# MISP development update

6 momths update

Team CIRCL

MISP Training @ Luxembourg December Edition 2019
20191203

# What happened in the past 6 months?

- **13** new MISP **releases** - on track for 2 / month
- Over **2000 commits** for the core alone from **34 contributors**
- Progress on a massive rework that is underways
- Before we get to the highlights...

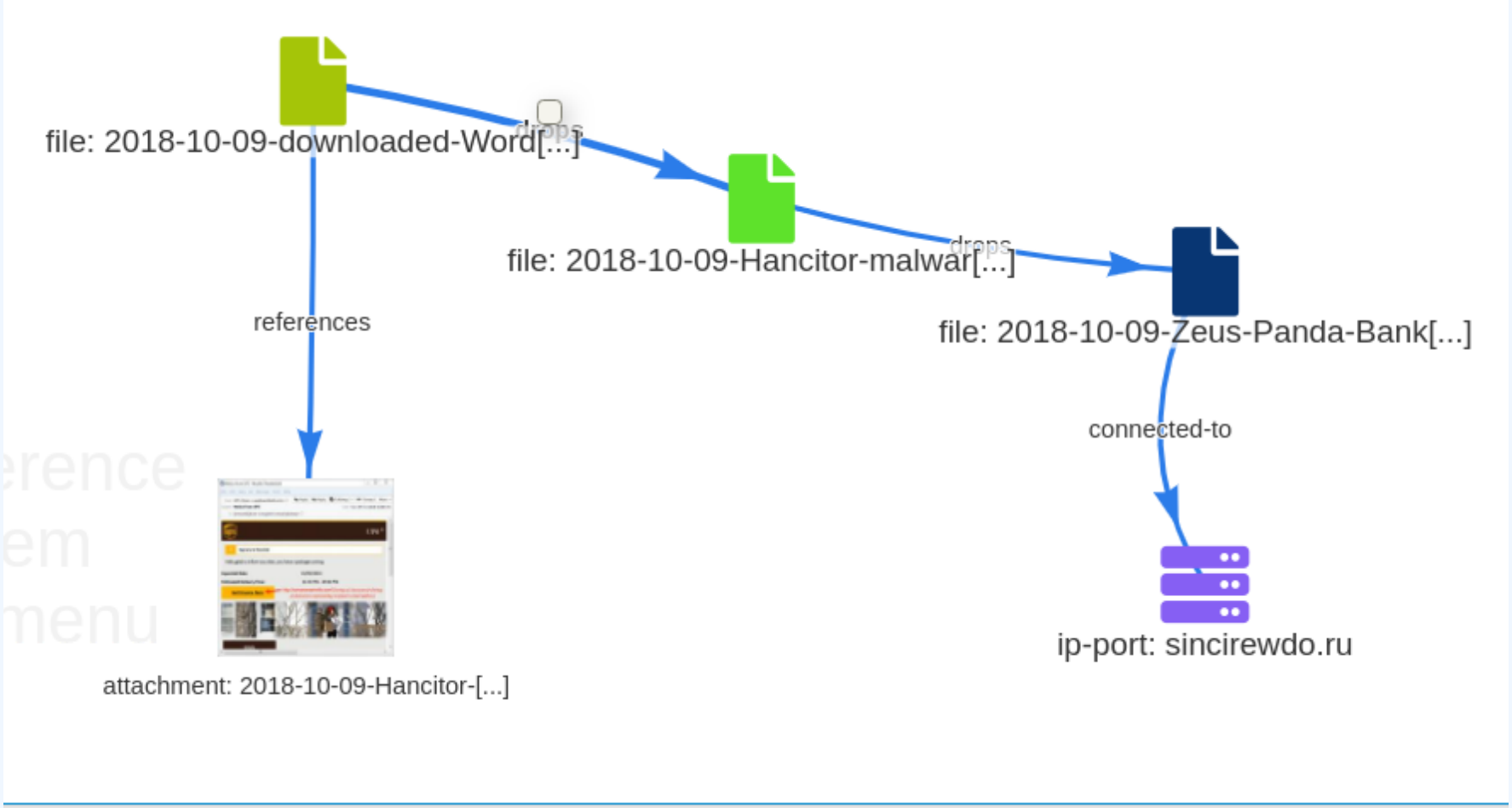
# Standardisation for open source formats

- `https://www.misp-standard.org`
- Standardising the **MISP related** and **other open source** formats
- We want a vehicle for publishing standards **without giving up control**
- Let us know if you would like to be listed!

