                 "Description": {
                   "type": "string"
                 }
               },
               "required": [
                 "TelephoneNumber"
               ],
               "additionalProperties": false
             },
             "Discovery": {
               "type": "object",
               "properties": {
                 "source": {},
                 "ext-source": {},
                 "restriction": {
                   "$ref": "#/definitions/restriction"
                 },
                 "ext-restriction": {
                   "type": "string"
                 },
                 "Description": {
                   "type": "string"
                 },
                 "Contact": {
                   "$ref": "#/definitions/Contact"
                 },
                 "DetectionPattern": {
                   "$ref": "#/definitions/DetectionPattern"
                 }
               },
               "required": [],
               "additionalProperties": false
             },
             "DetectionPattern": {
               "type": "object",
               "properties": {
                 "restriction": {
                   "$ref": "#/definitions/restriction"
                 },
                 "ext-restriction": {
                   "type": "string"
                 },
                 "observable-id": {
                   "$ref": "#/definitions/IDtype"
                 },
                 "Application": {
                   "$ref": "#/definitions/SoftwareType"
                 },
                 "Description": {
                   "type": "string"
                 },
                 "DetectionConfiguration": {}
               },
               "required": [
                 "Application"
               ],
               "additionalProperties": false
             },
             "Method": {
               "type": "object",
               "properties": {
                 "restriction": {
                   "$ref": "#/definitions/restriction"
                 },
                 "ext-restriction": {
                   "type": "string"
                 },
                 "References": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/Reference"
                   }
                 },
                 "Description": {
                   "type": "string"
                 },
                 "AttackPattern": {},
                 "Vulnerability": {},
                 "Weakness": {},
                 "AdditionalData": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/ExtensionType"
                   }
                 }
               },
               "required": [],
               "additionalProperties": false
             },
             "Reference": {
               "type": "object",
               "properties": {
                 "observable-id": {
                   "$ref": "#/definitions/IDtype"
                 },
                 "ReferenceName": {},
                 "URL": {
                   "$ref": "#/definitions/URLtype"
                 },
                 "Description": {
                   "type": "string"
                 }
               },
               "required": [],
               "additionalProperties": false
             },
             "Assessment": {
               "type": "object",
               "properties": {
                 "occurrence": {},
                 "restriction": {
                   "$ref": "#/definitions/restriction"
                 },
                 "ext-restriction": {
                   "type": "string"
                 },
                 "observable-id": {
                   "$ref": "#/definitions/IDtype"
                 },
                 "IncidentCategory": {},
                 "SystemImpact": {
                   "$ref": "#/definitions/SystemImpact"
                 },
                 "BusinessImpact": {},
                 "TimeImpact": {
                   "$ref": "#/definitions/TimeImpact"
                 },
                 "MonetaryImpact": {
                   "$ref": "#/definitions/MonetaryImpact"
                 },
                 "IntendedImpact": {},
                 "Counter": {
                   "$ref": "#/definitions/Counter"
                 },
                 "MitigatingFactor": {},
                 "Cause": {},
                 "Confidence": {
                   "$ref": "#/definitions/Confidence"
                 },
                 "AdditionalData": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/ExtensionType"
                   }
                 }
               },
               "required": [],
               "additionalProperties": false
             },
             "SystemImpact": {
               "type": "object",
               "properties": {
                 "severity": {},
                 "completion": {},
                 "type": {},
                 "ext-type": {},
                 "Description": {
                   "type": "string"
                 }
               },
               "required": [
                 "type"
               ],
               "additionalProperties": false
             },
             "BusinessImpact": {
               "type": "object",
               "properties": {
                 "severity": {},
                 "ext-severity": {},
                 "type": {},
                 "ext-type": {},
                 "Description": {
                   "type": "string"
                 }
               },
               "required": [
                 "type"
               ],
               "additionalProperties": false
             },
             "TimeImpact": {
               "type": "object",
               "properties": {
                 "value": {},
                 "severity": {},
                 "metric": {},
                 "ext-metric": {},
                 "duration": {},
                 "ext-duration": {}
               },
               "required": [
                 "metric"
               ],
               "additionalProperties": false
