NSM

NETWORK SECURITY MONITORING CLUSTER

OUR VISION YOUR SECURITY

AXENTA
Bezpečnost informací je pro nás na prvním místě

BlueFerret

novicom

inveaTECH

Monitoring, správa IP adresního prostoru a řízení přístupu do sítí

Jindřich Šavel
Novicom s.r.o.

jindrich.savel@novicom.cz

Novicom

- Česká společnost zabývající se
  - **vývojem,**
  - **dodávkami**
  - **a provozem**

  systémů pro
  - **správu sítí**
  - **monitoring**
  - **bezpečnost**
  - **a komunikace**

- Orientace na střední a velké zákazníky požadující vyžadující vysokou míru bezpečnosti a spolehlivosti svých systémů
- Společnost s historií - 20 let českém trhu

Novicom – nástroje pro monitoring a správu sítí

NSM
NETWORK SECURITY MONITORING CLUSTER

MoNet — *Řešení distribuovaného monitoringu IT infrastruktury*

AddNet — *Efektivní a správa IP prostoru a bezpečnost přístupu v rozsáhlých sítí*

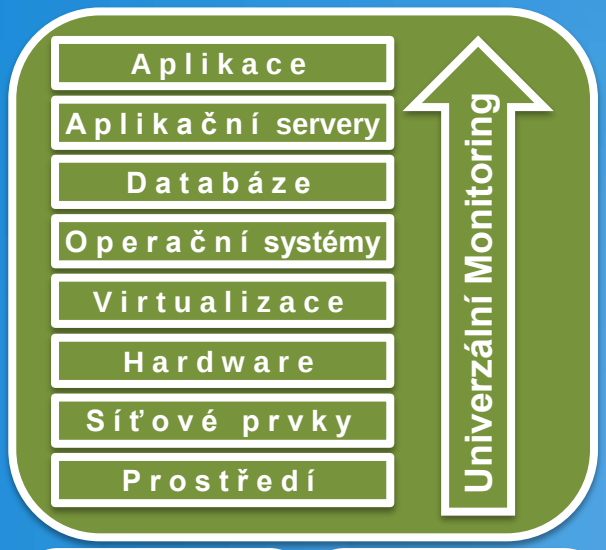
Network tools — *Sada nástrojů pro vysoce efektivní a bezpečný provoz IT infrastruktury*

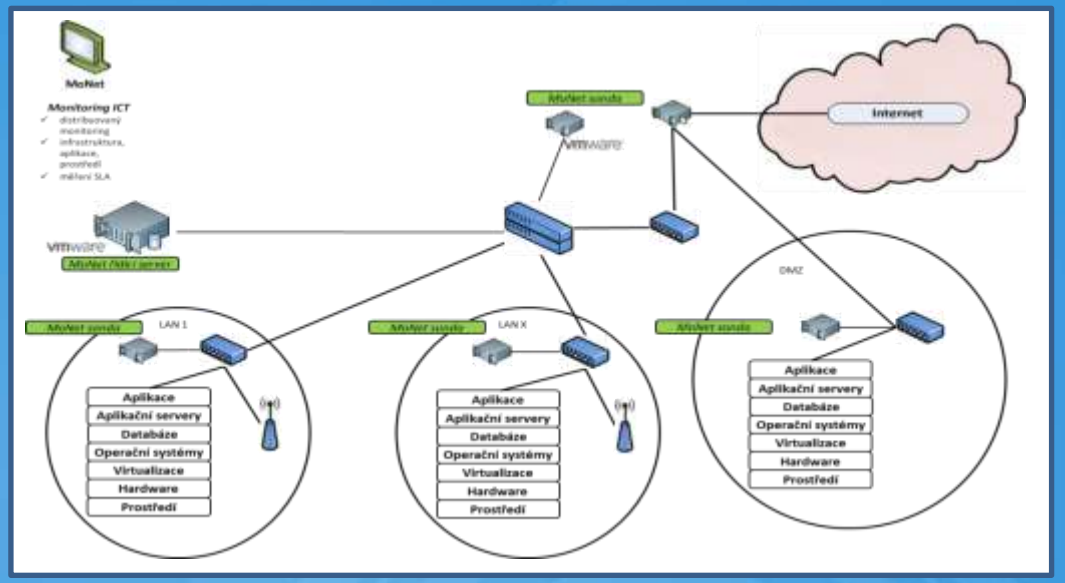
Projects — *Oborová a customizovaná řešení*

