Who do you think you are?

Stuart Murdoch, FIRST 2022
WHO

DO YOU THINK YOU ARE?
Britsoft: An Oral History
£30.00

Edited by Alex Wiltshire | Designed by Julia

Britsoft: An Oral History is a collective story of the early British games industry. Composed of interviews with thirty-five people who shaped the modern videogame, including David Braben (Elite), Peter Molyneux (Populous), Rob Hubbard (Commando) and Jeff Minter (Attack of the Mutant Camels), it documents a vibrant period of invention in Britain’s cultural history – the start of a new form of entertainment, created on ZX Spectrums, Commodore 64s, Amigas and Atari STs, in bedrooms and living rooms.
Who do you think you are?

*Part one - Standards*
MITRE Att&ck®
Submit a CVE Request

- Required
- **Select a request type**
  - Please choose an action
- **Enter your e-mail address**
  - Please enter a valid e-mail address where we can reach you.

⚠️ **IMPORTANT:** Please add cve-request@mitre.org and cve@mitre.org as safe senders in your email client before completing this form.

Enter a PGP Key (to encrypt)

If you would like us to send an encrypted response, please provide a PGP key up to 20,000 characters. If your PGP key is longer than 20,000 characters, provide a URL or contact us at cve@mitre.org to identify an alternative solution.
Abstract

Network security incidents, such as system compromises, viruses, phishing incidents, and denial of service, typically result in the loss of service, data, and resources both human and material. Network providers and Computer Security Incident Response Teams need to be equipped and ready to assist in communicating about security incidents with tools and procedures in place to prevent occurrence of an attack. Real-time Inter-network Defense outlines a proactive inter-network communication methodology to share incident handling data while integrating existing tools and mechanisms for incident tracing, source identification, and mitigation. This communication provides a way to achieve higher integrity levels on networks. Policy guidelines for handling incidents are recommended and can be agreed upon by a consortium using the security recommendations and considerations.

RID has found use within the international research communities, but has not been widely adopted in other sectors. This publication provides the specification to those communities that have adopted it, and communities currently considering solutions for real-time inter-network defense. The specification may also accelerate development of solutions where different transports or message formats are required by leveraging the data elements and structures specified here.
The Incident Object Description Exchange Format

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

The Incident Object Description Exchange Format (IODEF) defines a data representation that provides a framework for sharing information commonly exchanged by Computer Security Incident Response Teams (CSIRTs) about computer security incidents. This document describes the information model for the IODEF and provides an associated data model specified with XML Schema.
Figure 59: The Indicator Class
Resource-Oriented Lightweight Information Exchange (ROLIE)

Abstract

This document defines a resource-oriented approach for security automation information publication, discovery, and sharing. Using this approach, producers may publish, share, and exchange representations of software descriptors, security incidents, attack indicators, software vulnerabilities, configuration checklists, and other security automation information as web-addressable resources. Furthermore, consumers and other stakeholders may access and search this security information as needed, establishing a rapid and on-demand information exchange network for restricted internal use or public access repositories. This specification extends the Atom Publishing Protocol and Atom Syndication Format to transport and share security automation resource representations.

Status of This Memo

This is an Internet Standards Track document.
<?xml version="1.0" encoding="utf-8"?>
<!-
TITLE: OpenIOC 1.1 Schema
VERSION: 1.1 (draft)
DESCRIPTION: OpenIOC 1.1 Schema document, describing the structure of OpenIOC 1.1.
LICENSE: Copyright 2013 Mandiant Corporation. Licensed under the Apache 2.0 license.
Mandiant licenses this file to you under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at:
http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
implied. See the License for the specific language governing
permissions and limitations under the License.
-/>
## DDoS Open Threat Signaling (DOTS) Architecture

### RFC 8811

<table>
<thead>
<tr>
<th>Status</th>
<th>IESG evaluation record</th>
<th>IESG writeups</th>
<th>Email expansions</th>
<th>History</th>
</tr>
</thead>
</table>

