Prelude Universal SIM

State of the Art

Yoann Vandoorselaere <yoann.v@prelude-ids.com>

> Prelude Universal SIM > Introduction

> *Definition :*

- The Prelude Universal SIM (Security Information Management) system is interoperable with every systems on the market.
- **Prelude collects, normalizes, sorts, aggregates, correlates and reports** all security-related events to the security analyst**.**

> *Prelude :*

- Prelude interoperate with HIDS (Host-based IDS) as well as NIDS (Network-based IDS) by using the **IDMEF standard**.
- IDMEF is an international standard created upon the initiative of IETF along with the participation of Prelude teams to enable interacting with the various security tools.

> *Prelude Characteristics*

- **Can interoperate with all security systems** independantly from the number of components, their brand or their license.
- **Real-time Correlation** of security events.
- **Real-time Visualization** of security events, and attack scenario using a centralized console.
- **Secured architecture:** ssl, can handle DMZ restricted policy, redondancy...
- **Flexible Architecture:** distributed solution that offers unlimited evolution capability

Prelude is a Universal SIM system, it is composed of multiples modular elements distributed on the whole infrastructure.

> *System components*

- **The Concentrator, *Prelude Manager*:** high availability server that receives events coming from deployed sensors.
- **Prelude library, *libprelude*:** provides necessary features enabling events injection in the Prelude infrastructure.
- **The PreludeDB library, *libpreludedb*:** Transparent database access.
- **The Prelude interface, *Prewikka*:** Visualization interface.
- **The correlation engine, *Prelude Correlator*:** Multistream Correlation by virtue of the powerful programming language Lua.
- **The logs analyzer, *Prelude LML*:** Logs collection and normalisation.

> Prelude Universal SIM > Supported Systems

> *Native compatibility:*

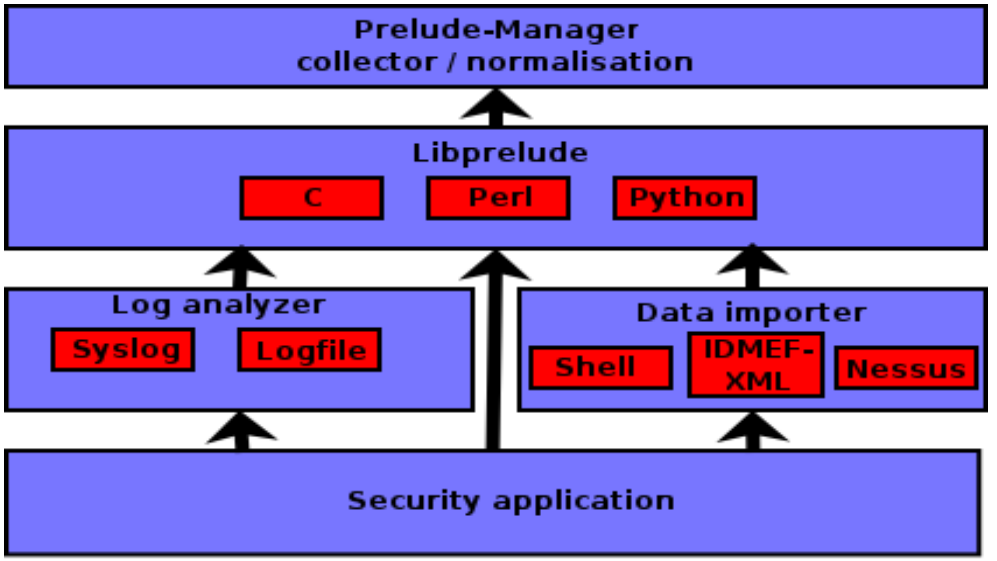
AuditD (handles records generated by the audit subsystem in the Linux 2.6 kernel), Nepenthes (collect malwares), NuFW (Identity access management solution, at the network level), OSSEC, PAM, Prelude-PFLogger (handles OpenBSD firewall alerts), Sancp (collects information regarding network traffic), Samhain, Snort.

