



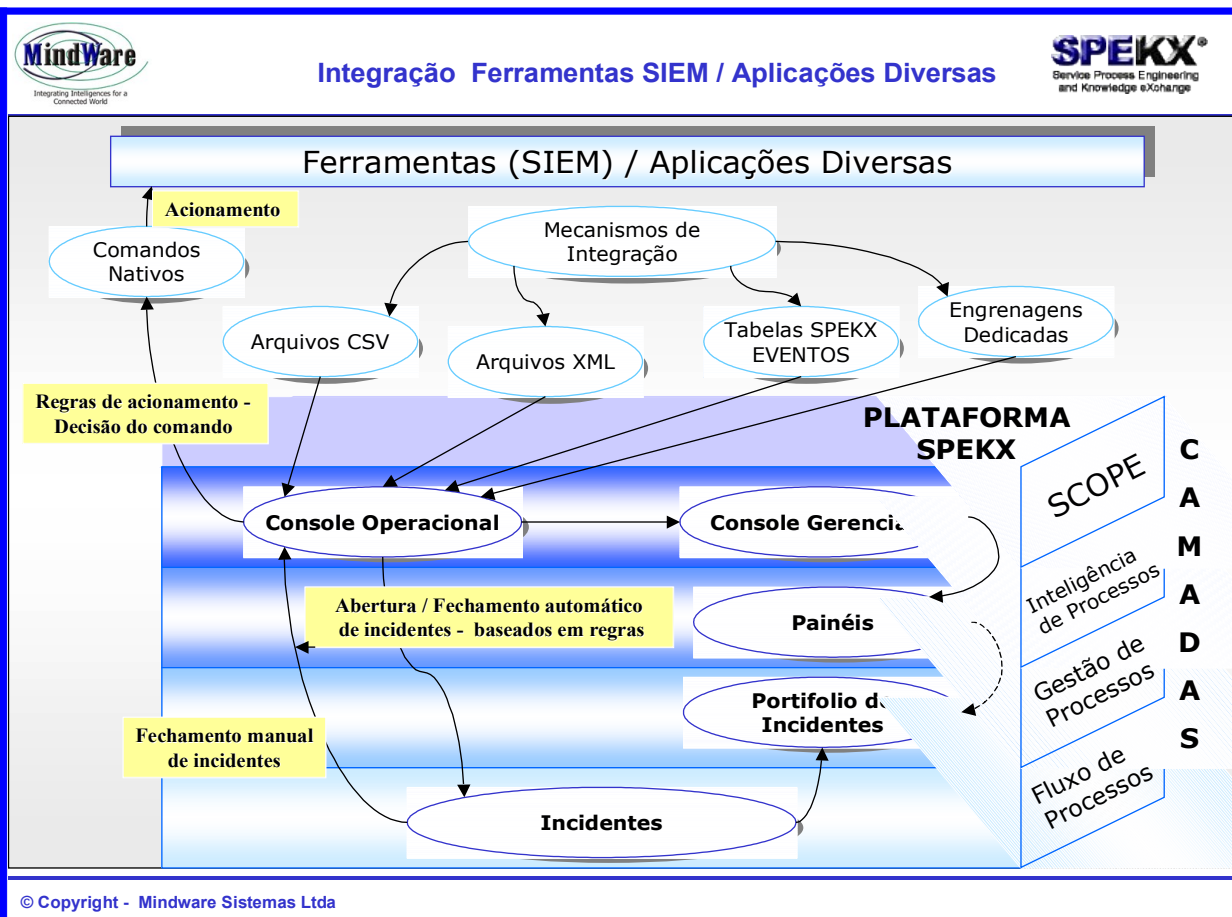
Resumo da Arquitetura de Integração

1. Objetivo

- Fornecer as diretrizes de integração das ferramentas (SIEM) e aplicações com a plataforma SPEKX utilizando a camada SCOPE (Spekx Connectivity and Open Protocol for Exchange) e demais camadas de inteligência, gestão e fluxo de processos.

2. Diagrama de Integração

- Abaixo apresentamos o diagrama de integração o qual apresenta os formatos de entradas e saídas suportados pela plataforma SPEKX.



3. Formatos de Entradas Suportados

Formato	Particularidades	Engrenagem SPEKX de Importação para as estruturas de eventos da Plataforma SPEKX
Arquivo CSV	Padrão CSV – Delimitados por ponto e virgula.	<ul style="list-style-type: none"> Mecanismos de import por JOB's assíncronos; Mecanismos de import síncronos através de visões de arquivo texto utilizando external tables.
Arquivo XML	Protocolo SPEKX.	<ul style="list-style-type: none"> Mecanismos de import por JOB's assíncronos.
Tabelas ORACLE – Camada de importação SPEKX	Estruturas de Dados SPEKX.	<ul style="list-style-type: none"> Mecanismos de gravação direta na plataforma SPEKX em estruturas de pré-eventos.
Específico	Não suportados pela plataforma SPEKX.	<ul style="list-style-type: none"> Mecanismos dedicados ou flexibilização dos mecanismos existentes para suportar as necessidades de import.

4. Layout de Entradas Padrão

4.1. Exemplo: Formato CSV



PERSPECTIVAS

Contexto aonde o Evento irá se enquadrar para armazenamento no repositório do SCOPE. As perspectivas iniciais são:

- DISPO – Disponibilidade;
- DESEM – Desempenho;
- CAPAC – Capacidade;
- SEGUR – Segurança;
- FUNCI – Funcionalidade.