### Versions:

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>Mar 2016</td>
<td>draft-mortensen-dots-architecture</td>
</tr>
<tr>
<td>00</td>
<td>Jul 2016</td>
<td>draft-ietf-dots-architecture</td>
</tr>
<tr>
<td>01</td>
<td>Oct 2016</td>
<td>rfc8811</td>
</tr>
<tr>
<td>02</td>
<td>Mar 2017</td>
<td></td>
</tr>
<tr>
<td>03</td>
<td>Jun 2017</td>
<td></td>
</tr>
<tr>
<td>04</td>
<td>Sep 2017</td>
<td></td>
</tr>
<tr>
<td>05</td>
<td>Dec 2017</td>
<td></td>
</tr>
<tr>
<td>06</td>
<td>Mar 2018</td>
<td></td>
</tr>
<tr>
<td>07</td>
<td>Jun 2018</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Sep 2018</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Nov 2018</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Jan 2019</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Mar 2019</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Aug 2020</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Aug 2020</td>
<td></td>
</tr>
</tbody>
</table>

### Document Information:

- **Type**: RFC - Informational (August 2020)
- Was [draft-ietf-dots-architecture](https://datatracker.ietf.org/doc/draft-ietf-dots-architecture/) (dots WG)

### Authors:

- Andrew Mortensen
- Tirumaleswar Reddy.K
- Flemming Andreasen
- Nik Teague
- Rich Compton

### Last Updated:

- 2020-08-17
Malware Attribute Enumeration and Characterization (MAEC™)

New! MAEC 5.0 now available!
**Indicator Pattern Language**

Indicator patterns in STIX 1.x were expressed using XML syntax. This made all but the simplest patterns difficult to create and to understand. STIX 2.0 takes a different approach, specifying a language for patterns which is independent of the serialization language. Patterns written in the STIX patterning language are more compact and easier to read. Additionally, there is no confusion between patterns and observations, because a pattern is not a top-level object, but a property of an indicator object.

**STIX 1 Indicator Example**

```xml
<stix:Indicator id="example:indicator-01"
    timestamp="2017-02-09T12:11:11.415000+00:00"
    xsi:type='indicator:IndicatorType'>
    <indicator:Title>HTRAN Hop Point Accessor</indicator:Title>
</stix:Indicator>

<stix:Kill_Chains>
    <stixCommon:Kill_Chain id="stix:TTP-02"
        name="mandiant-attack-lifecycle-model">;
        <stixCommon:Kill_Chain_Phase name="establish-foothold"
            phase_id="stix:TTP-03"/>
            ...
</stix:Kill_Chains>
```

**STIX 2 Indicator Example with Pattern**

```json
{
    "type": "indicator",
    "id": "indicator--01",
    "created": "2017-02-09T12:11:11.415000Z",
    "modified": "2017-02-09T12:11:11.415000Z",
    "name": "HTRAN Hop Point Accessor",
    "pattern": "[ipv4-addr:value = '10.1.0.0/15'],
    "labels": [ "malicious-activity" ],
    "valid_from": "2015-05-10T09:00:00.000000Z",
    "kill_chain_phases": [ {
        "kill_chain_name": "mandiant-attack-lifecycle-model",
        "phase_name": "establish-foothold"
    } ]
}
```
Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence (CTI).

STIX enables organizations to share CTI with one another in a consistent and machine readable manner, allowing security communities to better understand what computer-based attacks they are most likely to see and to anticipate and/or respond to those attacks faster and more effectively.

STIX is designed to improve many different capabilities, such as collaborative threat analysis, automated threat exchange, automated detection and response, and more.

Trusted Automated Exchange of Intelligence Information (TAXII™) is an application layer protocol for the communication of cyber threat information in a simple and scalable manner.

TAXII is a protocol used to exchange cyber threat intelligence (CTI) over HTTPS. TAXII enables organizations to share CTI by defining an API that aligns with common sharing models.

TAXII is specifically designed to support the exchange of CTI represented in STIX.
Cyber Observable eXpression (CybOX™) Archive Website

A structured language for cyber observables.

