DATA SYS

Datasys ELISA

Log management řízený Zabbixem

Lukáš Malý, DiS

IT konzultant bezpečnost a monitoring

maly@datasys.cz

Co je ELISA ?

- ELISA - Event Log Interception Storage and Analysis
- NÁSTROJ PRO SBĚR A VYHODNOCENÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ (§21 a §23 vyhlášky k ZoKB)

- Poskytuje sběr logů a událostí
  - Operační systémy – Windows, Linux
    - Systémové logy – eventlog, syslog
    - Sledování logů služeb např. DHCP, RADIUS, webové a aplikační servery
  - Síťové prvky – Přepínače, Routery, VPN, WiFi AP
    - syslog, SNMP Trap, Netflow
- Poskytuje nahlížení na zaznamenaná data
  - Podporuje přístupové role s autentizací vůči LDAP – Active Directory.

DATA SYS

Co je ELISA ?

- ELISA Portál
  - Úvodní rozcestník systému ELISA

Obecný popis ELISA – LM/SIEM

Svobodný software s podporou výrobce - Datasys s.r.o.

- Robustní noSQL databázové jádro
- Podpora standardních protokolů
- Nízké pořizovací i provozní náklady

Zachovává strukturu původních událostí

- Líbivé webové uživatelské rozhraní - Kibana
- Extrémní škálovatelnost a HA
- Vysoký výkon (až 5000 eps)