Novicom SGP – Secure Grid Platform

Novicom SDP – Secure Delivery Protocol

MoNet - Infrastrukturní monitoring





- Performance management
- Korelace přes všechny vrstvy a všechny lokality
- Vzdálený monitoring a alerting i v případě přerušení spojení do centra
- Automatizované měření SLA

AddNet - Integrovaná správa IP adresního prostoru a NAC

NSM NETWORK SECURITY MONITORING CLUSTER

IPAM

- Správa IP adresního prostoru
- L2 Monitor – historie IP/ MAC / lokalita

DDI - Základní síťové služby

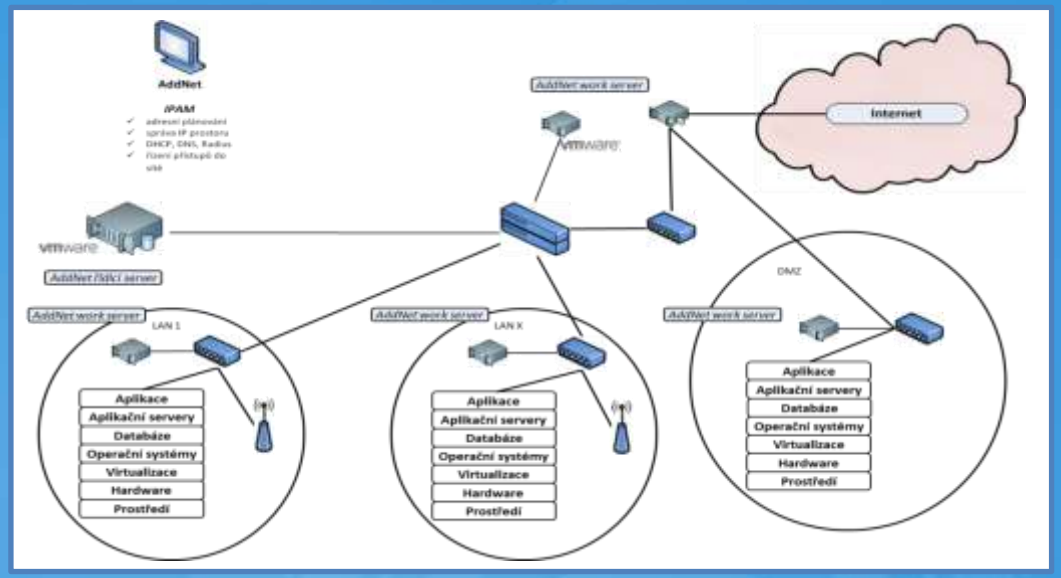
- DHCP
- DNS
- RADIUS

Aktivní prvky

- Repository AP
- Port monitor

Bezpečnost

- 802.1x - MAC autentizace a autorizace
- BYOD zařízení
- Krizové sety



- Integrovaný L2 monitor / DDI / NAC
- Určeno pro rozsáhlé a distribuované sítě
- Nadstandardní provozní spolehlivost

Kde se s řešením Novicom potkáte?

NSM
NETWORK SECURITY MONITORING CLUSTER

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Univerzita Tomáše Bati ve Zlíně

Office DEPOT
Taking Care of Business

Přínosy pro zákazníky

NSM
NETWORK SECURITY MONITORING CLUSTER

MoNet

- Nadstandardně spolehlivý monitoring infrastruktury a aplikací v rozsáhlých sítích

Addnet

- Řádová úspora práce a standardizace činností administrátorů při IP správě
- Zvýšení bezpečnosti sítě formou řízení přístupu zařízení (802.1x MAC autentizace a autorizace)
- Podstatné zvýšení provozní spolehlivosti základních síťových služeb (DHCP, DNS a RADIUS)
- Automatizovaná správa a jednoznačná identifikace BYOD a mobilních zařízení

Přínosy pro bezpečnost z hlediska ZoKB

NSM NETWORK SECURITY MONITORING CLUSTER

Nástroje pro detekci

- Detailní L2 monitoring včetně úplné historie (pro forenzní audit)
  - IP / MAC / lokalita výskytu

