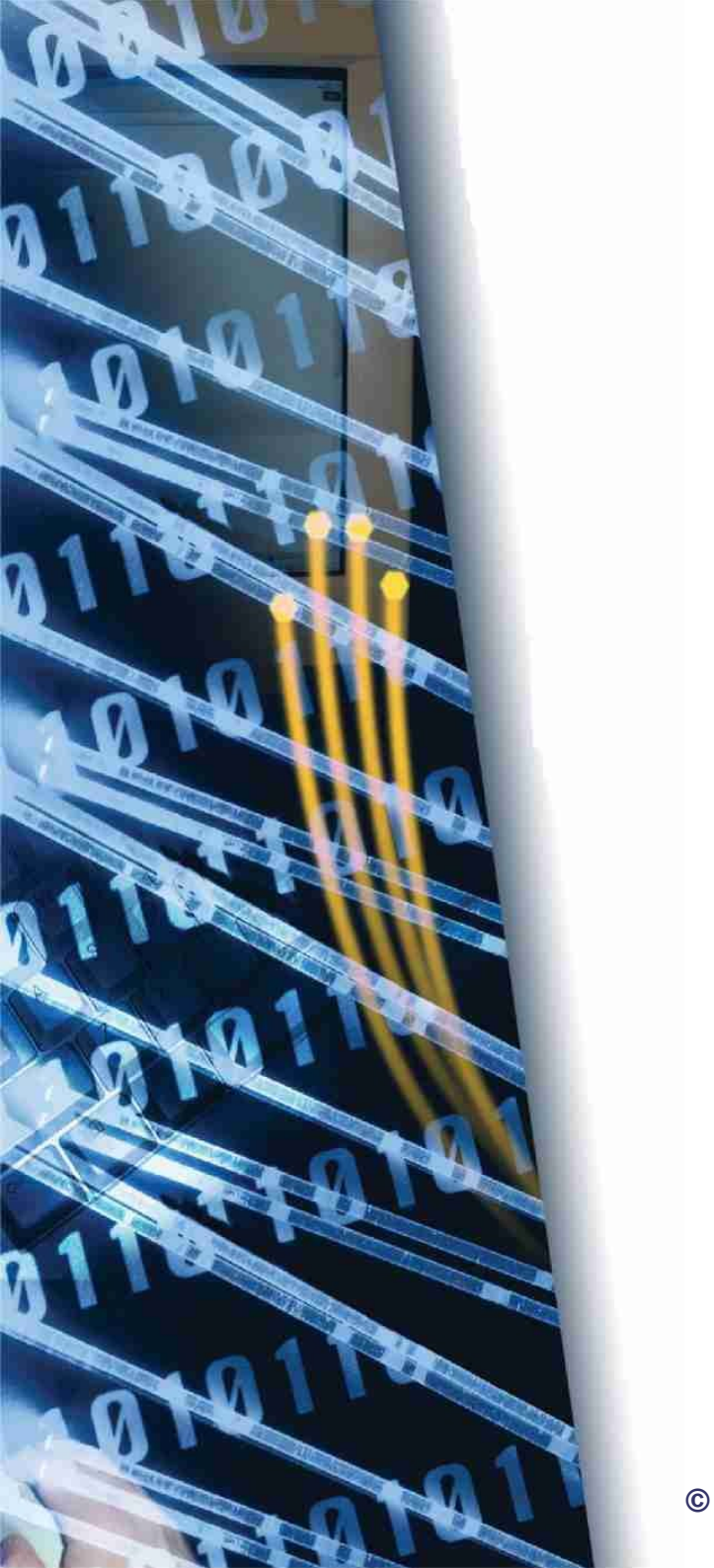


Proactive Security Monitoring in a Policy Managed Network

Till Dörges

Klaus-Peter Kossakowski

PRESECURE® Consulting GmbH

Outline / ToC

- Outline / ToC
- Motivation
- POSITIF: Overview
- POSITIF: Description Languages
- PSM: Black Box
- PSM: Detailed View
- Outlook