DATA SYS

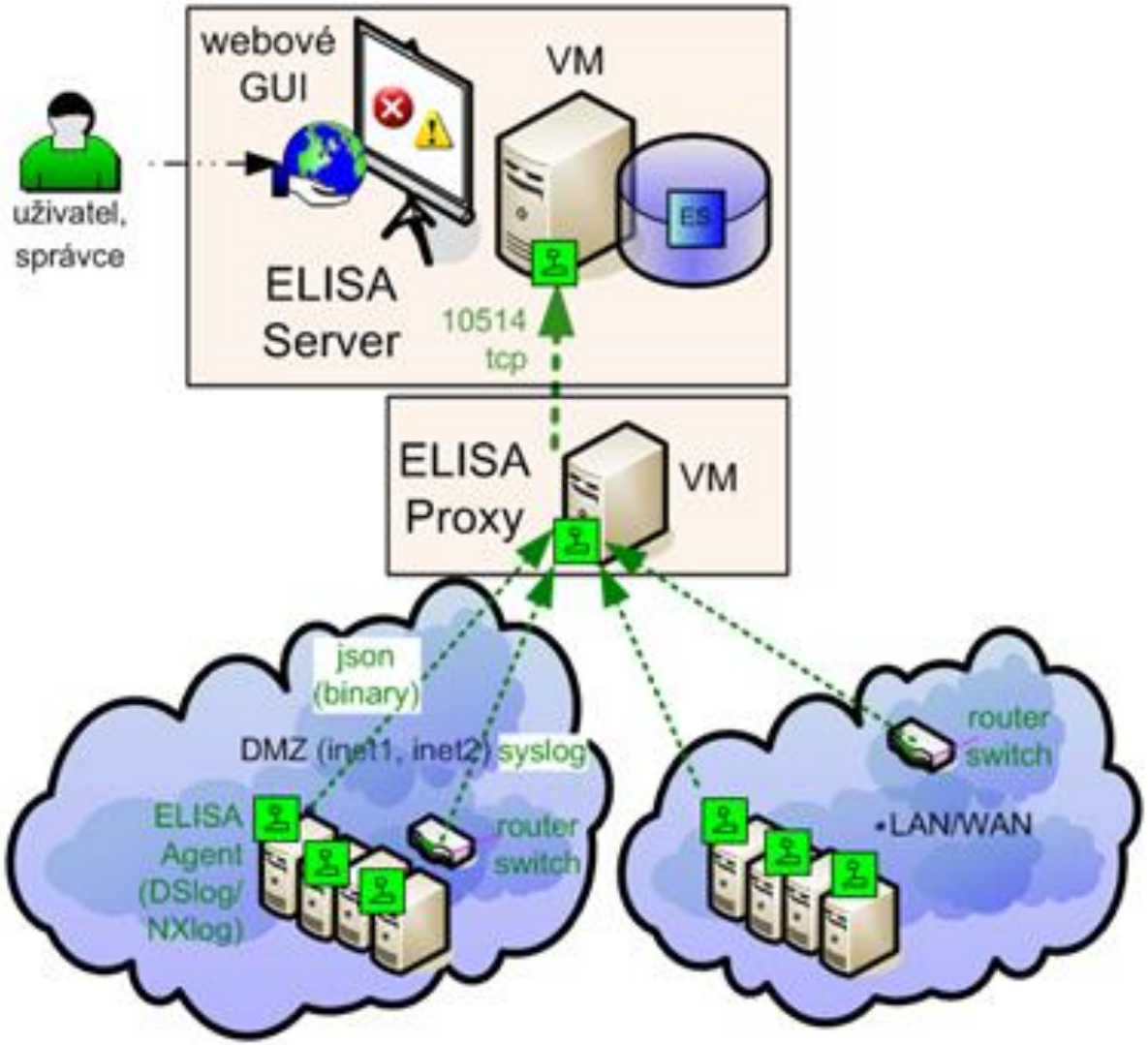
Open Source komponenty ELISA

LM/SIEM ELISA je postaven na komponentách, které díky propracované konfiguraci dílčích komponent tvoří funkční celek.

- Elasticsearch - slouží pro střednědobé nebo dlouhodobé ukládání dat (logů).
- Logstash - vstupní brána pro ukládání dat do Elasticsearch.
- NXlog a Dslog - multiplatformní agent, který zajišťuje sběr dat.
- Xlog - klíčová komponenta mechanismu centrální správy konfigurace agentů.
- Kibana – uživatelské rozhraní pro nahlížení na uložená data pomocí předdefinovaných dashboardů. Využívá webový server Apache.
- Zabbix - provozní monitorovací systém, který je integrován s ELISA.
- JasperReport - komponenta pro vytváření reportů.

DATA SYS

Architektura sběru dat



DATA SYS

Architektura sběru dat

- Elisa Server
  - Elasticsearch – úložiště dat
  - Kibana – nahlížení na data - logy
- Elisa Proxy
  - Server pro příjem logů, které předává do Elisa Server
  - Zpracovává přicházející zprávy dle konfigurace
  - Poskytuje instalace a autoregistrace NXLog a DSlog agentů
  - Poskytuje Zabbix API pro komponentu Xlog