Řízení přístupů do sítě

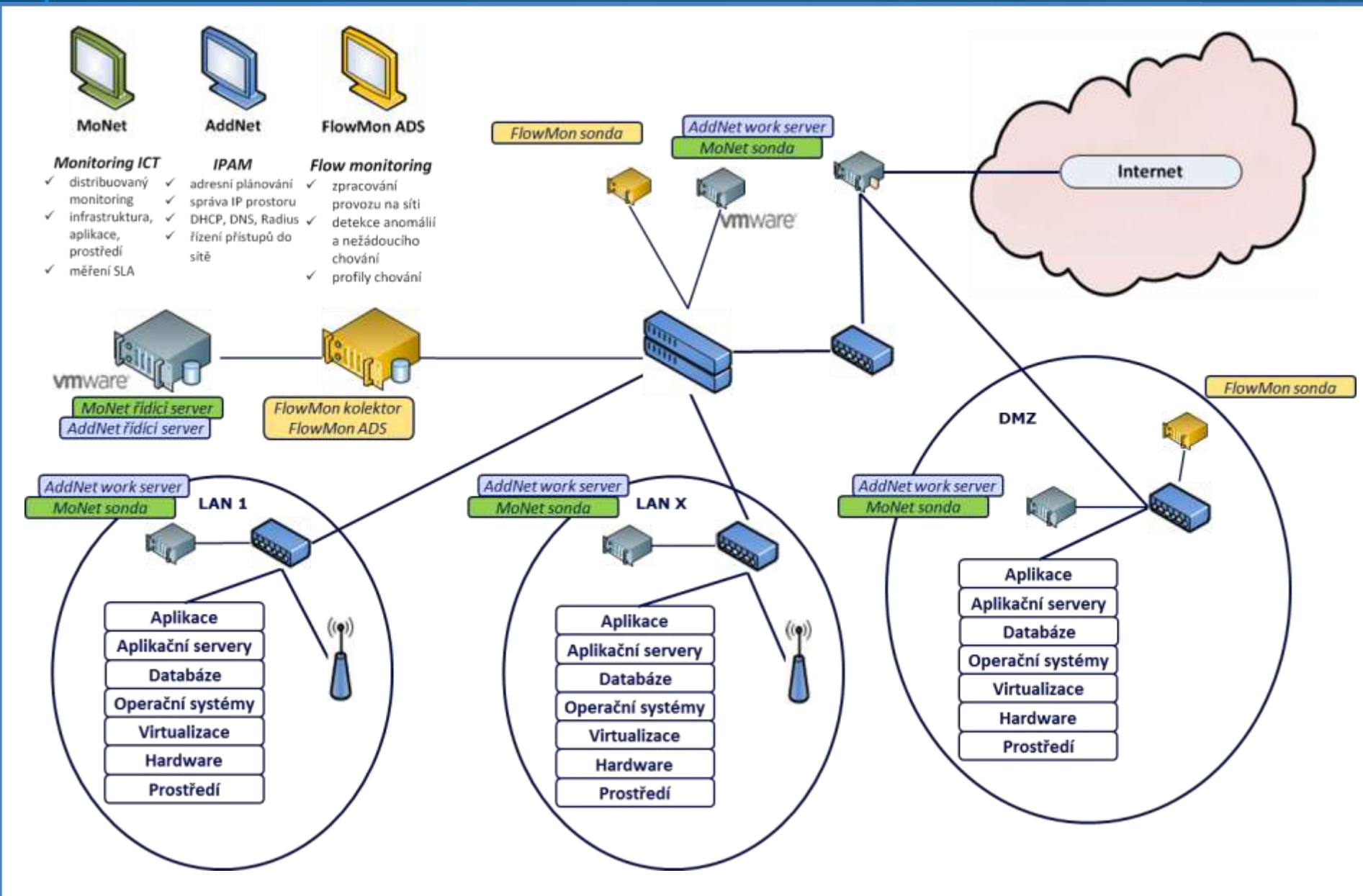
- Na 2. vrstvě – potřebný komplement k uživatelské autentizaci na 6.vrstvě (např. Microsoft doména)
  - 802.1x MAC autentizace
- Možnost snadné správy bezpečnostních domén na úrovni VLAN
  - autorizace

Součást konceptu Aktivní bezpečnosti sítě

- Na 4 kliknutí! Od zjištění kybernetického bezpečnostního incidentu po odpojení kompromitovaného zařízení

Bezpečnost na 4 kliknutí

NSM
NETWORK SECURITY MONITORING CLUSTER



Děkuji za pozornost.

Jindřich Šavel

Obchodní ředitel

Novicom s.r.o.

