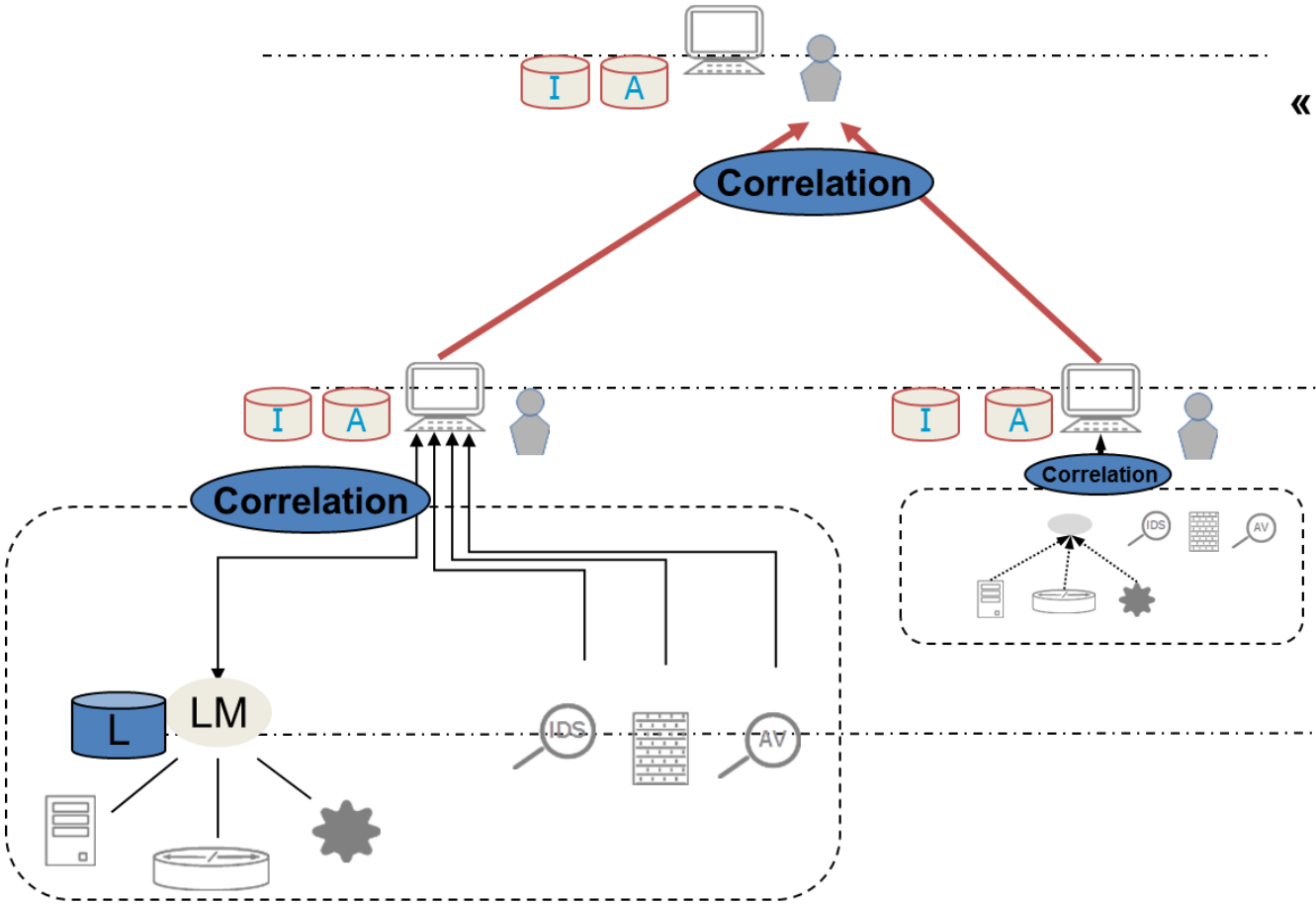
MODERNISATION DES FORMATS IDMEF ET IODEF

THOMAS ANDREJAK - CS

CS – Communication & Systèmes

IDMEF ET IODEF



SOC, CERT,
« SIEM de SIEM »

Incidents
Alertes
-
IODEF
IDMEF

SIEM

Alertes
-
IDMEF

Sondes

Traces
brutes
-
Formats
hétérogènes

IDMEF (RFC 4765) et IODEF (RFC 5070) recommandés par le RGI v2 !