             },
             "MonetaryImpact": {
               "type": "object",
               "properties": {
                 "MonetaryImpactValue": {},
                 "severity": {},
                 "currency": {}
               },
               "required": [],
               "additionalProperties": false
             },
             "Confidence": {
               "type": "object",
               "properties": {
                 "ConfidenceValue": {},
                 "rating": {},
                 "ext-rating": {}
               },
               "required": [
                 "rating"
               ],
               "additionalProperties": false
             },
             "History": {
               "type": "object",
               "properties": {
                 "restriction": {
                   "$ref": "#/definitions/restriction"
                 },
                 "ext-restriction": {
                   "type": "string"
                 },
                 "HistoryItem": {}
               },
               "required": [
                 "HistoryItem"
               ],
               "additionalProperties": false
             },
             "HistoryItem": {
               "type": "object",
               "properties": {
                 "action": {},
                 "ext-action": {},
                 "restriction": {
                   "$ref": "#/definitions/restriction"
                 },
                 "ext-restriction": {
                   "type": "string"
                 },
                 "observable-id": {
                   "$ref": "#/definitions/IDtype"
                 },
                 "DateTime": {},
                 "IncidentID": {},
                 "Contact": {
                   "$ref": "#/definitions/Contact"
                 },
                 "Description": {
                   "type": "string"
                 },
                 "DefinedCOA": {},
                 "AdditionalData": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/ExtensionType"
                   }
                 }
               },
               "required": [
                 "DateTime",
                 "action"
               ],
               "additionalProperties": false
             },
             "EventData": {
               "type": "object",
               "properties": {
                 "restriction": {
                   "$ref": "#/definitions/restriction"
                 },
                 "ext-restriction": {
                   "type": "string"
                 },
                 "observable-id": {
                   "$ref": "#/definitions/IDtype"
                 },
                 "Description": {
                   "type": "string"
                 },
                 "DetectTime": {},
                 "StartTime": {},
                 "EndTime": {},
                 "RecoveryTime": {},
                 "ReportTime": {
                   "type": "string"
                 },
                 "Contact": {
                   "$ref": "#/definitions/Contact"
                 },
                 "Discovery": {
                   "$ref": "#/definitions/Discovery"
                 },
                 "Assessment": {},
                 "Method": {
                   "$ref": "#/definitions/Method"
                 },
                 "System": {
                   "$ref": "#/definitions/System"
                 },
                 "Expectation": {
                   "$ref": "#/definitions/Expectation"
                 },
                 "Record": {
                   "$ref": "#/definitions/Record"
                 },
                 "EventData": {
                   "$ref": "#/definitions/EventData"
                 },
                 "AdditionalData": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/ExtensionType"
                   }
                 }
               },
               "required": [
                 "ReportTime"
               ],
               "additionalProperties": false
             },
             "Expectation": {
               "type": "object",
               "properties": {
                 "action": {},
                 "ext-action": {},
                 "severity": {},
                 "restriction": {
                   "$ref": "#/definitions/restriction"
                 },
                 "ext-restriction": {
                   "type": "string"
                 },
                 "observable-id": {
                   "$ref": "#/definitions/IDtype"
                 },
                 "Description": {
                   "type": "string"
                 },
                 "DefinedCOA": {},
                 "StartTime": {},
                 "EndTime": {},
                 "Contact": {
                   "$ref": "#/definitions/Contact"
                 }
               },
               "required": [],
               "additionalProperties": false
             },
             "System": {
               "type": "object",
               "properties": {
                 "category": {
                   "enum": [
                     "source",
                     "target",
                     "intermediate",
                     "sensor",
                     "infrastructure",
                     "ext-value"
                   ]
                 },
                 "ext-category": {},
                 "interface": {},
                 "spoofed": {},
                 "virtual": {},
                 "ownership": {},
                 "ext-ownership": {},
                 "restriction": {
                   "$ref": "#/definitions/restriction"
                 },
                 "ext-restriction": {
                   "type": "string"
                 },
                 "observable-id": {
                   "$ref": "#/definitions/IDtype"
                 },
                 "Node": {
                   "$ref": "#/definitions/Node"
                 },
                 "NodeRole": {
                   "$ref": "#/definitions/NodeRole"