# Steady growth in efforts to share refined informati

- Both on a **data** and a **context** level
- Growth in the **community's** and **tooling's** maturity
- **ATT&CK**'s quick adoption is partially to blame for recent surge
- Also a side effect of MISP becoming a sharing tool for completely **different domains**

# Object relations



# ATT&CK

mitre-mobile-attack | **mitre-attack** | mitre-pre-attack

0 — 98 — Show all

| Initial access (11 items) | Execution (34 items) | Persistence (63 items) | Privilege escalation (32 items) | Defense evasion (74 items) | Credential access (24 items) | Discovery (25 items) | Lateral movement (21 items) | Collection (14 items) | Command and control (22 items) | Exfiltration (10 items) | Impact (16 items) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Spearphishing Attachment | Scripting | Registry Run Keys / Startup Folder | Process Injection | Obfuscated Files or Information | Input Capture | System Information Discovery | Remote File Copy | Data from Local System | Standard Application Layer Protocol | Exfiltration Over Command and Control Channel | Resource Hijacking |
| Spearphishing Link | Execution through API | Scheduled Task | Scheduled Task | File Deletion | Credential Dumping | Process Discovery | Remote Desktop Protocol | Screen Capture | Commonly Used Port | Data Encrypted | Data Encrypted for Impact |
| Exploit Public-Facing Application | Scheduled Task | Hooking | Hooking | Scripting | Hooking | File and Directory Discovery | Windows Admin Shares | Input Capture | Remote File Copy | Automated Exfiltration | Inhibit System Recovery |
| Supply Chain Compromise | Command-Line Interface | New Service | New Service | Deobfuscate/Decode Files or Information | Credentials in Files | Query Registry | Pass the Ticket | Clipboard Data | Custom Cryptographic Protocol | Data Compressed | Stored Data Manipulation |
| Drive-by Compromise | User Execution | Hidden Files and Directories | DLL Search Order Hijacking | Modify Registry | Brute Force | System Network Configuration Discovery | Application Deployment Software | Automated Collection | Standard Cryptographic Protocol | Exfiltration Over Alternative Protocol | Data Destruction |
| Valid Accounts | PowerShell | DLL Search Order Hijacking | Bypass User Account Control | Process Injection | Account Manipulation | Account Discovery | Logon Scripts | Data Staged | Custom Command and Control Protocol | Exfiltration Over Other Network Medium | Network Denial of Service |
| Trusted Relationship | Rundll32 | Valid Accounts | Valid Accounts | Masquerading | Credentials in Registry | System Time Discovery | Exploitation of Remote Services | Audio Capture | Data Encoding | Scheduled Transfer | Runtime Data Manipulation |
| External Remote Services | Service Execution | PowerShell Profile | Exploitation for Privilege Escalation | Rundll32 | Forced Authentication | Network Share Discovery | Pass the Hash | Data from Removable Media | Data Obfuscation | Exfiltration Over Physical Medium | Service Stop |
| Spearphishing via Service | Execution through Module Load | Web Shell | PowerShell Profile | Disabling Security Tools | Bash History | System Network Connections Discovery | Remote Services | Email Collection | Connection Proxy | Data Transfer Size Limits | Account Access Removal |
| Replication Through Removable Media | Exploitation for Client Execution | Windows Management Instrumentation Event Subscription | Web Shell | Software Packing | Exploitation for Credential Access | Security Software Discovery | Replication Through Removable Media | Data from Network Shared Drive | Web Service | Transfer Data to Cloud Account | Defacement |
| Hardware Additions | Windows Management Instrumentation | Account Manipulation | Access Token Manipulation | Connection Proxy | Input Prompt | System Owner/User Discovery | Third-party Software | Video Capture | Fallback Channels | | Disk Content Wipe |
| | Mshta | BITS Jobs | Accessibility Features | Hidden Files and Directories | Private Keys | System Service Discovery | AppleScript | Man in the Browser | Uncommonly Used Port | | Disk Structure Wipe |
| | Regsvr32 | Create Account | Application Shimming | Code Signing | Cloud Instance Metadata API | Application Window Discovery | Application Access Token | Data from Information Repositories | Remote Access Tools | | Endpoint Denial of Service |