+420 777 222 961

jindrich.savel@novicom.cz

Aplikační monitoring BlueFerret

Tomáš Mezník

FerretApps s.r.o.

tomas.meznik@ferretapps.com

Výzva – dostupnost dat

NSM
NETWORK SECURITY MONITORING CLUSTER

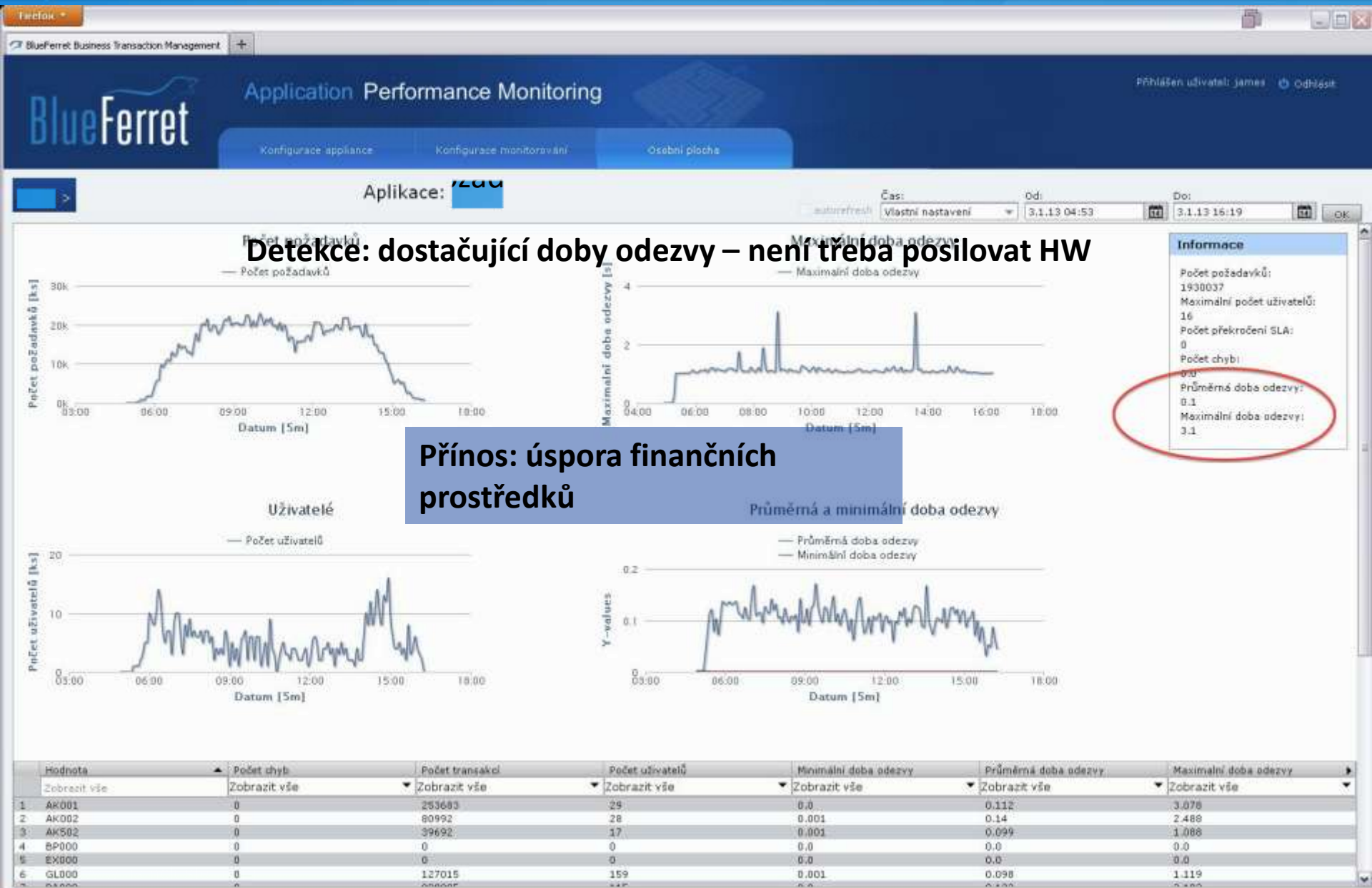
- Zajištění kvalitních služeb, poskytovaných prostřednictvím webových i pobočkových aplikací
- Fungují aplikace v požadované kvalitě?
- Identifikace zdrojů zhoršené výkonnosti
- Spokojený zákazník/produktivní zaměstnanec

Co je BlueFerret

- BEZAGENTNÍ monitoring uživatelských transakcí
- Pohled na výkonnost aplikací z pohledu koncových uživatelů
- Pro VŠECHNY uživatele
- Pro VŠECHNY uživatelské transakce
- V reálném čase
- Nástroj pro zvýšení dostupnosti kritických aplikací