                 },
                 "Service": {
                   "$ref": "#/definitions/Service"
                 },
                 "OperatingSystem": {},
                 "Counter": {
                   "$ref": "#/definitions/Counter"
                 },
                 "AssetID": {},
                 "Description": {
                   "type": "string"
                 },
                 "AdditionalData": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/ExtensionType"
                   }
                 }
               },
               "required": [
                 "Node"
               ],
               "additionalProperties": false
             },
             "Node": {
               "type": "object",
               "properties": {
                 "DomainData": {
                   "$ref": "#/definitions/DomainData"
                 },
                 "Address": {
                   "$ref": "#/definitions/Address"
                 },
                 "PostalAddress": {},
                 "Location": {
                   "type": "string"
                 },
                 "Counter": {
                   "$ref": "#/definitions/Counter"
                 }
               },
               "required": [],
               "additionalProperties": false
             },
             "Address": {
               "type": "object",
               "properties": {
                 "AddressValue": {},
                 "category": {},
                 "ext-category": {},
                 "vlan-name": {},
                 "vlan-num": {
                   "type": "integer"
                 },
                 "observable-id": {
                   "$ref": "#/definitions/IDtype"
                 }
               },
               "required": [
                 "category"
               ],
               "additionalProperties": false
             },
             "NodeRole": {
               "type": "object",
               "properties": {
                 "category": {},
                 "ext-category": {},
                 "Description": {
                   "type": "string"
                 }
               },
               "required": [
                 "category"
               ],
               "additionalProperties": false
             },
             "Counter": {
               "type": "object",
               "properties": {
                 "value": {
                   "type": "string"
                 },
                 "type": {},
                 "ext-type": {},
                 "unit": {},
                 "ext-unit": {},
                 "meaning": {},
                 "duration": {},
                 "ext-duration": {}
               },
               "required": [
                 "type",
                 "unit"
               ],
               "additionalProperties": false
             },
             "DomainData": {
               "type": "object",
               "properties": {
                 "system-status": {},
                 "ext-system-status": {},
                 "domain-status": {},
                 "ext-domain-status": {},
                 "observable-id": {
                   "$ref": "#/definitions/IDtype"
                 },
                 "Name": {},
                 "DateDomainWasChecked": {},
                 "RegistrationDate": {},
                 "ExpirationDate": {},
                 "RelatedDNS": {},
                 "NameServers": {
                   "$ref": "#/definitions/NameServers"
                 },
                 "DomainContacts": {
                   "$ref": "#/definitions/DomainContacts"
                 }
               },
               "required": [
                 "Name",
                 "system-status",
                 "domain-status"
               ],
               "additionalProperties": false
             },
             "NameServers": {
               "type": "object",
               "properties": {
                 "Server": {},
                 "Address": {
                   "$ref": "#/definitions/Address"
                 }
               },
               "required": [
                 "Server",
                 "Address"
               ],
               "additionalProperties": false
             },
             "DomainContacts": {
               "type": "object",
               "properties": {
                 "SameDomainContact": {},
                 "Contact": {
                   "$ref": "#/definitions/Contact"
                 }
               },
               "required": [
                 "Contact"
               ],
               "additionalProperties": false
             },
             "Service": {
               "type": "object",
               "properties": {
                 "ip-protocol": {},
                 "observable-id": {
                   "$ref": "#/definitions/IDtype"
                 },
                 "ServiceName": {},
                 "Port": {},
                 "Portlist": {},
                 "ProtoCode": {},
                 "ProtoType": {},
                 "ProtoField": {},
                 "ApplicationHeader": {},
                 "EmailData": {},
                 "Application": {}
               },
               "required": [],
               "additionalProperties": false
             },
             "ServiceName": {
               "type": "object",
               "properties": {
                 "IANAService": {},
                 "URL": {
                   "$ref": "#/definitions/URLtype"
                 },
                 "Description": {
                   "type": "string"
                 }
               },
               "required": [],
               "additionalProperties": false
             },
             "ApplicationHeader": {
               "type": "object",
               "properties": {
                 "ApplicationHeaderField": {}
               },
               "required": [
                 "ApplictionHeaderField"
               ],