**IMPORTANT NOTICE:** The CybOX Language has been integrated into Version 2.0 of Structured Threat Information eXpression (STIX™). Go to the STIX 2.0 documentation website.
3. TLP definitions

a. **TLP:RED** = Not for disclosure, restricted to participants only.
   Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

b. **TLP:AMBER** = Limited disclosure, restricted to participants' organizations.
   Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing; these must be adhered to.**

c. **TLP:GREEN** = Limited disclosure, restricted to the community.
   Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not released outside of the community.

d. **TLP:WHITE** = Disclosure is not limited.
   Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.
Who do you think you are?

Part two - Organisations
Authorized Users of the CERT Mark

"CERT" is a registered trademark owned by Carnegie Mellon University. CMU has decided to discontinue its practice of licensing the CERT mark internationally. As a result, we will no longer pursue license agreements outside of the United States. Computer security incident response teams (CSIRTs), within the United States, that share the SEI’s commitment to improving the security of networks connected to the Internet may apply for authorization to use the "CERT" mark in their names. For those CSIRTs outside of the U.S. CMU recommends that you consult with your own trademark counsel regarding your rights going forward. Should a non-U.S. CSIRT seek to file a trademark application for its own name including "CERT" in the country where it is located (and not the United States), CMU will not oppose the application.

Contact Us

Interested CSIRTs based in the United States must complete and submit a qualification form. Contact us to request a form.

Authorized to Use "CERT" Graphic

We created a graphic that authorized CSIRTs can add to their websites.* This graphic provides a visual indication that the CSIRT is part of a network of teams that provide similar services. The graphic indicates that the CSIRT is licensed to use "CERT" in its name; it does not indicate that we endorse or recommend any of the content or services on these sites. Organizations should also adhere to SEI guidelines for the use of "CERT."

* This seal is for use on the organization’s website only; it cannot be used on any other materials.

This image depicts how AlgoCERT is using the CERT mark on its website.
FIRST Members around the world

Search FIRST Teams
There are 612 Teams in 99 different countries.
FIRST members growth by year*

(*) The statistic measurement method and regional breakdown changed in 2007.
Field Offices

Our local FBI offices are all about protecting your communities.

The FBI has 56 field offices (also called divisions) centrally located in major metropolitan areas across the U.S. and Puerto Rico. They are the places where we carry out investigations, assess local and regional crime threats, and work closely with partners on cases and operations. Each field office is overseen by a special agent in charge, except our offices in Los Angeles, New York City, and Washington, D.C., which are headed by an assistant director in charge due to their large size. Within these field offices are a total of about 380 resident agencies located in smaller cities and towns. Resident agencies are managed by supervisory special agents.
What happened in 1998?

- Clinton - Presidential Decision Directive/NSC-63
- 22 May 1998 “Critical Infrastructure Protection”

“strongly encourage the creation of a private sector information sharing and analysis center [ISAC]”
MEMBER ISACS

AMERICAN CHEMISTRY COUNCIL

The American Chemistry Council (ACC) represents a diverse set of companies engaged in the business of chemistry. An innovative, $553 billion enterprise, our mission is to deliver value to our members through advocacy, member engagement, political advocacy, information sharing, communications, and scientific research. The Chemical Information Technology Center (ChemITC®) of the ACC is a forum for companies to address common IT, cyber security, and security issues. Through strategic programs and networking groups dedicated to addressing specific technology issues, ChemITC is committed to advancing the use of information technology to streamline processes, manage cyber threats, and improve decision-making. www.americanchemistry.com/

AUTOMOTIVE ISAC

The Automotive Information Sharing and Analysis Center (Auto-ISAC) is a non-profit information sharing organization that provides a trusted environment and platform for automotive manufacturers and suppliers to collaborate on cybersecurity. Founded by a global group of automakers in 2015, the Auto-ISAC is the central hub for industry-wide sharing of cyber threats, vulnerabilities, and best practices related to the connected vehicle. We embrace a working together model, engaging across the community with automotive strategic partners, trade associations, researchers and universities, and government. Membership is open to light and heavy-duty automotive manufacturers, suppliers, carriers, and fleet operators. www.automotiveisac.com
Membership Benefits

FS-ISAC members around the world receive trusted and timely expert information that increases sector-wide knowledge of physical and cybersecurity threats.