PRESECURE® Consulting GmbH

POSITIF – Motivation

- **complexity of networks ever increasing**
- **individual administration of components impossible**
- **potential solution: Policy Based Management**
- **POSITIF**
  - Policy based Security Tools and Framework
  - EC funded project
  - provides tools and framework
  - aims at high level policies

PRESECURE® Consulting GmbH

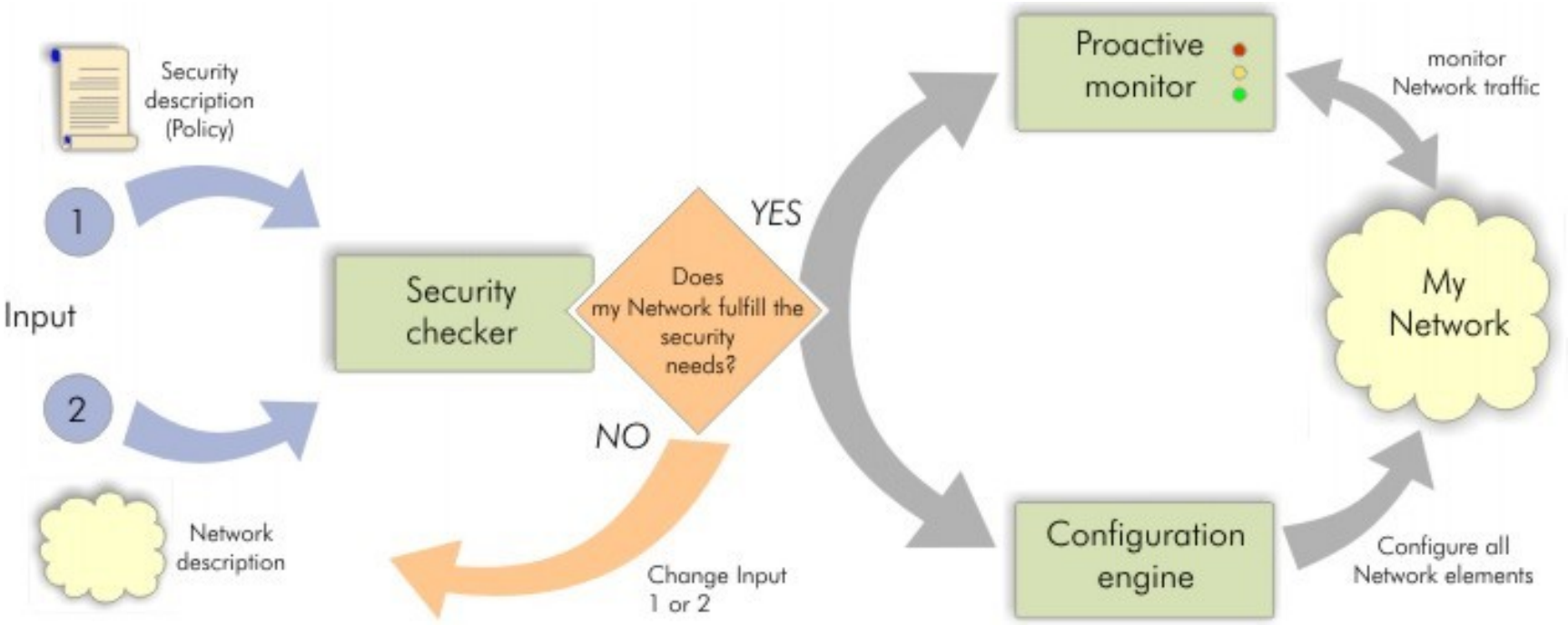
Outline / ToC

- Outline / ToC
- Motivation
- POSITIF: Overview
- POSITIF: Description Languages
- PSM: Black Box
- PSM: Detailed View
- Outlook

PRESECURE® Consulting GmbH

POSITIF – Framework (1)

■ schematic overview



PRESECURE® Consulting GmbH

POSITIF – Framework (2)

- **key elements**
  - tools for administrators
- **description**
  - System Description Language (SDL)
  - Security Policy Language (SPL)
- **automatic deployment of**
  - policies
  - (configurations)
- **specifying a policy pointless without monitoring**