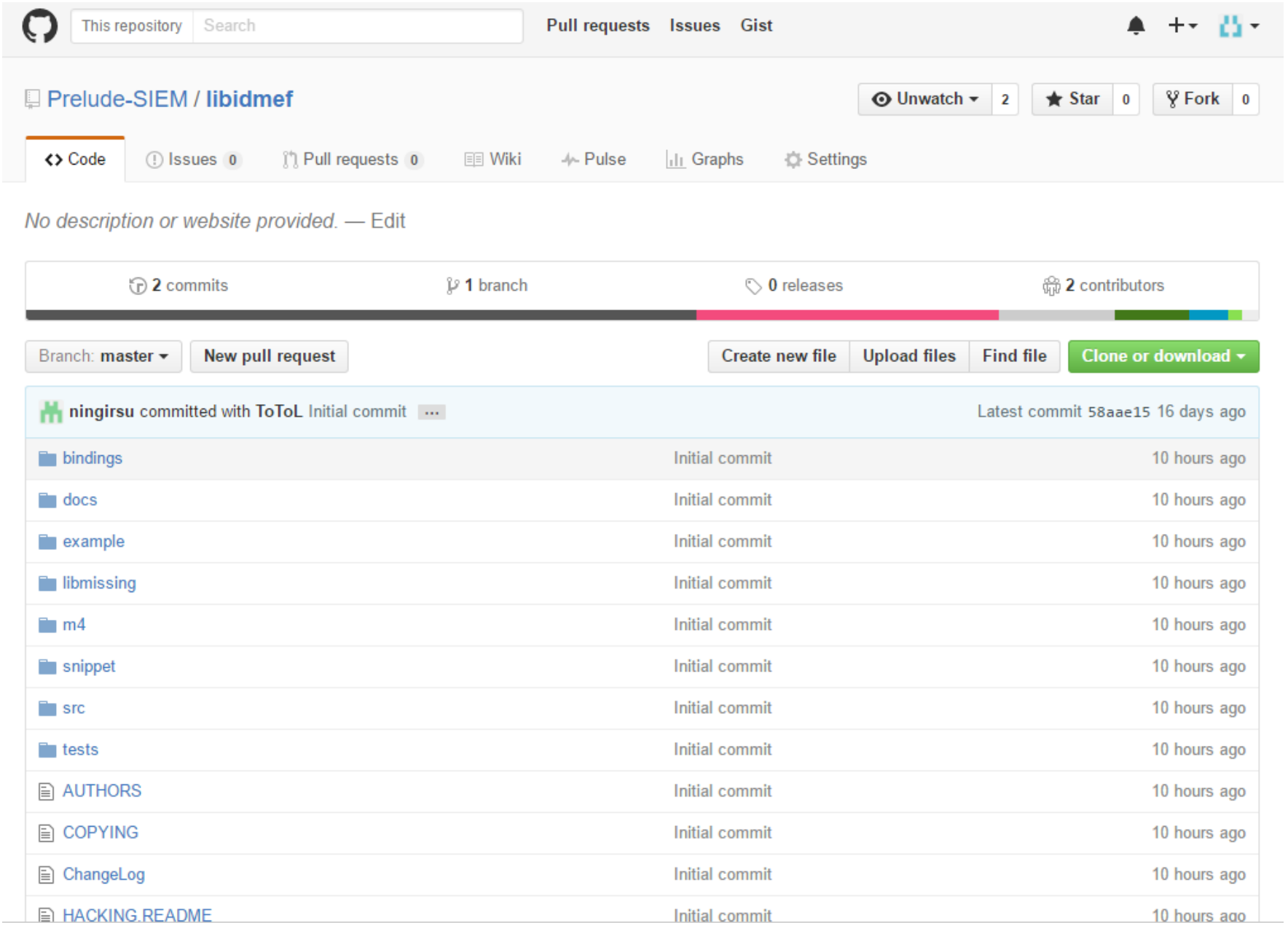
PLUSIEURS ACTEURS DANS LE CONSORTIUM

www.secef.net

MANIPULATION IDMEF ET IODEF

- Réalisation d'une LibIDMEF
  - Basée sur la libPrelude
  - https://github.com/Prelude-SIEM/libidmef
- Réalisation d'une LibIODEF
  - https://github.com/Prelude-SIEM/libiodef
- Licence GPLv2

LIBIDMEF


This repository
Search
Pull requests
Issues
Gist
Prelude-SIEM / libidmef
Unwatch 2
Star 0
Fork 0
Code
Issues 0
Pull requests 0
Wiki
Pulse
Graphs
Settings
No description or website provided. — Edit
2 commits
1 branch
0 releases
2 contributors
Branch: master
New pull request
Create new file
Upload files
Find file
Clone or download
ningirsu committed with ToToL Initial commit
Latest commit 58aae15 16 days ago
bindings Initial commit 10 hours ago
docs Initial commit 10 hours ago
example Initial commit 10 hours ago
libmissing Initial commit 10 hours ago
m4 Initial commit 10 hours ago
snippet Initial commit 10 hours ago
src Initial commit 10 hours ago
tests Initial commit 10 hours ago
AUTHORS Initial commit 10 hours ago
COPYING Initial commit 10 hours ago
ChangeLog Initial commit 10 hours ago
HACKING.README Initial commit 10 hours ago

LIBIDMEF : PRINT EXEMPLE

```
import idmef
import json

msg = idmef.IDMEF()

msg.set("alert.classification.text", "Scan port detected")
msg.set("alert.source(0).node.address(0).address", "213.56.166.109")
msg.set("alert.assessment.impact.severity", "medium")
msg.set("alert.assessment.impact.description", "Someone tries to connect to a computer using too many ports")
msg.set("alert.target(0).service.portlist", "23,45,64,90,443,1194,2452,5832,5911,7530")
msg.set("alert.target(0).node.address(0).address", "192.168.45.21")

print("Pretty print !")
print("==============")
print(msg)

print("JSON print !")
print("==============")
print(json.dumps(json.loads(msg.toJSON()),indent=4))

print("Binary print !")
print("==============")
print(msg.toBinary())
```

LIBIDMEF : PRETTY PRINT

```
Pretty print !
==============
version: <empty>
alert:
        create_time: 29/05/2016 11:27:27.18541 +02:00
        classification:
                text: Scan port detected
        source(0):
                spoofed: unknown (0)
                node:
                        category: unknown (0)
                        address(0):
                                category: unknown (0)
                                address: 213.56.166.109
        target(0):
                decoy: unknown (0)
                node:
                        category: unknown (0)
                        address(0):
                                category: unknown (0)
                                address: 192.168.45.21
                service:
                        portlist: 23,45,64,90,443,1194,2452,5832,5911,7530
        assessment:
                impact:
                        severity: medium (3)
                        type: other (0)
                        description: Someone tries to connect to a computer using too many ports
```

LIBIDMEF : JSON PRINT

JSON print !