# ATT&CK LIKE MATRICES

example-of-threats

Show all

| Setup \| party/candidate registration *(3 items)* | Setup \| electoral rolls *(3 items)* | Campaign \| campaign IT *(5 items)* | All phases \| governement IT *(3 items)* | Voting \| election technology *(7 items)* | Campaign/public communication \| media/press |
|---|---|---|---|---|---|
| DoS or overload of party/campaign registration, causing them to miss the deadline | Deleting or tampering with voter data | Hacking campaign websites (defacement, DoS) | DoS or overload of government websites | Breach of voters privacy during the casting of votes | Defacement, DoS or overload of websites or other systems used for publication of the results |
| Fabricated signatures from sponsor | DoS or overload of voter registration system, suppressing voters | Hacking candidate laptops or email accounts | Hacking campaign websites, spreading misinformation on the election process, registered parties/candidates, or results | Software bug altering results | Hacking of internal systems used by media or press |
| Tampering with registrations | Identity fraud during voter registration | Hacking candidate laptops or email accounts | Hacking/misconfiguration of government servers, communication networks, or endpoints | Tampering or DoS of communication links uesd to transfer (interim) results | Tampering, DoS, or overload of media communication links |
| | | Leak of confidential information | | Tampering or DoS of voting and/or vote confidentiality during or after the elections | |
| | | Misconfiguration of a website | | Tampering with logs/journals | |
| | | | | Tampering with supply chain involved in the movement or transfer data | |
| | | | | Tampering, DoS or overload of the systems used for counting or aggregating results | |

Select Some Options

Cancel

# Community management

- Sectorial, regional, topical groupings becoming more organised
- Inherently more difficult to find the right communities
- We're starting to build an opt-in **community registry**
- Still very early days, but let us know if you would like to **announce yourselves**!

# Community request

circl.lu
Computer Incident
Response Center
LUXEMBOURG

## Community CIRCL Private Sector Information Sharing Community - aka MISPPRIV

| | |
|---|---|
| **Id** | 1 |
| **UUID** | 3ab3a65a-0171-401a-9895-8d42bc7bed7c |
| **Name** | CIRCL Private Sector Information Sharing Community - aka MISPPRIV |
| **Host organisation** | CIRCL (55f6ea5e-2c60-40e5-964f-47a8950d210f) |
| **Vetted by MISP-project** | **Yes** |
| **Type** | Vetted Information Sharing Community |
| **Description** | CIRCL operates a fairly large MISP sharing community (more than 1100 international organizations are members) mainly targeting private organizations, companies, financial organizations or IT security companies. Computer Incident Response Center Luxembourg (CIRCL) operates this sharing community for the benefit of the security community at large. |
| **Email** | info@circl.lu |
| **Sector** | Various |
| **Nationality** | International |
| **GnuPG key** | ▶ Details |

# Sightings improved

- More organisations involved in the feedback-loop of reporting back sightings
- Sighting synchronisation improved
- Alternate sighting back-end for heavy, bulk sightings
- SightingDB, open source, developed by Devo
- Experimental for now, but fully functional.
- SightingDB standard for alternate implementations via misp-standard.org

# Various improvements to taxonomies

- Tag exclusivity allows for taxonomies with inherent rules
  - For example: It makes no sense to have multiple TLP tags on an event
  - You can also restrict on a predicate level
- Require taxonomies to be set
  - Certain taxonomies can be set as requirements for publishing in a community
  - Example: No TLP/PAP? No right to publish.