               "additionalProperties": false
             },
             "EmailData": {
               "type": "object",
               "properties": {
                 "EmailTo": {},
                 "EmailFrom": {},
                 "EmailSubject": {},
                 "EmailX-Mailer": {},
                 "EmailHeaderField": {},
                 "EmailHeaders": {},
                 "EmailBody": {},
                 "EmailMessage": {},
                 "HashData": {
                   "$ref": "#/definitions/HashData"
                 },
                 "SignatureData": {
                   "$ref": "#/definitions/SignatureData"
                 }
               },
               "required": [],
               "additionalProperties": false
             },
             "Record": {
               "type": "object",
               "properties": {
                 "restriction": {
                   "$ref": "#/definitions/restriction"
                 },
                 "ext-restriction": {
                   "type": "string"
                 },
                 "observable-id": {
                   "$ref": "#/definitions/IDtype"
                 },
                 "DateTime": {},
                 "Description": {
                   "type": "string"
                 },
                 "Applicadtion": {},
                 "RecordPattern": {},
                 "RecordItem": {},
                 "URL": {
                   "$ref": "#/definitions/URLtype"
                 },
                 "FileData": {
                   "$ref": "#/definitions/FileData"
                 },
                 "WindowsRegistryKeysModified": {},
                 "CertificateData": {
                   "$ref": "#/definitions/CertificateData"
                 },
                 "AdditionalData": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/ExtensionType"
                   }
                 }
               },
               "required": [],
               "additionalProperties": false
             },
             "RecordPattern": {
               "type": "object",
               "properties": {
                 "RecordPatternValue": {},
                 "type": {},
                 "ext-type": {},
                 "offset": {},
                 "offsetunit": {},
                 "ext-offsetunit": {},
                 "instance": {
                   "type": "integer"
                 }
               },
               "required": [
                 "type"
               ],
               "additionalProperties": false
             },
             "WindowsRegistryKeysModified": {
               "type": "object",
               "properties": {
                 "observabile-id": {},
                 "Key": {}
               },
               "required": [
                 "Key"
               ],
               "additionalProperties": false
             },
             "Key": {
               "type": "object",
               "properties": {
                 "registryaction": {},
                 "ext-registryaction": {},
                 "observable-id": {
                   "$ref": "#/definitions/IDtype"
                 },
                 "KeyName": {},
                 "KeyValue": {}
               },
               "required": [
                 "KeyName"
               ],
               "additionalProperties": false
             },
             "CertificateData": {
               "type": "object",
               "properties": {
                 "restriction": {
                   "$ref": "#/definitions/restriction"
                 },
                 "ext-restriction": {
                   "type": "string"
                 },
                 "observable-id": {
                   "$ref": "#/definitions/IDtype"
                 },
                 "Certificate": {
                   "$ref": "#/definitions/Certificate"
                 }
               },
               "required": [
                 "Certificate"
               ],
               "additionalProperties": false
             },
             "Certificate": {
               "type": "object",
               "properties": {
                 "observable-id": {
                   "$ref": "#/definitions/IDtype"
                 },
                 "X509Data": {},
                 "Description": {
                   "type": "string"
                 }
               },
               "required": [
                 "X509Data"
               ],
               "additionalProperties": false
             },
             "FileData": {
               "type": "object",
               "properties": {
                 "restriction": {
                   "$ref": "#/definitions/restriction"
                 },
                 "ext-restriction": {
                   "type": "string"
                 },
                 "observable-id": {
                   "$ref": "#/definitions/IDtype"
                 },
                 "File": {
                   "$ref": "#/definitions/File"
                 }
               },
               "required": [
                 "File"
               ],
               "additionalProperties": false
             },
             "File": {
               "type": "object",
               "properties": {
                 "FileName": {
                   "type": "string"
                 },
                 "FileSize": {},
                 "FileType": {},
                 "URL": {
                   "$ref": "#/definitions/URLtype"
                 },
                 "HashData": {
                   "$ref": "#/definitions/HashData"
                 },
                 "SignatureData": {
                   "$ref": "#/definitions/SignatureData"
                 },
                 "AssociatedSoftware": {},
                 "FileProperties": {}
               },
               "required": [],
               "additionalProperties": false
             },
             "HashData": {
               "type": "object",
               "properties": {
                 "scope": {},