> *Logs compatibility:*

Apache, Arbor, ArpWatch, Asterisk, APC-EMU, BIG-IP, Cacti, Checkpoint, CISCO ASA, CISCO CSS, CISCO IOS, CISCO IPS, CISCO Router, CISCO VPN, ClamAV, Dell OpenManage, D-Link, Exim, GrSecurity, Honeyd, Honeytrap, Ipchains, IpFw, Juniper Networks NetScreen, Kojoney, Libsafe, Linux bonding, Linux-PAM, Linksys WAP11, Microsoft Cluster Service, Microsoft SQL Server, ModSecurity, Nagios, NetApp ONTAP, Netfilter, NTSyslog, OpenHostAPD, OpenSSH, Oracle, PaX, P3Scan, Portsentry, Postfix, ProFTPD, Qpopper, Rishi, SELinux, Sendmail, Shadow, Shadow Utils, Squid, SonicGuard SonicWall, SpamAssassin, Squid, Sudo, Suhosin, Symantec Norton Antivirus, Symantec pcAnywhere, Tripwire, Unix specific logs, Vpopmail, WU-FTPD, Webmin, Windows Server...

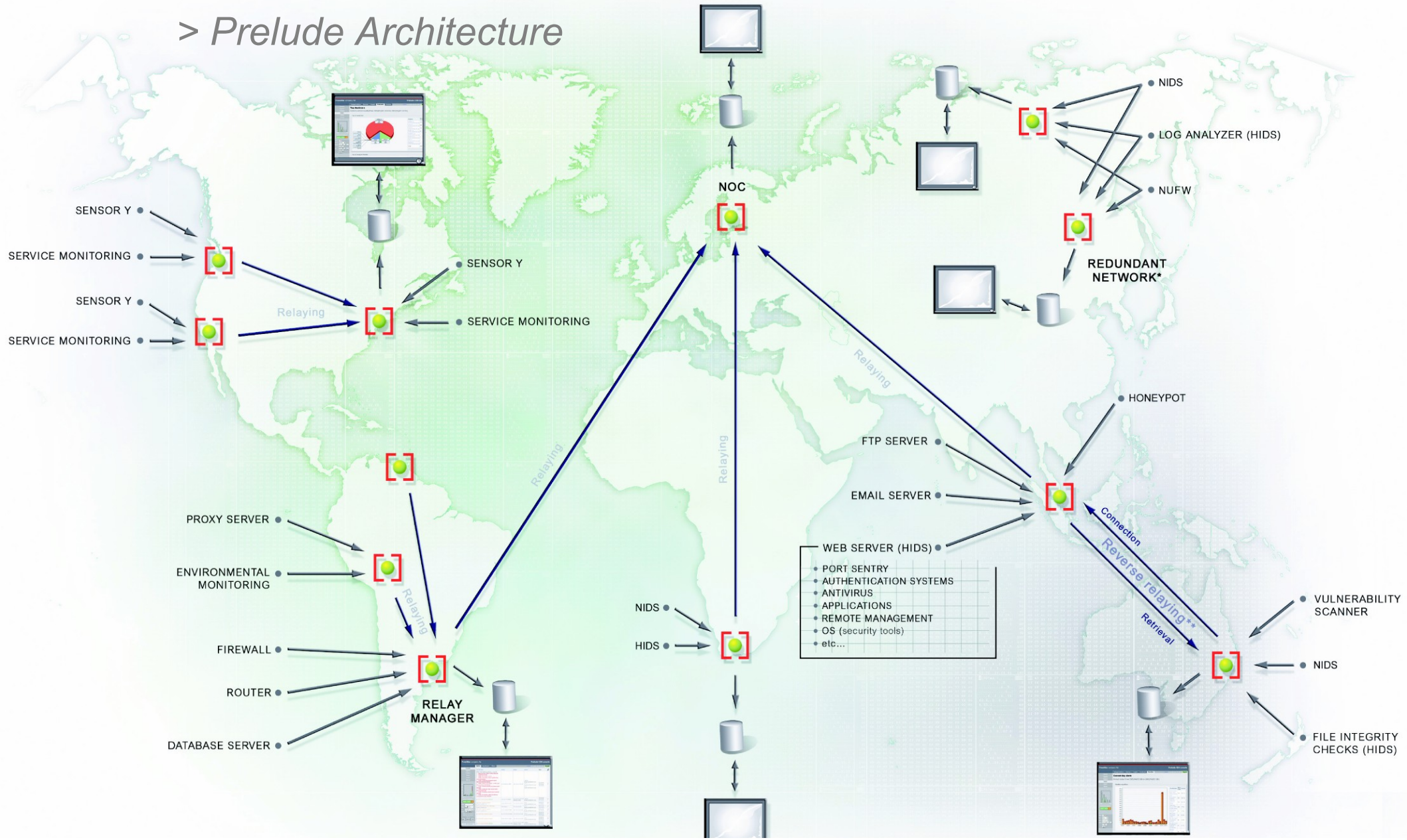
> Compatibility options:

- **Native:** libPrelude (C) ; Support C++, Perl, Python, Ruby, Lua
- **Prelude-LML:** Logs (system logs, syslog, flat files, etc.)