# Alerting rules

- First steps for our user settings system
- Customise the rules that decide what you want to get alerted on

Setting

publish_alert_filter

Value

```
Example:
{
    "AND": {
        "NOT": {
            "EventTag.name": [
                "%osint%"
            ]
        },
        "OR": {
            "Tag.name": [
                "tlp:green",
                "tlp:amber",
```

# Decaying of indicators

- MISP has a powerful toolbox that allows users to filter their dataset based on their needs
- We were still missing a way to use all of these systems in combination to decay indicators
- Move the decision making **from complex filter options to** complex **decay models**
- Decay models would take into account various **taxonomies**, **sightings**, the **type** of each indicator **Sightings** and **Creation date**
- The first iteration of what we have in MISP now took:
  - 2 years of research
  - 3 published research papers
  - A lot of prototyping

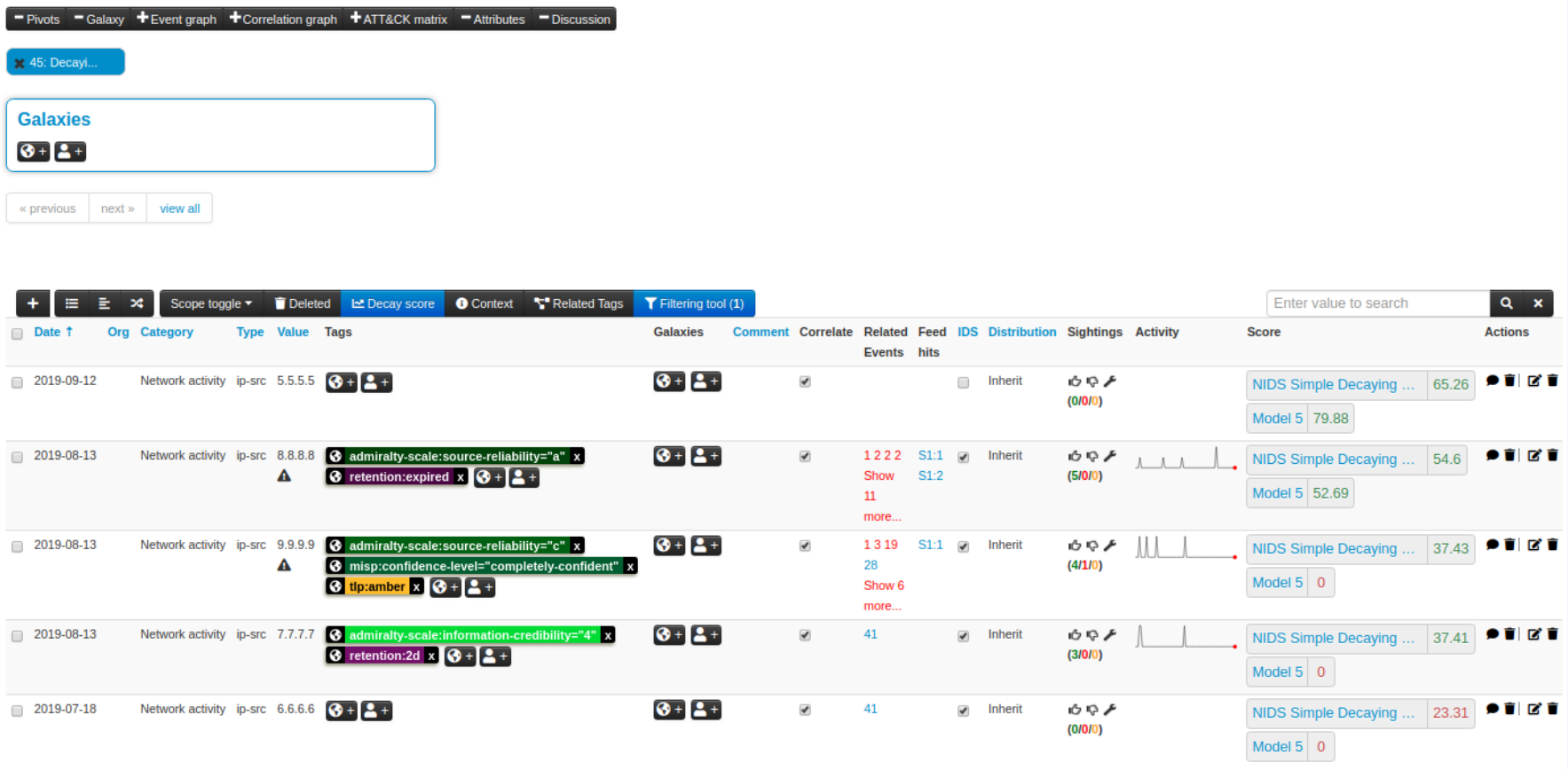
# Scoring Indicators: Our solution

$$\texttt{score}(\texttt{Attribute}) = \texttt{base\_score}(\texttt{Attribute, Model}) \bullet \texttt{decay}(\texttt{Model, time})$$

Where,

- $\texttt{score} \in [0, 100]$
- $\texttt{base\_score} \in [0, 100]$
- `decay` is a function defined by model's parameters controlling decay speed
- `Attribute` Contains *Attribute*'s values and metadata (*Taxonomies*, *Galaxies*, ...)
- `Model` Contains the *Model*'s configuration

# Implementation in MISP: Event/view




- Decay score toggle button
  - Shows Score for each *Models* associated to the *Attribute* type

# Implementation in MISP: API result

/attributes/restSearch


```
"Attribute": [
  {