Este campo é formado por 5 (cinco) posições.

ESTÍMULOS

Contexto de onde foram enviados os eventos para o SCOPE. Os estímulos iniciais são:

- NEGOCIO;
- SERVICO;
- APLICACAO;
- RECURSO.

Este campo é formado por 10 (dez) posições.

DADOS DO EVENTO

String com as informações específicas dos eventos com formato próprio para cada perspectiva informada. Cada informação deve ser separada por “;” (ponto e virgula). Detalhamento do incidente gerado depende de regras específicas, como por exemplo, o pacote de categorização. Ex: Criticidade: Alta.

EXEMPLOS DE EVENTOS PARA CADA PERSPECTIVA

Descrição	Exemplo de Valor
A – Perspectiva	DISPO
B – Estimulo	NEGOCIO; SERVICO
C – Ferramenta de Coleta	SPEKX; OPENV
D – Destino do Evento	INCIDENTE
E – Sequência de Identificação	12345
F – Item de Configuração (IC)	XPTO
G – Valor	DOWN; UP

Exemplo:
DISPO#SERVICO#SPEKX;INCIDENTE;2432;LABDIR;DOWN

SPEKX® © Copyright - MINDWARE Sistemas Ltda 3 18/12/2006

Descrição	Exemplo de Valor
A – Perspectiva	DESEM
B – Estimulo	NEGOCIO; SERVICO
C – Ferramenta de Coleta	SPEKX; OPENV
D – Destino do Evento	INCIDENTE
E – Sequência de Identificação	12345
F – Item de Configuração (IC)	XPTO
G – Camada	UNIX; WINDOWS; REDE
H – Componente	CPU
I – Elemento	CPU; RUNQUEUE
J – Atributo	IDLE
K – Valor	10

Exemplo:
DESEM#SERVICO#SPEKX;INCIDENTE;2432;LABDIR;UNIX;CPU;CPU;IDLE;10

SPEKX® © Copyright - MINDWARE Sistemas Ltda 4 18/12/2006

Formato do Evento : Perspectiva - **CAPACIDADE**


Descrição	Exemplo de Valor
A – Perspectiva	CAPAC
B – Estimulo	NEGOCIO; SERVICO
C – Ferramenta de Coleta	SPEKX; OPENV
D – Destino do Evento	INCIDENTE
E – Sequência de Identificação	12345
F – Item de Configuração (IC)	XPTO
G – Camada	UNIX; WINDOWS; REDE
H – Componente	STORAGE
I – Elemento	DISK
J – Atributo	FREE
K – Valor	10

Exemplo:
CAPAC#SERVICO#SPEKX;INCIDENTE;2432;LABDIR;UNIX;STORAGE;DISK;FREE;10

Formato do Evento : Perspectiva - **SEGURANCA**

Descrição	Exemplo de Valor
A – Perspectiva	SEGUR
B – Estimulo	APLICACAO; RECURSO
C – Ferramenta de Coleta	SPEKX; OPENV
D – Destino do Evento	INCIDENTE
E – Sequência de Identificação	12345
F – Item de Configuração (IC)	XPTO
G – Camada	APLICACAO
H – Componente	ACESSO
I – Elemento	LOGIN
J – Atributo	REJEICAO
K – Valor	3


Exemplo:
SEGUR#APLICACAO#SPEKX;INCIDENTE;2432;LABDIR;APLICACAO;ACESSO;LOGIN;REJEICAO; 3



MindWare
Integrating Intelligence for a
Connected World

Formato do Evento :

Perspectiva - **FUNCIONALIDADE**



SPEKX®
Service Process Engineering
and Knowledge eXchange

Descrição	Exemplo de Valor
A – Perspectiva	FUNCI
B – Estimulo	APLICACAO
C – Ferramenta de Coleta	SPEKX
D – Destino do Evento	INCIDENTE
E – Seqüência de Identificação	12345
F – Item de Configuração (IC)	XPTO
G – Camada	SISTEMA
H – Componente	MODULO
I – Elemento	PROGRAMA
J – Atributo	TEMPO; ABORT
K – Valor	3
<p><u>Exemplo:</u> FUNCION#APLICACAO#SPEKX;INCIDENTE;2432;LABDIR;SISTEMA;MODULO;PROGRAMA;TEMPO; 600</p>	

SPEKX® © Copyright - MINDWARE Sistemas Ltda

7

18/12/2006

- Os demais formatos (XML e Tabelas SPEKX pré-eventos - ORACLE) obedecem a mesma estruturação do formato CSV, obviamente dentro das características demandadas pelos TAGS XML e colunas de tabelas ORACLE.

4. Formatos de Saída

- Os formatos de saída oriundos da plataforma SPEKX para acionamento das ferramentas de destino (geradoras de eventos e/ou ferramentas de integração) possuem a flexibilidade de se adequar como resultado de configurações de pacotes de dados e/ou strings de comandos inteligíveis por parte da ferramenta em questão.

Ex: Openview - Configura-se o seguinte comando para acionamento:

Acknowledge de Eventos

```
telnet <TARGET HOST> 5525 << EOFEOF > /dev/null 2> /dev/null
ACKN <MESSAGE ID>
EOFEOF
```

Annotate de Eventos

```
telnet <TARGET HOST> 5525 << EOFEOF > /dev/null 2> /dev/null
ANNOTATE <MESSAGE ID> <SPEKX REQUEST ID>
EOFEOF
```