PRESECURE® Consulting GmbH

Outline / ToC

- Outline / ToC
- Motivation
- POSITIF: Overview
- POSITIF: Description Languages
- PSM: Black Box
- PSM: Detailed View
- Outlook

PRESECURE® Consulting GmbH

Description Languages

- **XML based**
- **high level versions for administrators describing the network**
- **low level versions for actual reasoning and automatic processing**
  - basically contain more details
  - set as defaults

PRESECURE® Consulting GmbH

SDL example

- (partial) description of a firewall

```
<firewall id="Firewall">
  <interface id="eth0" number="1" connector="RJ45"
   technology="Ethernet" protocol="10-100BaseT">
    <addr type="ipv4"
     netmask="255.255.255.128">1.2.3.4</addr>
  </interface>
  <interface id="eth1" number="2" technology="Ethernet"
   connector="RJ45" protocol="10-100BaseT">
    <addr type="ipv4"
     netmask="255.255.255.240">1.2.3.5</addr>
  </interface>
</firewall>
```


PRESECURE® Consulting GmbH

SPL example

- (partial) description of filtering rule

```
<xCIM_FilterEntry>
  <CIM_FilterEntryBase.Name>access1
  </CIM_FilterEntryBase.Name>
  <IsNegated>false</IsNegated>
  <TrafficType>IPv4</TrafficType>
  <MatchConditionType>Source Address and Mask
  </MatchConditionType>
  <MatchConditionValue>1.2.3.4/255.255.255.255
  </MatchConditionValue>
  <Action>Permit</Action>
  <DefaultFilter>false</DefaultFilter>
</xCIM_FilterEntry>
```


PRESECURE® Consulting GmbH

Outline / ToC

- Outline / ToC
- Motivation
- POSITIF: Overview
- POSITIF: Description Languages
- PSM: Black Box
- PSM: Detailed View
- Outlook