    "category": "Network activity",
    "type": "ip-src",
    "to_ids": true,
    "timestamp": "1565703507",
    [...]
    "value": "8.8.8.8",
    "decay_score": [
      {
        "score": 54.475223849544456,
        "decayed": false,
        "DecayingModel": {
          "id": "85",
          "name": "NIDS Simple Decaying Model"
        }
```

# Implementation in MISP: Index

## Decaying Models

« previous next »

All Models | My Models | Shared Models | Default Models

| ID | Organization | Usable to everyone | Name | Description | Parameters { } | Formula | # Assigned Types | Version | Enabled | Actions |
|---|---|---|---|---|---|---|---|---|---|---|
| 29 | 1 | ✔ | Phishing model | Simple model to rapidly decay phishing website. | { "lifetime": 3, "decay_speed": 2.3, "threshold": 30, "default_base_score": 80, "base_score_config": { "estimative-language": 0.5, "phishing": 0.5 } } | Polynomial | 9 | 1 | ✔ | |
| 85 | 1 | ✘ | NIDS Simple Decaying Model MISP | Simple decaying model for Network Intrusion Detection System (NIDS). | { "lifetime": 120, "decay_speed": 2, "threshold": 30, "default_base_score": 80, "base_score_config": { "estimative-language": 0.25, "priority-level": 0.25, "retention": 0.25, "targeted-threat-index": 0.125, "false-positive": 0.125 } } | Polynomial | 13 | 1 | ✔ | |

Page 1 of 1, showing 2 records out of 2 total, starting on record 1, ending on 2

« previous next »

View

update, add, create, delete, enable, export, import

# Implementation in MISP: Fine tuning tool

Home | Event Actions | Galaxies | Input Filters | Global Actions | Sync Actions | Administration | Audit | MISP

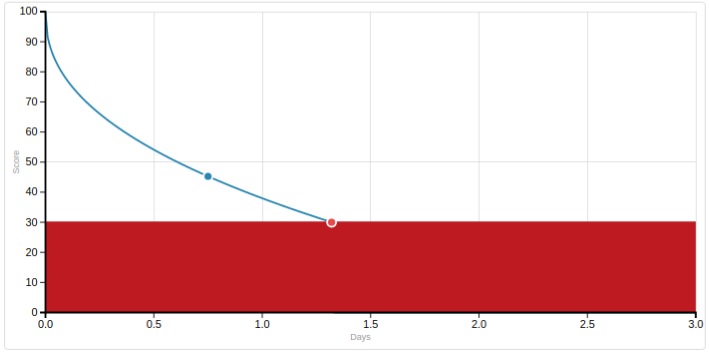
Import Decaying Model
Add Decaying Model
Decaying Tool
List Decaying Models