DATA SYS

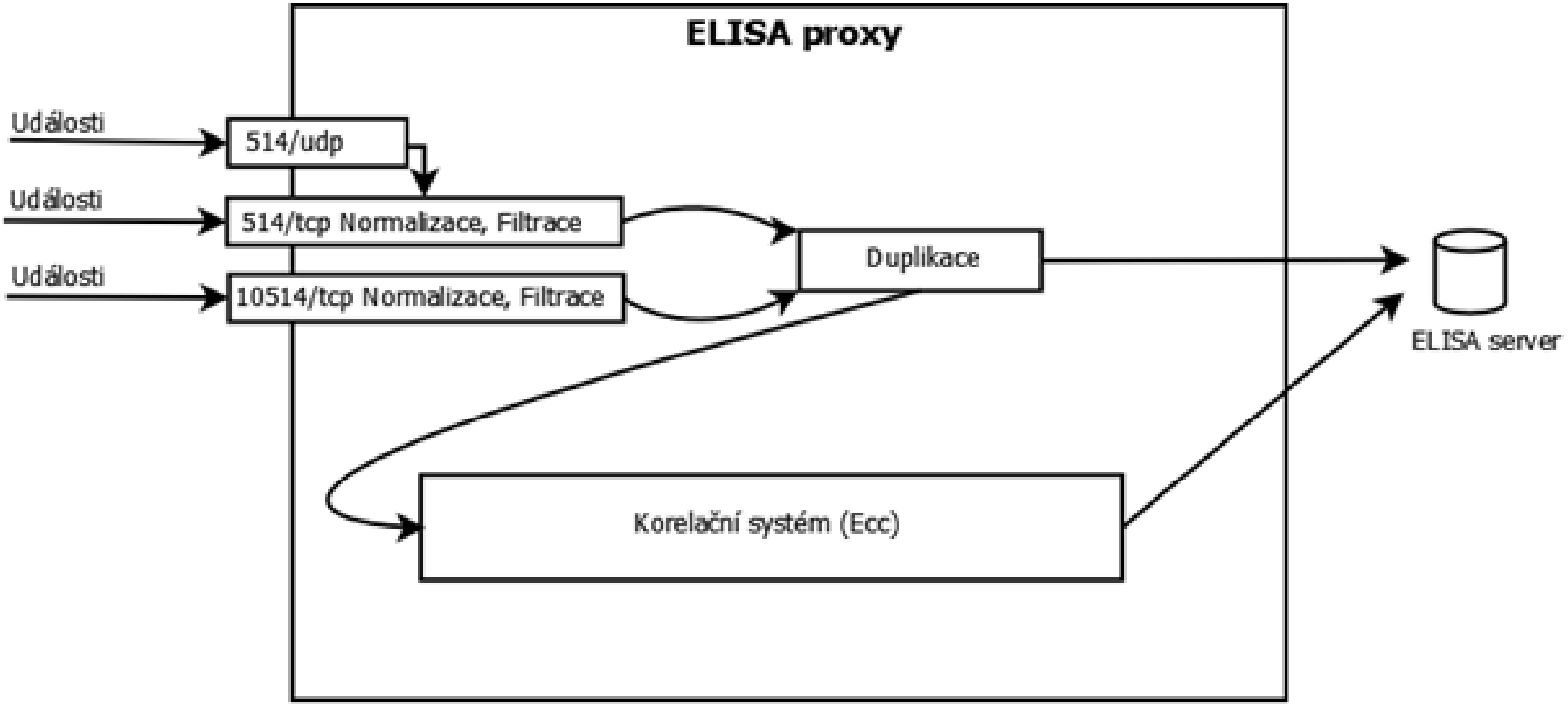
ELISA vstupní data

Hlavními vstupními kanály systému ELISA jsou:

- binární protokol pro přenos strukturovaných událostí
- syslog (udp i tcp) s možností SSL
  - BSD standard RFC 3164
  - IETF standard RFC 5424-5426
- SNMP trapy
  - snmptrapd (NET-SNMP)
- Netflow data
  - v9 a v5 (logstash plugin)

DATA SYS

ELISA vstupní data



Logstash & Elasticsearch

- Staví na projektu Apache Lucene
  - Nejrychlejší Open Source implementace fulltext vyhledávání
  - Disponuje velkou rychlostí vyhledávání
- Elasticsearch umožňuje instalaci velkého množství rozšíření
  - ELISA používá Elasticsearch + Elastic HQ Site Plugin
  - Plugin poskytuje statistické údaje o Elasticsearch
  - Poskytuje správu a údržbu indexů
- Ukládá data do indexů oddělených po jednotlivých dnech

Struktura datového záznamu v ELISA

- Normalizované atributy
  - @message – výstižný stručný popis události @msgHost – identifikace zařízení, na kterém událost vznikla (hostname, IP)
  - @msgSource – bližší identifikace zdroje, který událost vygeneroval
  - @msgSeverity – klasifikace závažnosti události dle pravidel zpracování
    DEBUG, INFO, NOTICE, WARNING, MAJOR, CRITICAL, FATAL
  - @msgUsername – identifikátor identity, se kterou je událost spojena
  - @timestamp – časová značka uložení události do datového úložiště ELISA

DATA SYS

Proč používat agenta ?

- Agent usnadňuje možnosti, jak se dostat k logům různých aplikací
- Umí převzít lokální syslog zprávy
- Používá modulární architekturu
- Je nenáročný na systémové zdroje, je psán v C++
- Poskytuje podporu pro různé formáty událostí
  - Syslog (BSD a IETF), CSV, JSON, XML, GELF, Windows EventLog
- Umí ukládat zprávy do bufferu a odeslat později
- Umí detekovat znakové sady
- Poskytuje bezpečnou komunikaci pomocí TLS/SSL

Agent NXlog a DSlog

- NXlog
  - Multiplatformní aplikace - Windows, Unix, Linux, BSD, Android
  - NXLog Community Edition
    - Volně dostupná verze klienta i v podobě src
  - NXLog Enterprise Edition
    - Placená verze, doplňkové funkce
- DSlog
  - Fork NXlog 2.5 s přidanými funkcemi (zejména „remote eventlog“)
  - Používán zejména pro instalace na Windows
    - ve formě bezobslužného instalačního MSI balíčku
    - před konfigurován pro konkrétní prostředí

Agentem podporované systémy

- NXlog podporuje množství operačních systémů
  - Windows 32bit, 64bit
  - CentOS / RHEL 32bit, 64bit
  - Debian / Ubuntu 32bit, 64bit

DATA SYS

Centrální správa agentů

Centrální správu tvoří tři komponenty

- NXlog a DSlog
  - Instalace agenta obsahuje konfiguraci, která se umí sama zaktualizovat.
- Xlog – aplikace v PHP využívající Zabbix API
  - Sestavuje konfiguraci pro jednotlivé agenty.
- Zabbix – monitorovací systém
  - Vytváření a přiřazovaní konfigurace pomocí šablon.