                 "HashTargetID": {},
                 "Hash": {
                   "$ref": "#/definitions/Hash"
                 },
                 "FuzzyHash": {
                   "$ref": "#/definitions/FuzzyHash"
                 }
               },
               "required": [
                 "scope"
               ],
               "additionalProperties": false
             },
             "Hash": {
               "type": "object",
               "properties": {
                 "DigestMethod": {
                   "type": "string"
                 },
                 "DigestValue": {
                   "type": "string"
                 },
                 "CanonicalizationMethod": {},
                 "Application": {}
               },
               "required": [
                 "DigestMethod",
                 "DigestValue"
               ],
               "additionalProperties": false
             },
             "FuzzyHash": {
               "type": "object",
               "properties": {
                 "FuzzyHashValue": {
                   "$ref": "#/definitions/ExtensionType"
                 },
                 "Application": {},
                 "AdditionalData": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/ExtensionType"
                   }
                 }
               },
               "required": [
                 "FuzzyHashValue"
               ],
               "additionalProperties": false
             },
             "SignatureData": {
               "type": "object",
               "properties": {
                 "Signature": {
                   "SignatureValue": "xxxxxxxx",
                   "id": "xxxxxxxx"
                 }
               },
               "required": [
                 "Signature"
               ],
               "additionalProperties": false
             },
             "Indicator": {
               "type": "object",
               "properties": {
                 "restriction": {
                   "$ref": "#/definitions/restriction"
                 },
                 "ext-restriction": {
                   "type": "string"
                 },
                 "IndicatorID": {
                   "$ref": "#/definitions/IndicatorID"
                 },
                 "AlternativeIndicatorID": {
                   "$ref": "#/definitions/AlternativeIndicatorID"
                 },
                 "Description": {
                   "type": "string"
                 },
                 "StartTime": {},
                 "EndTime": {},
                 "Confidence": {
                   "$ref": "#/definitions/Confidence"
                 },
                 "Contact": {
                   "$ref": "#/definitions/Contact"
                 },
                 "Observable": {},
                 "ObservableReference": {
                   "$ref": "#/definitions/ObservableReference"
                 },
                 "IndicatorExpression": {
                   "$ref": "#/definitions/IndicatorExpression"
                 },
                 "IndicatorReference": {
                   "$ref": "#/definitions/IndicatorReference"
                 },
                 "NodeRole": {
                   "$ref": "#/definitions/NodeRole"
                 },
                 "AttackPhase": {
                   "$ref": "#/definitions/AttackPhase"
                 },
                 "Reference": {
                   "$ref": "#/definitions/Reference"
                 },
                 "AdditionalData": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/ExtensionType"
                   }
                 }
               },
               "required": [
                 "IndicatorID"
               ],
               "additionalProperties": false
             },
             "IndicatorID": {
               "type": "object",
               "properties": {
                 "id": {},
                 "name": {
                   "type": "string"
                 },
                 "version": {
                   "type": "string"
                 }
               },
               "required": [
                 "name",
                 "version"
               ],
               "additionalProperties": false
             },
             "AlternativeIndicatorID": {
               "type": "object",
               "properties": {
                 "restriction": {
                   "$ref": "#/definitions/restriction"
                 },
                 "ext-restriction": {
                   "type": "string"
                 },
                 "IndicatorReference": {
                   "$ref": "#/definitions/IndicatorReference"
                 }
               },
               "required": [
                 "IndicatorReference"
               ],
               "additionalProperties": false
             },
             "Observable": {
               "type": "object",
               "properties": {
                 "restriction": {
                   "$ref": "#/definitions/restriction"
                 },
                 "ext-restriction": {
                   "type": "string"
                 },
                 "System": {},
                 "Address": {},
                 "DomainData": {
                   "$ref": "#/definitions/DomainData"
                 },
                 "EmailData": {},
                 "Service": {
                   "$ref": "#/definitions/Service"
                 },
                 "WindowsRegistryKeysModified": {},
                 "FileData": {
                   "$ref": "#/definitions/FileData"
                 },
                 "CertificateData": {
                   "$ref": "#/definitions/CertificateData"
                 },
                 "RegistryHandle": {},
                 "Record": {
                   "$ref": "#/definitions/Record"
                 },
                 "EventData": {},
                 "Incident": {},
                 "Expectation": {
                   "$ref": "#/definitions/Expectation"