> Prelude Universal SIM > Architecture

> *Prelude Architecture*

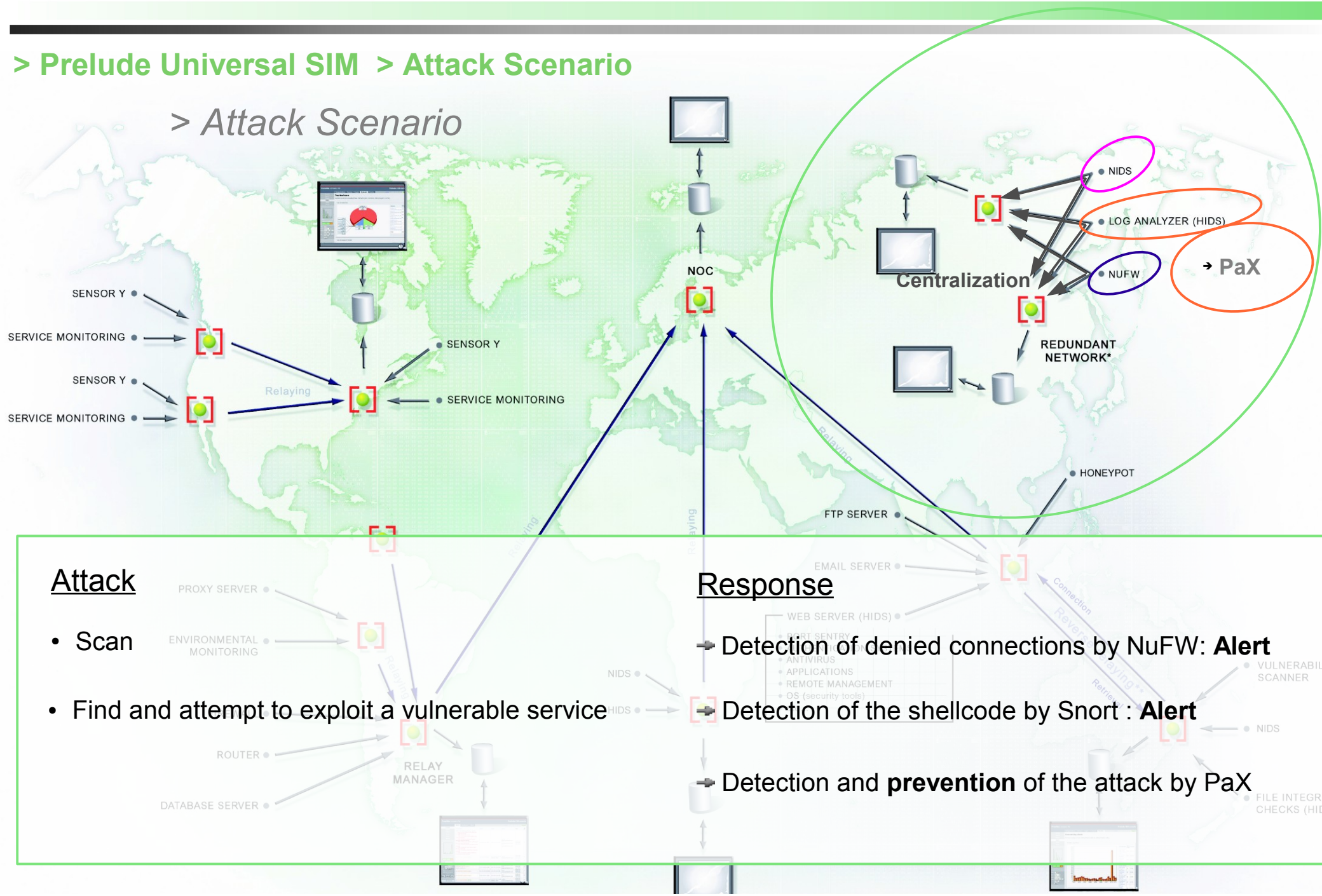


SENSOR X: made Prelude-compatible upon customer's request
SENSOR Y: developed by the customer