DATA SYS

Princip centrální správy

- Po instalaci agenta se provede první spojeni s Xlog komponentou
  - Provede se autoregistrace „hosta“ v ramci Zabbix
    - vygeneruje se unikátní autentizační řetězec (zabezpečení další komunikace)
    - host je zařazen do skupiny „Discovered host“
    - přiřadí se základní konfigurační šablona pro danou platformu
      - další šablony přiřazuje administrátor manuálně dle požadované funkcionality
- V pravidelných intervalech si agent aktualizuje svou konfiguraci
  - Defaultně 1x za hodinu
  - Lze (centrálně) přenastavit
  - Každý agent se může aktualizovat v jiném intervalu

DATA SYS

Komponenta Xlog

- Komponenta psaná v PHP
  - Používá Zabbix API - JSON
  - Komponenta zajišťuje komunikaci s NXlog agenty
  - Sestavuje konfigurace individuálně pro konkrétní servery
    - Dle „items“ a maker přiřazených danému hostu v Zabbixu
- Využívá kvalit řízení konfigurace v Zabbix
  - Monitorovací šablony
    - Typizované konfigurace pro různé aplikace (logy)
    - Pružné přiřazování jednotlivým hostům
  - Makra
    - Přizpůsobení typizované konfigurace konkrétním serverům

DATA SYS

Zabbix Xlog šablony

- Definování pravidel sběru a zpracování logů
- Využíváme položky (items) typu „Zabbix Trapper“
- Konfigurační bloky v syntaxi NXlogu zapisujeme do pole „Comment“
  - Pružné použití všech direktiv podporovaných programem NXlog

- Pro pojmenování položek používáme standardizovanou konvenci
  - xlog.config[AGENT,Extension,InFileXlogRotation]
  - xlog.config[AGENT,Input,InSyslogLocal,001,NormalizeAttribs]
  - xlog.config[AGENT,Input,InSyslogLocal,015,Rules-SSH]
  - xlog.config[AGENT,Input,InSyslogLocal,999,FinalStatements]
  - xlog.config[AGENT,Output,OutTcpXlog]
  - xlog.config[AGENT,Route,SyslogLocal2Collector]

DATA SYS

Zabbix Item

Name	ELISA receiver (binary Xlog format)
Type	Zabbix trapper
Key	xlog.config[AGENT,Output,OutTcpXlog] Select
Type of information	Numeric (unsigned)
Data type	Decimal
Units	
Use custom multiplier	☐ 1
History storage period (in days)	10
Trend storage period (in days)	1500
Store value	As is
Show value	As is show value mappings
Allowed hosts	
New application	
Applications	-None- Xlog Config - Linux Base
Populates host inventory field	-None-
Description	# sleep(100000) = 10 messages per second # <Output OutTcpXlog> Module om_tcp Host %ELISA_RCVR_HOST% Port %ELISA_RCVR_PORT% OutputType binary Exec \ if not defined($Hostname) and $Message =~ /^last message/ \ { \ $SourceName = 'Xlog'; \ $Hostname = hostname(); \ } \ sleep(%EVENT_RATE_LIMIT_PAUSE%); </Output>
Enabled	☑

DATA SYS

ELISA výstupní data

Hlavními výstupními kanály systému ELISA jsou:

- Kibana – uživatelské rozhraní pro nahlížení na události
- JasperReport – reporting systém pro zasílání periodických reportů
  - JasperReports® Server, Tomcat aplikace využívající MySQL
  - Jaspersoft® Studio, založeno na Eclipse IDE
  - Jasper Reports ElasticSearch plugin od Wedjaa Open Source Initiative
- Elasticsearch API – přístup dalších komponent k datům ELISA
  - Perl - Search::ElasticSearch DRTECH/Search-Elasticsearch-2.00.tar.gz
  - Python - elasticsearch (2.1.0)
  - Java, JS, Groovy, PHP, Ruby, .NET atd.