                 },
                 "Reference": {
                   "$ref": "#/definitions/Reference"
                 },
                 "Assessment": {},
                 "DetectionPattern": {},
                 "HistoryItem": {},
                 "BulkObservable": {
                   "type": "string"
                 },
                 "AdditionalData": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/ExtensionType"
                   }
                 }
               },
               "required": [],
               "additionalProperties": false
             },
             "BulkObservable": {
               "type": "object",
               "properties": {
                 "type": {},
                 "ext-type": {},
                 "BulkObservableFormant": {},
                 "BulkObservableList": {
                   "type": "string"
                 },
                 "AdditionalData": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/ExtensionType"
                   }
                 }
               },
               "required": [],
               "additionalProperties": false
             },
             "BulkObservableFormat": {
               "type": "object",
               "properties": {
                 "Hash": {
                   "$ref": "#/definitions/Hash"
                 },
                 "AdditionalData": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/ExtensionType"
                   }
                 }
               },
               "required": [],
               "additionalProperties": false
             },
             "IndicatorExpression": {
               "type": "object",
               "properties": {
                 "operator": {},
                 "ext-operator": {
                   "type": "string"
                 },
                 "IndicatorExpression": {
                   "$ref": "#/definitions/IndicatorExpression"
                 },
                 "Observable": {},
                 "ObservableReference": {
                   "$ref": "#/definitions/ObservableReference"
                 },
                 "IndicatorReference": {
                   "$ref": "#/definitions/IndicatorReference"
                 },
                 "AdditionalData": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/ExtensionType"
                   }
                 }
               },
               "required": [],
               "additionalProperties": false
             },
             "ObservableReference": {
               "type": "object",
               "properties": {
                 "uid-ref": {}
               },
               "required": [
                 "uid-ref"
               ],
               "additionalProperties": false
             },
             "IndicatorReference": {
               "type": "object",
               "properties": {
                 "uid-ref": {},
                 "euid-ref": {
                   "type": "string"
                 },
                 "version": {
                   "type": "string"
                 }
               },
               "required": [],
               "additionalProperties": false
             },
             "AttackPhase": {
               "type": "object",
               "properties": {
                 "AttackPhaseID": {
                   "type": "string"
                 },
                 "URL": {
                   "$ref": "#/definitions/URLtype"
                 },
                 "Description": {
                   "type": "string"
                 },
                 "AdditionalData": {
                   "type": "array",
                   "items": {
                     "$ref": "#/definitions/ExtensionType"
                   }
                 }
               },
               "required": [],
               "additionalProperties": false
             }
           },
           "title": "IODEF-Document",
           "description": "JSON schema for IODEF-Document class",
           "type": "object",
           "properties": {
             "version": {
               "type": "string"
             },
             "lang": {
               "$ref": "#/definitions/lang"
             },
             "format-id": {
               "type": "string"
             },
             "private-enum-name": {
               "type": "string"
             },
             "private-enum-id": {
               "type": "string"
             },
             "Incidents": {
               "type": "array",
               "items": {
                 "$ref": "#/definitions/Incident"
               }
             },
             "AdditionalData": {
               "type": "array",
               "items": {
                 "$ref": "#/definitions/ExtensionType"
               }
             }
           },
           "required": [
             "version",
             "Incidents"
           ],
           "additionalProperties": false
         }
```

Figure 62: JSON schema

6. Acknowledgements

TBD.

7. IANA Considerations

This memo includes no request to IANA.

8. Security Considerations

This memo does not provide any further security considerations than the one described in RFC 5070-bis.

9. References

9.1. Normative References

[min_ref] authSurName, authInitials., "Minimal Reference", 2006.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

9.2. Informative References

[DOMINATION] Mad Dominators, Inc., "Ultimate Plan for Taking Over the World", 1984, <http://www.example.com/dominator.html>.

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, DOI 10.17487/RFC2629, June 1999, <http://www.rfc-editor.org/info/rfc2629>.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <http://www.rfc-editor.org/info/rfc3552>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, DOI 10.17487/RFC5226, May 2008, <http://www.rfc-editor.org/info/rfc5226>.

Author’s Address

Takeshi Takahashi
NICT
4-2-1 Nukui-Kitamachi
Koganei, Tokyo 184-8795
Japan

Phone: +81 42 327 5862
Email: takeshi_takahashi@nict.go.jp