MANAGER PRELUDE (concentrator)
PREWIKKA GUI
DATABASE
secured connection (SSL) between every modules

> Prelude Universal SIM > Attack Scenario

> Attack Scenario



Attack

- Scan
- Find and attempt to exploit a vulnerable service

Response

- Detection of denied connections by NuFW: **Alert**
- Detection of the shellcode by Snort : **Alert**
- Detection and **prevention** of the attack by PaX

SENSOR X: made Prelude-compatible upon customer's request
SENSOR Y: developed by the customer

MANAGER PRELUDE (concentrator)
PREWIKKA GUI
DATABASE
secured connection (SSL) between every modules

> Prelude Universal SIM > Major improvements

> *New sensors*

- **Asterisk:** Open Source PBX & Telephony platform
- **Auditd:** Manage audits records generated by the Linux audit subsystem
- **Clamav (upcoming):** An open source anti-virus toolkit for UNIX
- **Honeytrap:** Honeypot collecting information regarding known/unknown network-based attack
- **Kojoney:** Honeypot that emulates an SSH server
- **Nagios V2:** Host/service monitor that inform you of network problems
- **OSSEC:** Log analysis, integrity checking, Windows registry monitoring, rootkit detection, real-time alerting and active response
- **Rishi:** Identify Bot Contaminated Hosts
- **Suhosin:** Advanced protection system for PHP installations

> Framework

- Easy bindings!
- Prelude-Admin (new prelude-adduser) can now list agents profile
- Major API improvements.
- RFC 4122 UUIDv1 identifier generation

> *Prelude Manager*

- **The Mail Reporting plugin is now open-source!**

  Can retrieve Correlated Alert from the database

- **Embed libev**

  Support select, poll, epoll, kqueue, event ports backends

- **Improved scheduler, and disk pool**

  Delayed heartbeat timer, unfairness with certain flows, journal file.

- **Thresholding plugin**

  Can suppress repetitive events

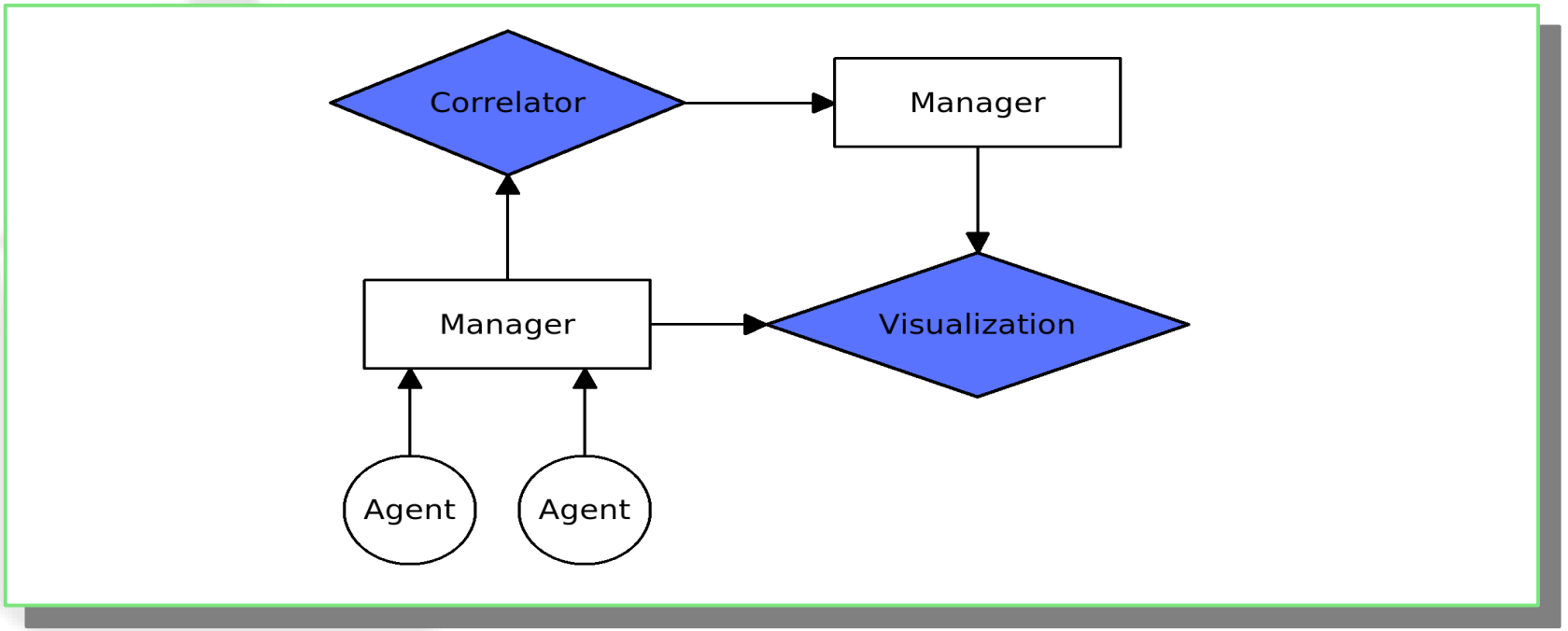
> Prelude Universal SIM > Major improvements