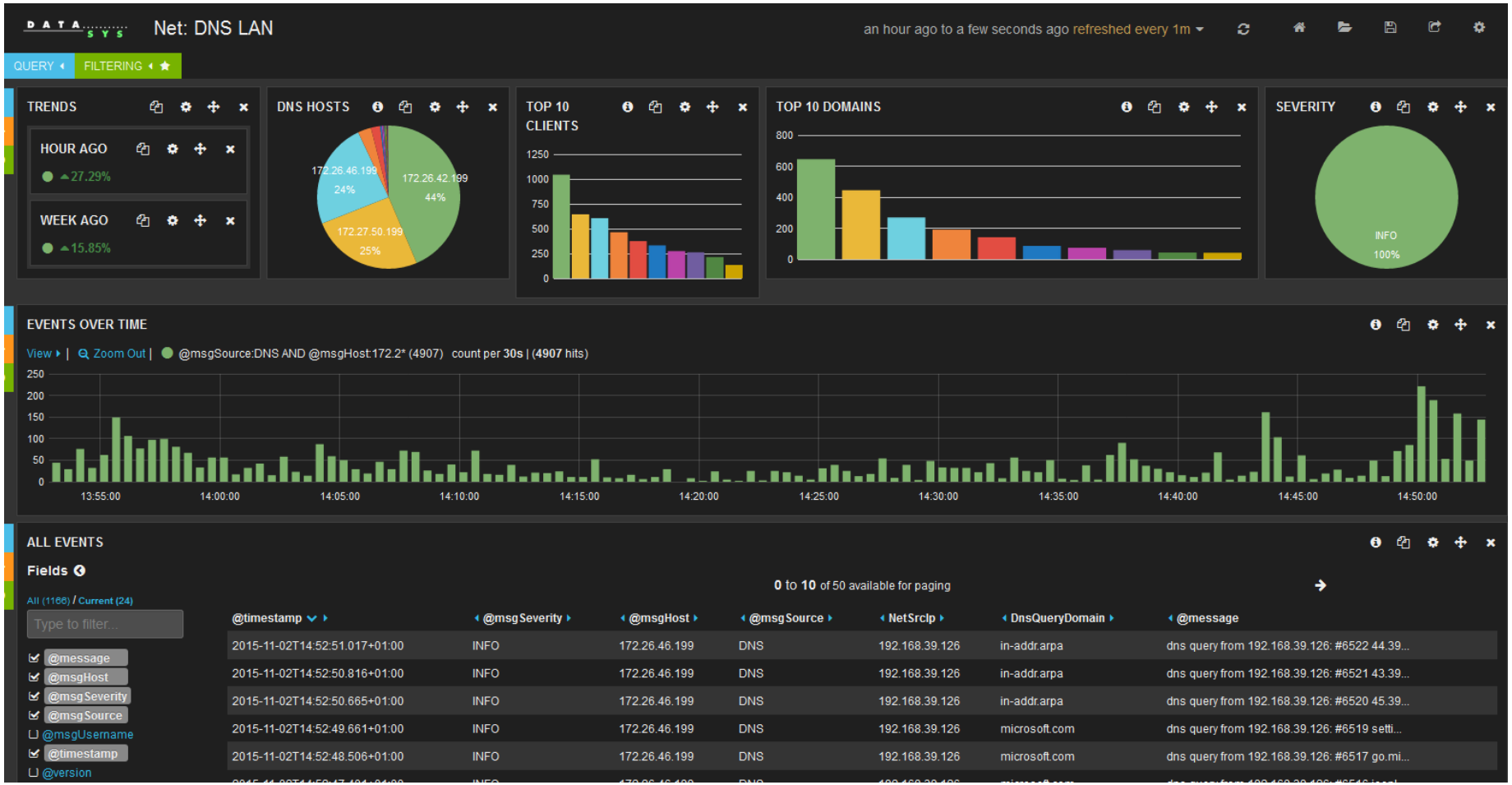
DATA SYS

ELISA GUI - Kibana

- Umožnuje tvorbu vlastních pohledů na zaznamenaná data
- ELISA Dashboard - umožňuje reprezentovat informace
  - Vzhledné grafy
  - Přehledy událostí na časové ose
  - Filtrování
  - Analýza logovaných informací
  - Snadné sdílení
  - Uživatelské role