PRESECURE® Consulting GmbH

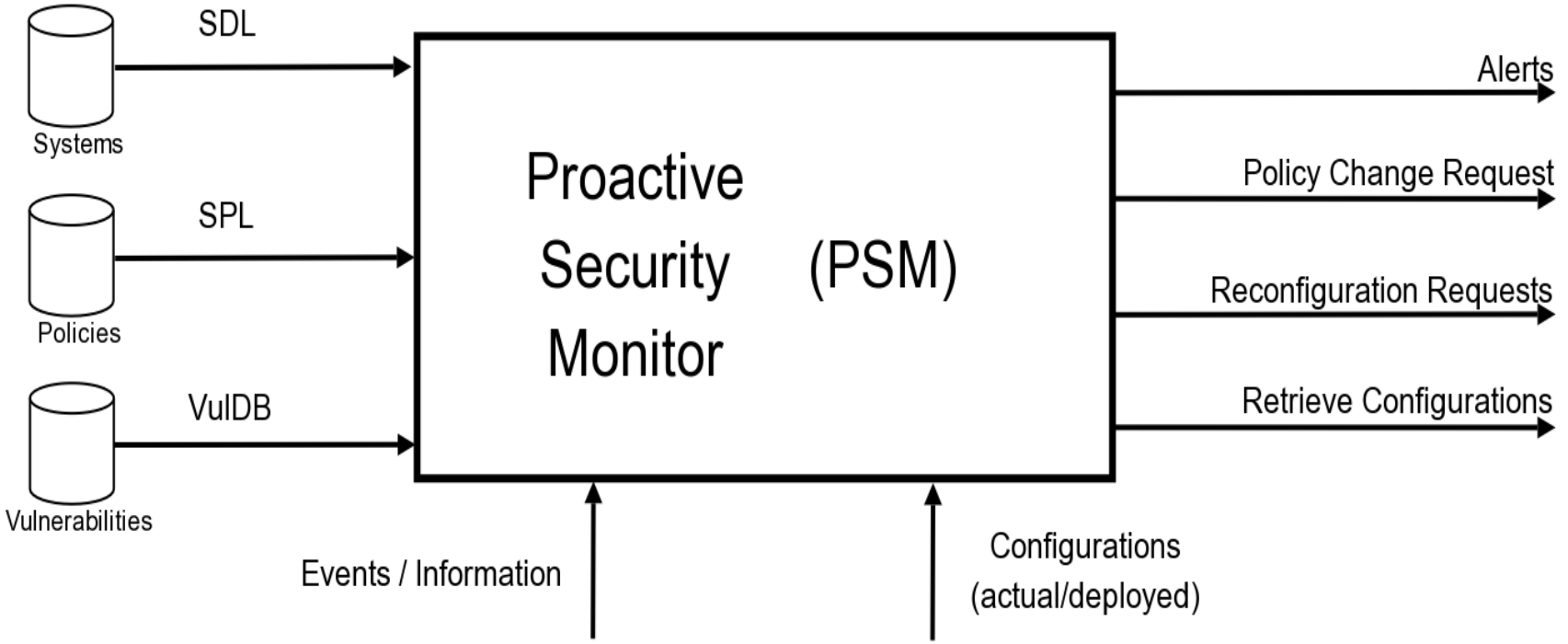
Proactive Security Monitor – Overview

- **monitors administrative domain for**
  - policy violations
  - attacks (slightly different from policy violations)
- **highly distributed component itself**
- **analyzes events, takes appropriate actions**
- **reactions can be (semi-) automatic**

PRESECURE® Consulting GmbH

Proactive Security Monitor – Blackbox

- PSM as a black box



[PRESECURE / V 2.0]

PRESECURE Consulting GmbH

Proactive Security Monitor – Blackbox

- SDL: description of the systems to be checked
- SPL: description of the policies
- events: all information processed by the PSM
- configurations: to verify their integrity
- outputs
  - Alerts
  - Policy Change Requests
  - Reconfiguration Requests
  - Retrieve Configurations

PRESECURE® Consulting GmbH

Proactive Security Monitor – Msg Formats

- **use existing standards**
- **IDMEF**
  - report events
- **IODEF**
  - report incidents
  - aggregated information