Based on level of service, FS-ISAC members take advantage of a host of important benefits, including early notification of security threats and attacks, anonymous information sharing across the financial services industry, regularly scheduled member meetings and bi-weekly conference calls.

If your firm is not a financial institution, click here for information on how to participate.

Membership Guidelines

The table below outlines the minimum membership level at which your firm is required to join.

<table>
<thead>
<tr>
<th>Core</th>
<th>Standard</th>
<th>Premier</th>
<th>Gold</th>
<th>Platinum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banks, Credit Unions, Insurance/Reinsurance Companies and Publicly Held Securities/Brokerage Firms</td>
<td>Assets: $1B - $10B</td>
<td>Assets: $10B - $20B</td>
<td>Assets: $20B - $100B</td>
<td>Assets: $100B - $250B</td>
</tr>
<tr>
<td>Financial Service Trade Associations, Financial Industry Utilities, Pension Funds, Processors, Utilities and Privately Held Stan</td>
<td>Revenue: &lt; $100M</td>
<td>Revenue: $100M - $1B</td>
<td>Revenue: $1B - $2.5B</td>
<td>Revenue: $2.5B - $5B</td>
</tr>
</tbody>
</table>

Protect your firm and valued customers while taking an active role in safeguarding critical financial infrastructures. Join your peers by becoming a member of FS-ISAC. For more information, please use our membership inquiry form, or contact us at 877-612-2622.

Compare FS-ISAC Membership Benefits

<table>
<thead>
<tr>
<th>Core</th>
<th>Standard</th>
<th>Premier</th>
<th>Gold</th>
<th>Platinum</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Access Credentials</td>
<td>$850.00/yr/yr Join Now</td>
<td>$5,000.00/yr/yr Join Now</td>
<td>$10,000.00/yr/yr Join Now</td>
<td>$24,950.00/yr/yr Join Now</td>
</tr>
<tr>
<td>CINS Crisis Notifications</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Government, Member, and Partner Alerts</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Customized Email Notification Profile</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>24 x 7 Watch Desk</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Member Submissions</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Member Surveys</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Industry Best Practices</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Member Contact Directory</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Threat Conference Calls</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>FS-ISAC Committees/Workgroups</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Number of Free Passes for Member Meetings/Summits</td>
<td>2</td>
<td>5</td>
<td>10</td>
<td>Yes</td>
</tr>
<tr>
<td>XML Data Feeds</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>FS-ISAC Governance</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Cyber Obama

• 2013 - Executive Order 13691
  – “Promoting Private Sector Cybersecurity Information Sharing”

• 2015 – Cybersecurity Information Sharing Act (CISA)
Sec. 2. Information Sharing and Analysis Organizations. (a) The Secretary of Homeland Security (Secretary) shall strongly encourage the development and formation of Information Sharing and Analysis Organizations (ISAOs).

(b) ISAOs may be organized on the basis of sector, sub-sector, region, or any other affinity, including in response to particular emerging threats or vulnerabilities. ISAO membership may be drawn from the public or private sectors, or consist of a combination of public and private sector organizations. ISAOs may be formed as for-profit or nonprofit entities.

(c) The National Cybersecurity and Communications Integration Center (NCCIC), established under section 226(b) of the Homeland Security Act of 2002 (the "Act"), shall engage in continuous, collaborative, and inclusive coordination with ISAOs on the sharing of information related to cybersecurity risks and incidents, addressing such risks and incidents, and strengthening information security systems consistent with sections 212 and 226 of the Act.