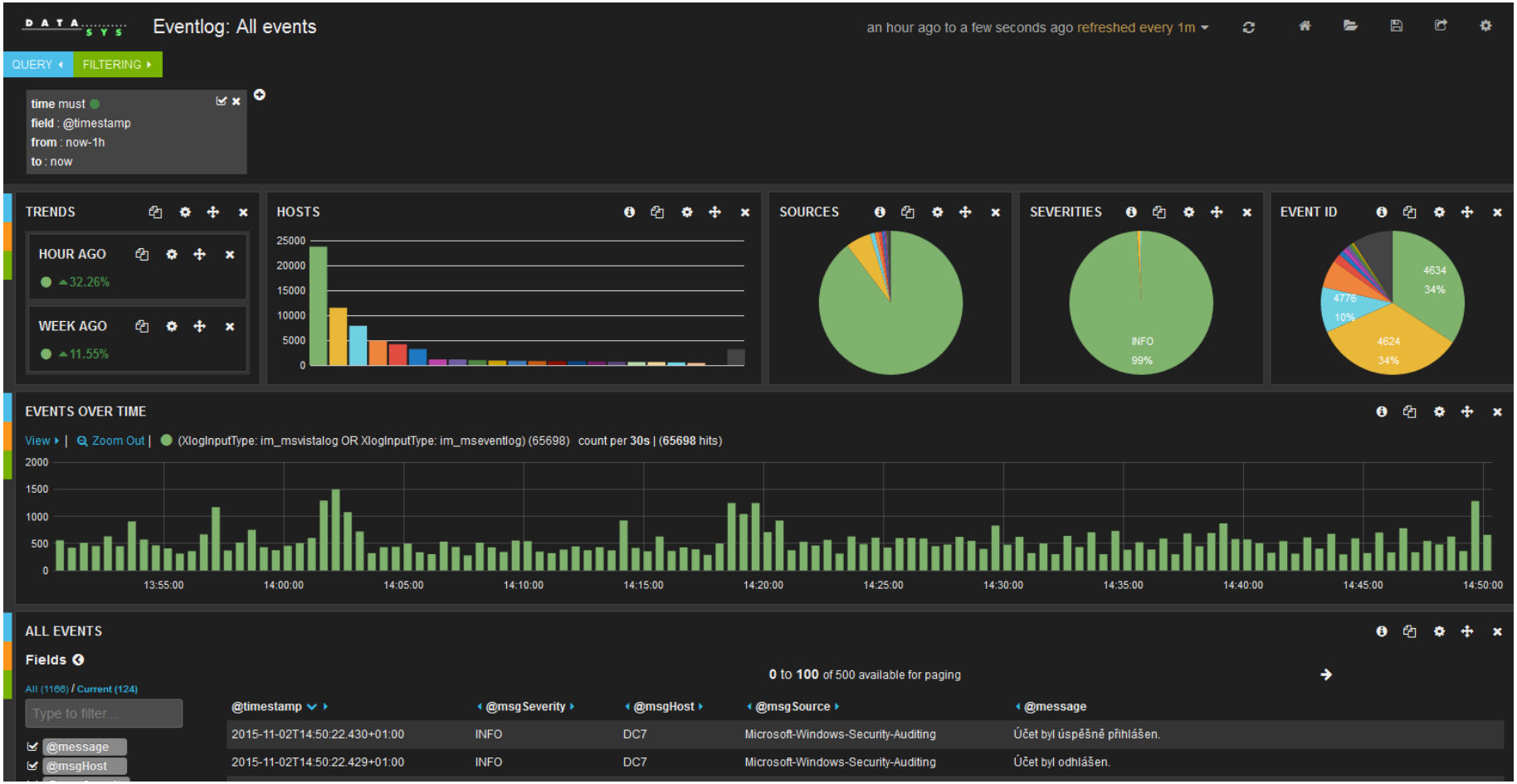
DATA SYS

ELISA GUI - Kibana

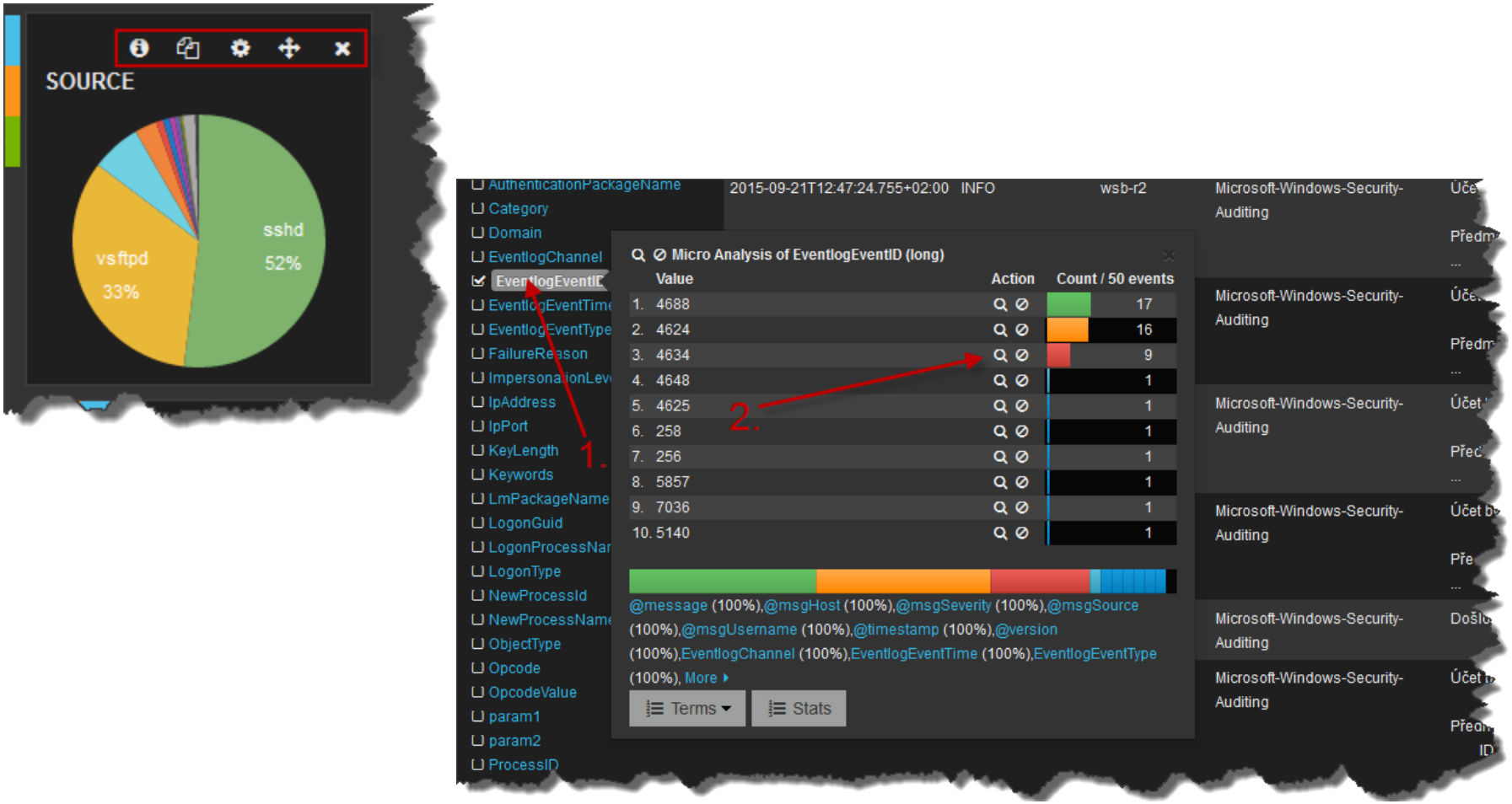


DATA SYS

ELISA GUI - Kibana



ELISA GUI – Analýza dat



ELISA - JasperReports® Server

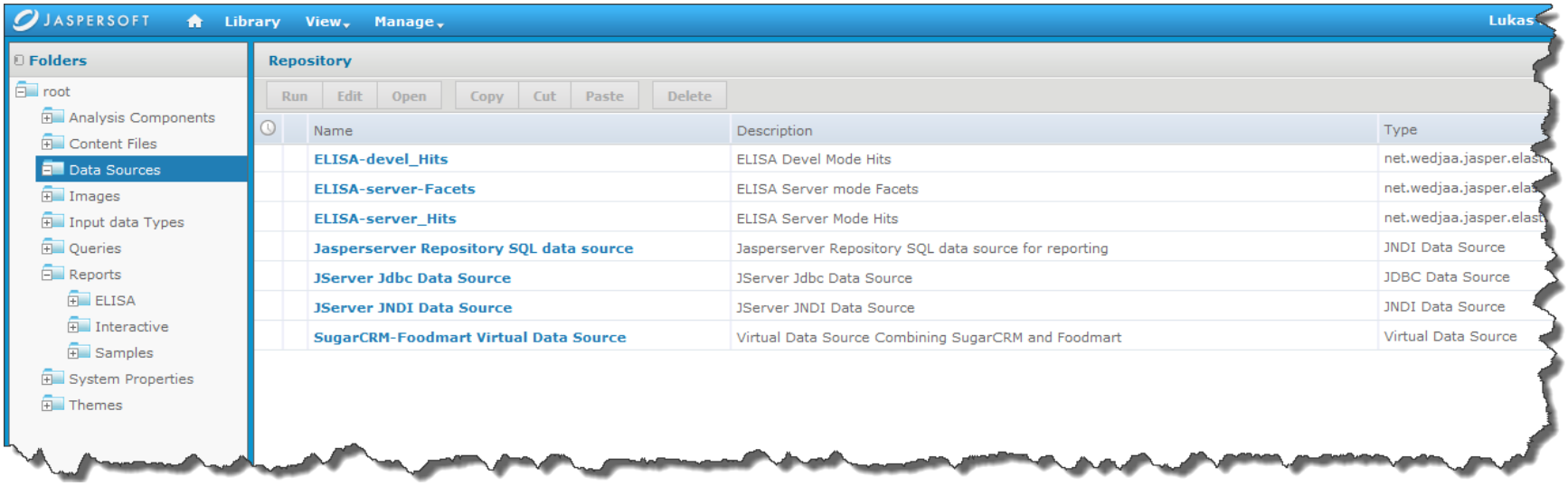
- Robustní reportovací nástroj od společnosti - TIBCO Jaspersoft
  - Umožňuje tvorbu reportů a grafů zaznamenaných událostí
  - Pro tvorbu reportů je používána aplikace Jaspersoft® Studio
    - Studio i Server se pomocí DataSource napojí na data Elasticsearch
  - Reporty mohou být vytvářeny v mnoha formátech
    - PDF, RTF, XML, XLS, CSV, HTML, XHTML, text, DOCX, nebo OpenOffice
    - mohou být periodicky zasílány na E-Mail nebo ukládány na nastavený FTP server.