> *Prewikka*

- Asynchronous DNS resolution
- Events auto-refresh system
- Translations (Brazilian Portuguese, French, German, Polish, Russian, Spanish)
- Use jquery for Javascript + advanced effects
- New agent view: Overview of the agents situation at first glance

> *Prelude Correlator*

- Initial beta version released!
- Fetch events from Prelude-Manager
- Rules writing is done using the ***Lua*** programming language



> Prelude Correlator – Rule example

> Rule example (1/3) – Fetch data of interest

```
local is_failed_auth = INPUT:match("alert.classification.text", "[Ll]ogin|[Aa]uthentication",
                                   "alert.assessment.impact.completion", "failed")

local result = INPUT:match("alert.source(*).node.address(*).address", "(.+)",
                           "alert.target(*).node.address(*).address", "(.+)");
```

> Prelude Correlator – Rule example

> Rule example (2/3) – Keep interesting data

```
if is_failed_auth and result then
    for i, source in ipairs(result[1]) do
        for i, target in ipairs(result[2]) do

            local ctx = Context.update("BRUTE_ST_" .. source .. target, { expire = 2, threshold = 5 })
            ctx:set("alert.source(>>)", INPUT:getraw("alert.source"))
            ctx:set("alert.target(>>)", INPUT:getraw("alert.target"))
            ctx:set("alert.correlation_alert.alertident(>>).alertident", INPUT:getraw("alert.messageid"))
            ctx:set("alert.correlation_alert.alertident(-1).analyzerid", INPUT:getAnalyzerid())
```

> Prelude Correlator – Rule example

> Rule example (3/3) – Emit Correlation Alert

```
        if ctx:CheckAndDecThreshold() then
            ctx:set("alert.classification.text", "Brute force attack")
            ctx:set("alert.correlation_alert.name", "Multiple failed login")
            ctx:set("alert.assessment.impact.severity", "high")
            ctx:set("alert.assessment.impact.description",
                    "Multiple failed attempts have been made to login to a user account")
            ctx:alert()
            ctx:del()
        end
    end
  end
end
```

➔ You get the big picture
➔ Improved safety, circumvention made harder
➔ Unlimited adaptability

... The Prelude Universal SIM will get you the higher level of protection on your infrastructure.

> Futur... Development :

- Advanced event categorization
- Advanced Correlation method
- Prelude 1.0 ...

> *Links*

- **Prelude Project:** http://www.prelude-ids.com/development/
- **PreludeIDS Technologies SARL:** http://www.prelude-ids.com

Auditd:	http://people.redhat.com/sgrubb/audit/
IDMEF:	http://www.rfc-editor.org/rfc/rfc4765.txt
Nepenthes:	http://www.mwcollect.org
Nessus:	http://www.nessus.org
NuFW:	http://www.nufw.org/
OSSEC:	http://www.ossec.net/
Samhain:	http://la-samhna.de/samhain/
Sancp:	http://www.metre.net/sancp.html
Snort:	http://www.snort.org

Thank you for your attention