## Decaying Of Indicator Fine Tuning Tool

Show All Types | Show MISP Objects | Search Attribute Type

| Attribute Type | Category | Model ID |
|---|---|---|
| aba-rtn | Financial fraud | |
| authentihash | Payload delivery | |
| bank-account-nr | Financial fraud | |
| bic | Financial fraud | |
| bin | Financial fraud | |
| bro | Network activity | 10 11 |
| btc | Financial fraud | 11 |
| cc-number | Financial fraud | |
| cdhash | Payload delivery | |
| community-id | Network activity | |
| domain | Network activity | |
| domain\|ip | Network activity | 10 84 |
| email-attachment | Payload delivery | |
| email-dst | Network activity | 11 |
| email-src | Payload delivery | |
| filename | Payload delivery | |
| filename\|authentihash | Payload delivery | |
| filename\|impfuzzy | Payload delivery | |
| filename\|imphash | Payload delivery | |
| filename\|md5 | Payload delivery | 13 |
| filename\|pehash | Payload delivery | 13 |
| filename\|sha1 | Payload delivery | 13 |

Polynomial




Lifetime 3 days
Decay speed 2.3
Cutoff threshold 30

| | |
|---|---|
| Expire after (lifetime) | 1 days and 7 hours |
| Score halved after (Half-life) | 0 day and 6 hours |

Adjust base score | Simulate this model

Phishing model | Simple model to rapidly decay | Edit

All available models | My models | Default models

| | ID | Model Name | Org ID | Description | Formula | Parameters: Lifetime | Decay speed | Threshold | Default basescore | Basescore config | Settings | # Types | Enabled | Action |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ✓ | 29 | Phishing model | 1 | Simple model to rapidly decay phishing website. | Polynomial | 3 | 2.3 | 30 | 80 | estimative-language 0.5; phishing 0.5 | | 9 | ✓ | Load model |

Crea

modify, visualise, perform mapping

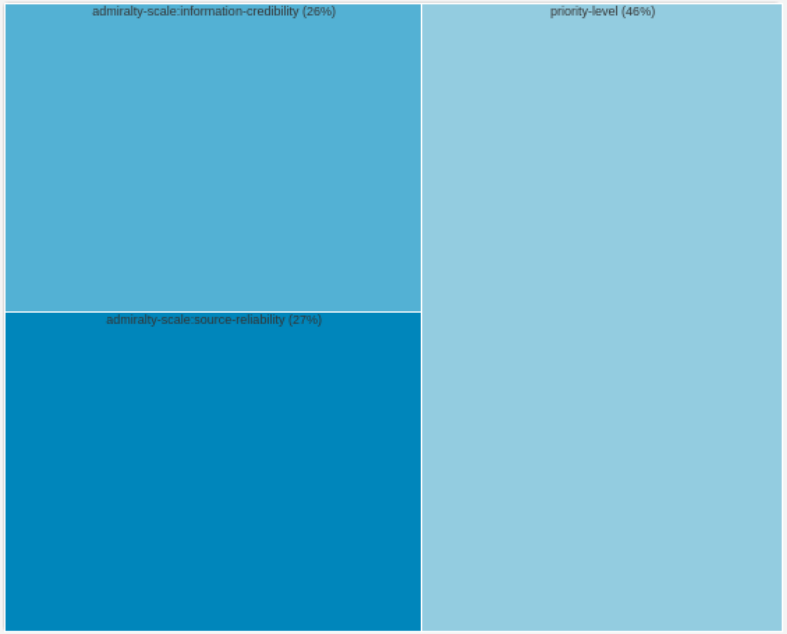
# Implementation in MISP: base_score tool

Search Taxonomy

3 not having numerical value

Default basescore 80

| Taxonomies | Weight |
|---|---|
| admiralty-scale | |
| source-reliability | 31 |
| information-credibility | 30 |
| priority-level | |
| priority-level | 53 |
| retention | |
| retention | 0 |
| estimative-language | |
| likelihood-probability | 0 |
| confidence-in-analytic-judgment | 0 |
| misp | |
| confidence-level | 0 |
| threat-level | 0 |
| automation-level | 0 |
| phishing | |
| state | 0 |
| psychological-acceptability | 0 |
| Excluded | |