==========


```
{
    "_self": "idmef_message_t",
    "version": "",
    "alert": {
        "_self": "idmef_alert_t",
        "target": [
            {
                "_self": "idmef_target_t",
                "decoy": "unknown",
                "node": {
                    "_self": "idmef_node_t",
                    "category": "unknown",
                    "address": [
                        {
                            "_self": "idmef_address_t",
                            "category": "unknown",
                            "address": "192.168.45.21"
                        }
                    ]
                },
                "service": {
                    "_self": "idmef_service_t",
                    "portlist": "23,45,64,90,443,1194,2452,5832,5911,7530"
                }
            }
        ],
        "classification": {
            "_self": "idmef_classification_t",
            "text": "Scan port detected"
        },
        "source": [
            {
                "_self": "idmef_source_t",
                "node": {
                    "_self": "idmef_node_t",
                    "category": "unknown",
                    "address": [
                        {
                            "_self": "idmef_address_t",
                            "category": "unknown",
                            "address": "213.56.166.109"
                        }
                    ]
                },
                "spoofed": "unknown"
            }
        ],
        "create_time": "2016-05-29T11:27:27.18541+02:00",
        "assessment": {
            "_self": "idmef_assessment_t",
            "impact": {
                "_self": "idmef_impact_t",
                "type": "other",
                "severity": "medium",
                "description": "Someone tries to connect to a computer using too many ports"
            }
        }
    }
}
```

LIBIDMEF : BINARY PRINT

Binary print !

==========

WJ��Hm Scan port detected�

!213.56.166.109���

!192.168.45.21�� #)23,45,64,90,443,1194,2452,5832,5911,7530�� <Someone tries to connect to a computer using too many ports����

LIBIDMEF : LOAD EXEMPLE

```
import idmef
import json

msg = {
    "_self": "idmef_message_t",
    "version": "",
    "alert": {
        "_self": "idmef_alert_t",
        "target": [
            {
                "_self": "idmef_target_t",
                "decoy": "unknown",
                "node": {
                    "_self": "idmef_node_t",
                    "category": "unknown",
                    "address": [
                        {
                            "_self": "idmef_address_t",
                            "category": "unknown",
                            "address": "192.168.45.21"
                        }
                    ]
                },
                "service": {
                    "_self": "idmef_service_t",
                    "portlist":
"23,45,64,90,443,1194,2452,5832,5911,7530"
                }
            }
        ],
        "classification": {
            "_self": "idmef_classification_t",
            "text": "Scan port detected"
        },
    }
}

msg_idmef = idmef.IDMEF(json.dumps(msg))

print("Pretty print !")
print("==============")
print(msg_idmef)
```

LIBIDMEF : PRETTY PRINT

```
Pretty print !
==============
version: <empty>
alert:
        create_time: 29/05/2016 12:10:30.656469 +02:00
        classification:
                text: Scan port detected
        target(0):
                decoy: unknown (0)
                node:
                        category: unknown (0)
                        address(0):
                                category: unknown (0)
                                address: 192.168.45.21
                service:
                        portlist: 23,45,64,90,443,1194,2452,5832,5911,7530
```

LIBIODEF

Même principe que LIBIDMEF !

- Un Schéma provenant de la RFC
- Un « IODEF Path »
- Les fonctions de load() et dump()

LIBIDMEF ET LIBIODEF

- Basé sur la libPrelude
- Code source en C
- Licence GPLv2
- Bindings C++ et Python

https://github.com/Prelude-SIEM/libidmef

https://github.com/Prelude-SIEM/libiodef

- Prochaine version des libs implémentant IDMEFv2 pour le SECEF Day (septembre)
  - Pré-version du schéma (textes et images) disponible sur http://www.secef.net/idmef_parser/

LIBIDMEF ET LIBIODEF

- SIEMs implémentant nativement IDMEF et IODEF
  - Prelude OSS
- Sonde implémentant nativement IDMEF
  - Suricata
  - Barnyard2 (Snort)
  - OSSEC
  - Auditd
  - Nepenthes
  - Samhain
  - Sancp
  - Orchids
- Sonde en cours d'intégration d'IDMEF
  - ClamAV
  - Squid
  - SpamAssassin
  - Mod_security
  - CrawlProtect
  - NFSen
  - Kismet

Merci !

https://github.com/Prelude-SIEM/libidmef

https://github.com/Prelude-SIEM/libiodef