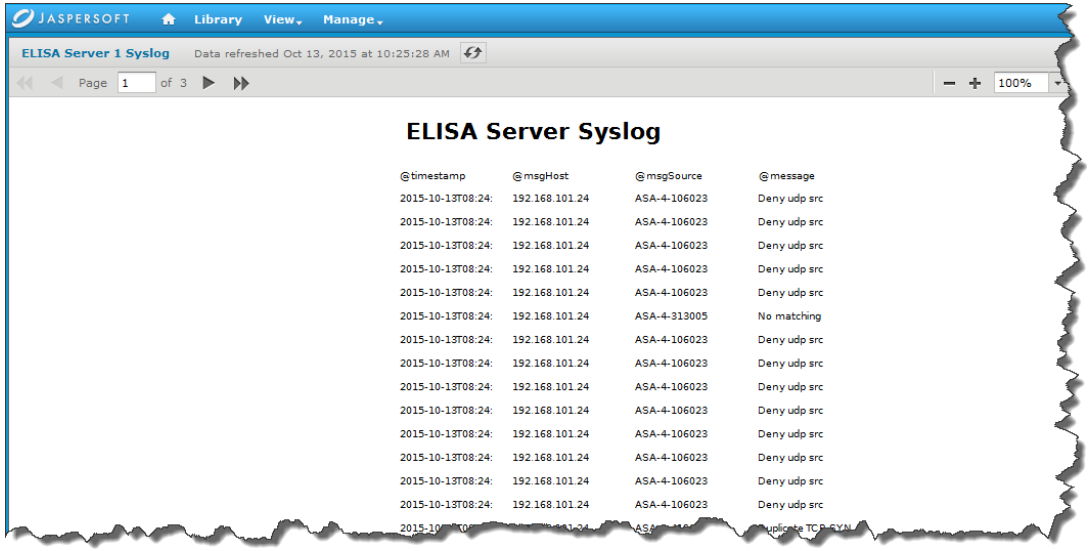
DATA SYS

ELISA - JasperReports® Server

- Přihlašovací obrazovka

ELISA - JasperReports® Server





DATA SYS

ELISA - Jaspersoft® Studio

- Designer studio pro tvorbu reportů
- Export reportů na JasperReport Server
- Grafy, obrázky, sestavy a tabulky
- Napojení na Elasticsearch
- Používá plugin ElasticSearch

DATA SYS

Detekce incidentů

Bezpečnostní události jsou v systému ELISA vyhodnocovány na dvou úrovních:

1) na vstupu při prvotním zpracování událostí
- detekce výskytu konkrétních událostí
- korelace mezi událostmi
  - opakované výskyty
  - relace mezi různými událostmi
  - kontextové korelace

Detekce incidentů

Bezpečnostní události jsou v systému ELISA vyhodnocovány na dvou úrovních:

2) definovanými periodickými dotazy do databáze
- statistické anomálie
- „first“ události apod.

Závěrem

Log management systém ELISA ocení nejen bezpečnostní správci, ale i správci odpovědní za provoz systémů.

Vyhledávání v událostech vznikajících v informačních systémech už prakticky nemůže být jednodušší!

http://www.logmanagement.cz/

DATA SYS

Děkuji
za pozornost

Lukáš Malý, DiS

IT konzultant bezpečnost a monitoring

maly@datasys.cz

DATASYS