(d) In promoting the formation of ISAOs, the Secretary shall consult with other Federal entities responsible for conducting cybersecurity activities, including Sector-Specific Agencies, independent regulatory agencies at their discretion, and national security and law enforcement agencies.
The U.S. Department of Homeland Security (DHS) Cyber Information Sharing and Collaboration Program (CISCP) enables actionable, relevant, and timely unclassified information exchange through trusted public-private partnerships across all critical infrastructure (CI) sectors. CISCP fosters this collaboration by leveraging the depth and breadth of DHS cybersecurity capabilities within a focused operational context. Through analyst-to-analyst sharing of threat and vulnerability information, CISCP helps partners manage cybersecurity risks and enhances our collective ability to proactively detect, prevent, mitigate, respond to, and recover from cybersecurity incidents. CISCP’s overall objective is to build cybersecurity resiliency and to harden the defenses of the United States and its strategic partners.
Homeland Security Information Network

The Cybersecurity and Infrastructure Security Agency (CISA) uses the Homeland Security Information Network (HSIN) to provide a secure, web-based, collaborative system to share sensitive cyber-related information and news with select cybersecurity partners. The CISA Portal on HSIN enables the U.S. Government and its partners to enhance their shared situational awareness on cyber activities by promoting a collaborative workspace for cybersecurity-related discussions.

The Department of Homeland Security (DHS), through CISA, shares threat indicators and advisory information with public, private, and international partners in the network defense community of practice using the CISA Portal, which provides a number of features that enable collaboration and information sharing including:

- A secure messaging capability to allow CISA and its partners to communicate and coordinate during cybersecurity incidents.
- A document library to share documents, files, and indicators of compromise.
- A web conferencing solution for webinars and online meetings.
- A message board for communication and coordination.

To request access, email HSIN.HelpDesk@hq.dhs.gov.
National Infrastructure are those facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends. It also includes some functions, sites and organisations which are not critical to the maintenance of essential services, but which need protection due to the potential danger to the public (civil nuclear and chemical sites for example).

In the UK, there are 13 national infrastructure sectors: Chemicals, Civil Nuclear, Communications, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport and Water. Several sectors have defined ‘sub-sectors’: Emergency Services for example can be split into Police, Ambulance, Fire Services and Coast Guard.

Each sector has one or more Lead Government Department(s) (LGD) responsible for the sector, and ensuring protective security is in place for critical assets.

Not everything within a national infrastructure sector is judged to be ‘critical’. The UK government’s official definition of CNI is:

‘Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:

a) Major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or

b) Significant impact on national security, national defence, or the functioning of the state.’

CPNI is focussed on providing advice and assistance to those who have responsibility for protecting these most crucial elements of the UK’s national infrastructure from national security threats.
DIB – MANDATORY SHARING
Cooperation among all the Member States, by setting up a cooperation group, in order to support and facilitate strategic cooperation and the exchange of information among Member States. They will also need to set up a CSIRT Network, in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks;
NEW YORK STATE
DEPARTMENT OF FINANCIAL SERVICES
23 NYCRR 500

CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES

I, Maria T. Vullo, Superintendent of Financial Services, pursuant to the authority granted by sections 102, 201, 202, 301, 302 and 408 of the Financial Services Law, do hereby promulgate Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York, to take effect March 1, 2017, to read as follows:

(ALL MATTER IS NEW)

Section 500.00 Introduction.

The New York State Department of Financial Services ("DFS") has been closely monitoring the ever-growing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors. Recently, cybercriminals have sought to exploit technological vulnerabilities to gain access to sensitive electronic data. Cybercriminals can cause significant financial losses for DFS regulated entities as well as for New York consumers whose private information may be revealed and/or stolen for illicit purposes. The financial services industry is a significant target of cybersecurity threats. DFS appreciates that many firms have proactively increased their cybersecurity programs with great success.

Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted, while not being overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances. Accordingly, this regulation is designed to promote the protection of customer information as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. Senior management must take this issue seriously and be responsible for the organization’s cybersecurity program and file an annual certification confirming compliance with these regulations. A regulated entity’s cybersecurity program must ensure the safety and soundness of the institution and protect its customers.
Participate | Collaborate | Innovate