PRESECURE® Consulting GmbH

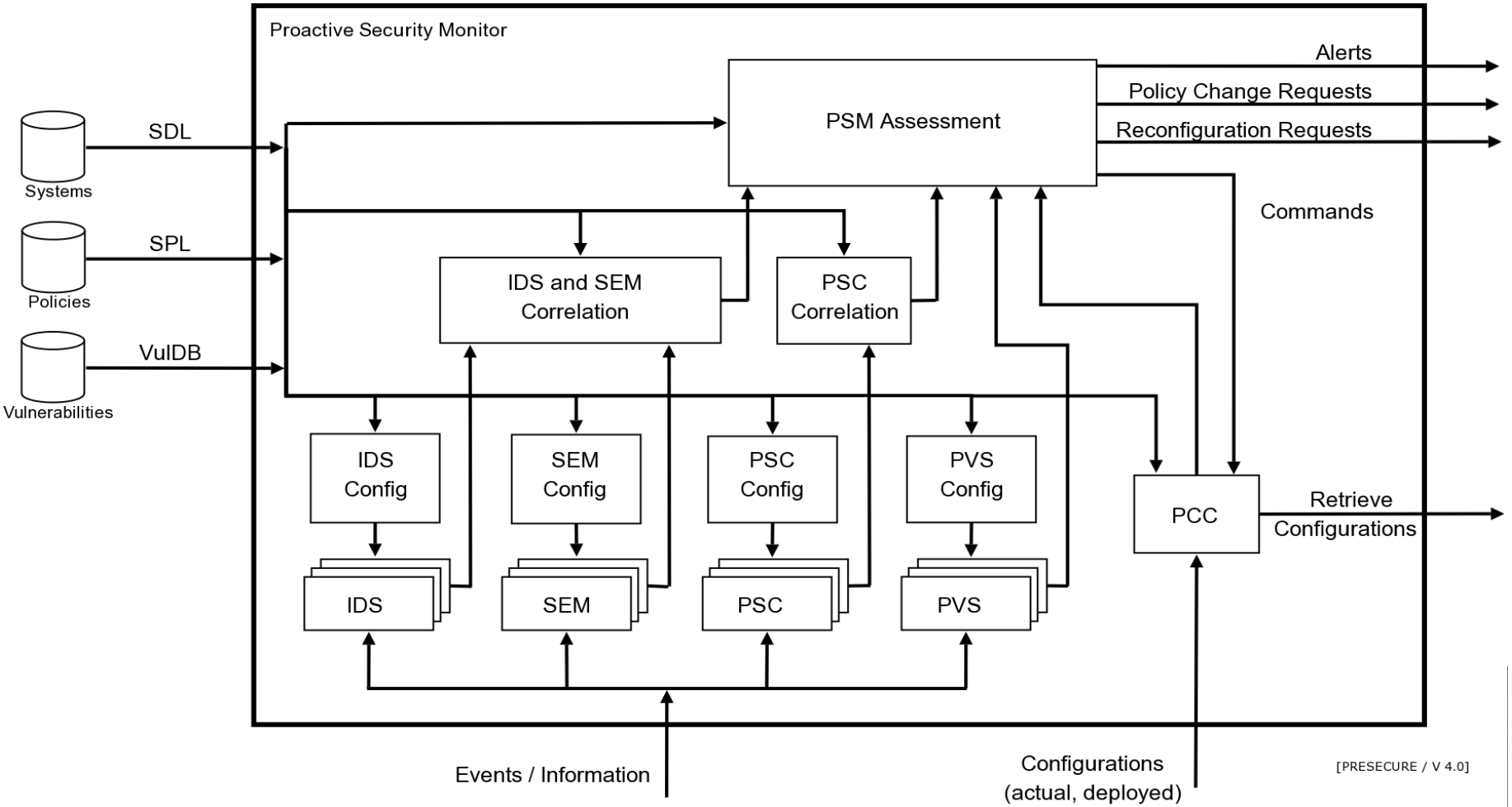
Outline / ToC

- Outline / ToC
- Motivation
- POSITIF: Overview
- POSITIF: Description Languages
- PSM: Black Box
- PSM: Detailed View
- Outlook

PRESECURE® Consulting GmbH

Proactive Security Monitor – Detailed View

internal components



Proactive Security Monitor – Detailed View

- **sensing components**
  - IDS/SEM Intrusion Detection Systems
  - Proactive Security Scanner
  - Policy Violation Sensor
  - Proactive Configuration Checker
- **correlation and assessment**
  - IDS and SEM Correlation
  - PSC Correlation
  - PSM Assessment

PRESECURE® Consulting GmbH

Sensing Components

- **Comparison of IDS/SEM, PSC, PVS, PCC**

	Behavior	Recognizes
IDS/SEM	*reactive*	Attacks / Policy Violations
PVS	*reactive*	Attacks / Policy Violations
PCC	*proactive*	Misconfigurations, Potential Attacks and Potential Policy Violations
PSC	*proactive*	Vulnerabilities, Potential Attacks and Potential Policy Violations

PRESECURE® Consulting GmbH

Sensing Components – Examples

Detection by Component

Incident	IDS/SEM	PVS	PCC	PSC
portscan	**yes**	no	no	no
cmd32.exe exploit	**yes**	**yes**	no	**yes**
reach. of forbidden serivce	**yes**	**yes**	**yes**	**yes**
denial of allowed service	no	**yes**	**yes**	**yes**
faulty configuration	no	no	**yes**	**yes**
write to forbidden dirs	**yes**	**yes**	**yes**	**yes**
forbidden attachments	no	**yes**	no	**yes**
succ. auth, wrong method	no	no	**yes**	**yes**
SSL conn., wrong certs	no	**yes**	no	**yes**
WWW down, no alert	no	no	no	**yes**

PRESECURE® Consulting GmbH

Outline / ToC

- Outline / ToC
- Motivation
- POSITIF: Overview
- POSITIF: Description Languages
- PSM: Black Box
- PSM: Detailed View
- Outlook

PRESECURE® Consulting GmbH

Outlook

- project is not finished yet
- first results look promising
- pretty complex task
  - real benefit only if everything is integrated
  - hindered by large abundance of proprietary procotols

PRESECURE® Consulting GmbH

Contact Information

- http://www.positif.org/

- Till Dörges
  PRE-CERT
  PRESECURE Consulting GmbH

  td@pre-secure-de

PRESECURE®
Consulting GmbH