Placeholder for `Organisation source confidence`

## Example

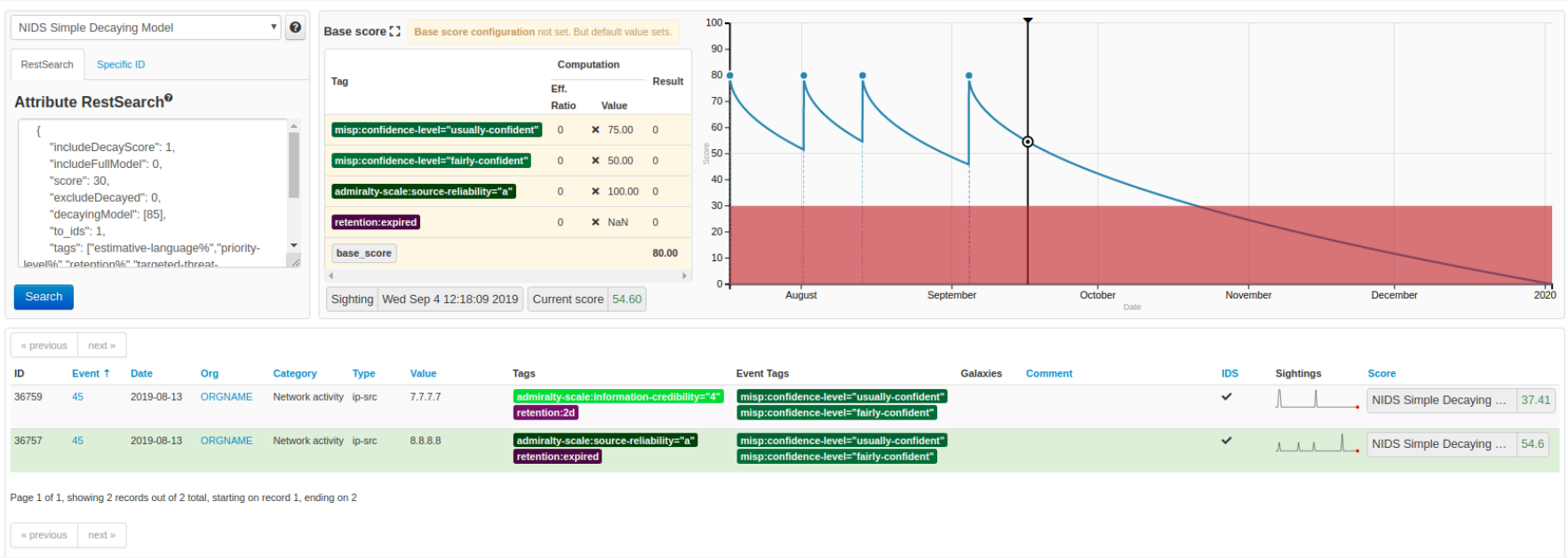
| Attribute | Tags | Base score |
|---|---|---|
| Tag your attribute | + | |
| Attribute 1 | admiralty-scale:information-credibility="5" | 0.0 |
| Attribute 2 | priority-level:baseline-minor admiralty-scale:source-reliability="d" admiralty-scale:information-credibility="2" | 38.2 |
| Attribute 3 | priority-level:severe admiralty-scale:information-credibility="2" | 84.6 |

## Computation steps

| Tag | Computation | | | Result |
|---|---|---|---|---|
| | Eff. Ratio | | Value | |
| priority-level:baseline-minor | 0.46 | * | 25.00 | 11.62 |
| admiralty-scale:source-reliability="d" | 0.27 | * | 25.00 | 6.80 |

Adju

# Implementation in MISP: simulation tool




Simu

*Attributes* with different *Models*

# Implementation in MISP: API query body

/attributes/restSearch

```
{
    "includeDecayScore": 1,
    "includeFullModel": 0,
    "excludeDecayed": 0,
    "decayingModel": [85],
    "modelOverrides": {
        "threshold": 30
    }
    "score": 30,
}
```