Příklad užití

NSM
NETWORK SECURITY MONITORING CLUSTER

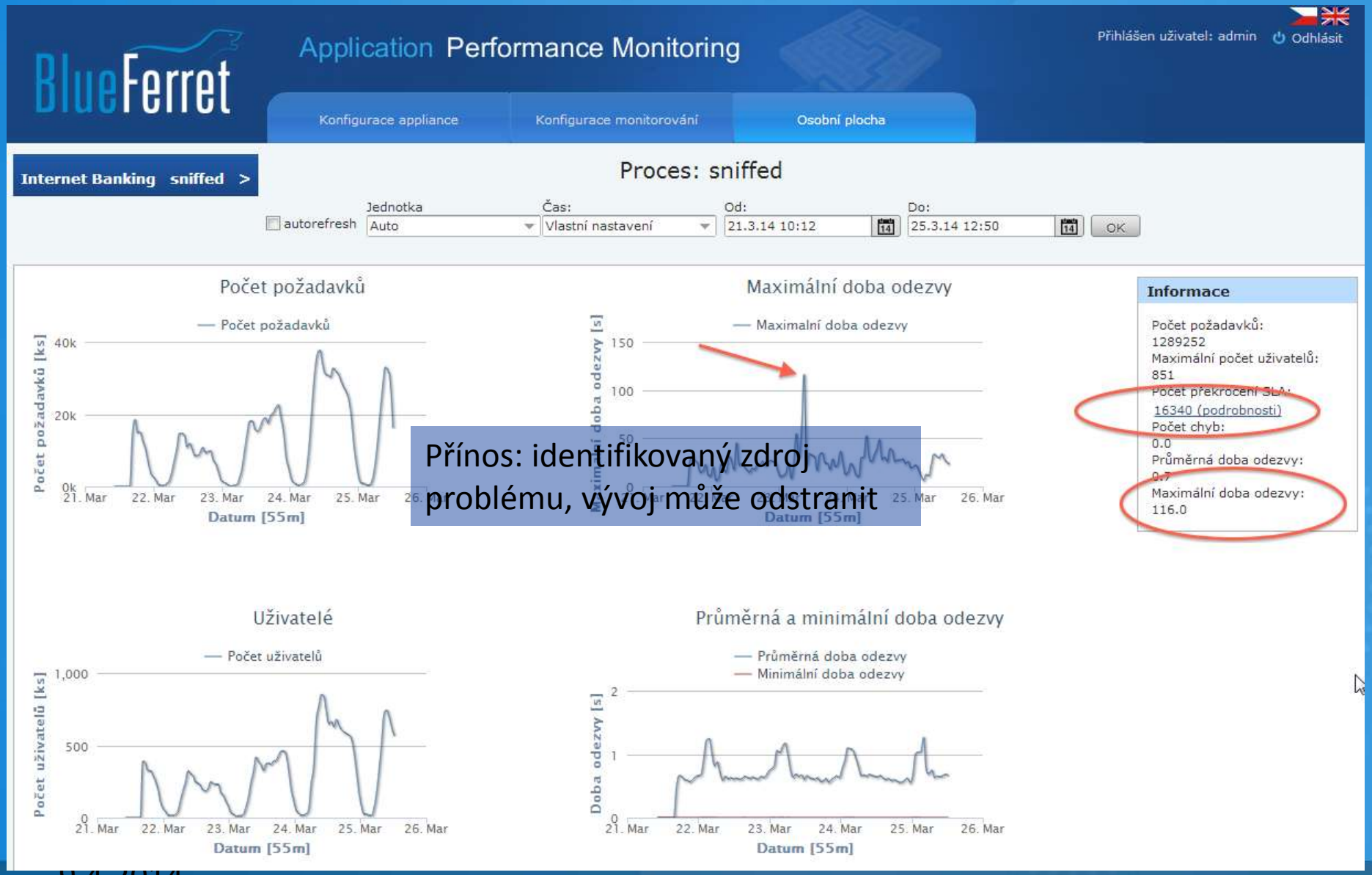


Detekce: dostačující doby odezvy – není třeba posilovat HW

Přínos: úspora finančních prostředků

	Hodnota	Počet chyb	Počet transakcí	Počet uživatelů	Minimální doba odezvy	Průměrná doba odezvy	Maximální doba odezvy
	Zobrazit vše	Zobrazit vše	Zobrazit vše	Zobrazit vše	Zobrazit vše	Zobrazit vše	Zobrazit vše
1	AK001	0	253683	29	0.0	0.112	3.078
2	AK002	0	80992	28	0.001	0.14	2.488
3	AK502	0	39692	17	0.001	0.099	1.088
4	BP000	0	0	0	0.0	0.0	0.0
5	EX000	0	0	0	0.0	0.0	0.0
6	GL000	0	127015	159	0.001	0.098	1.119

Příklad užití

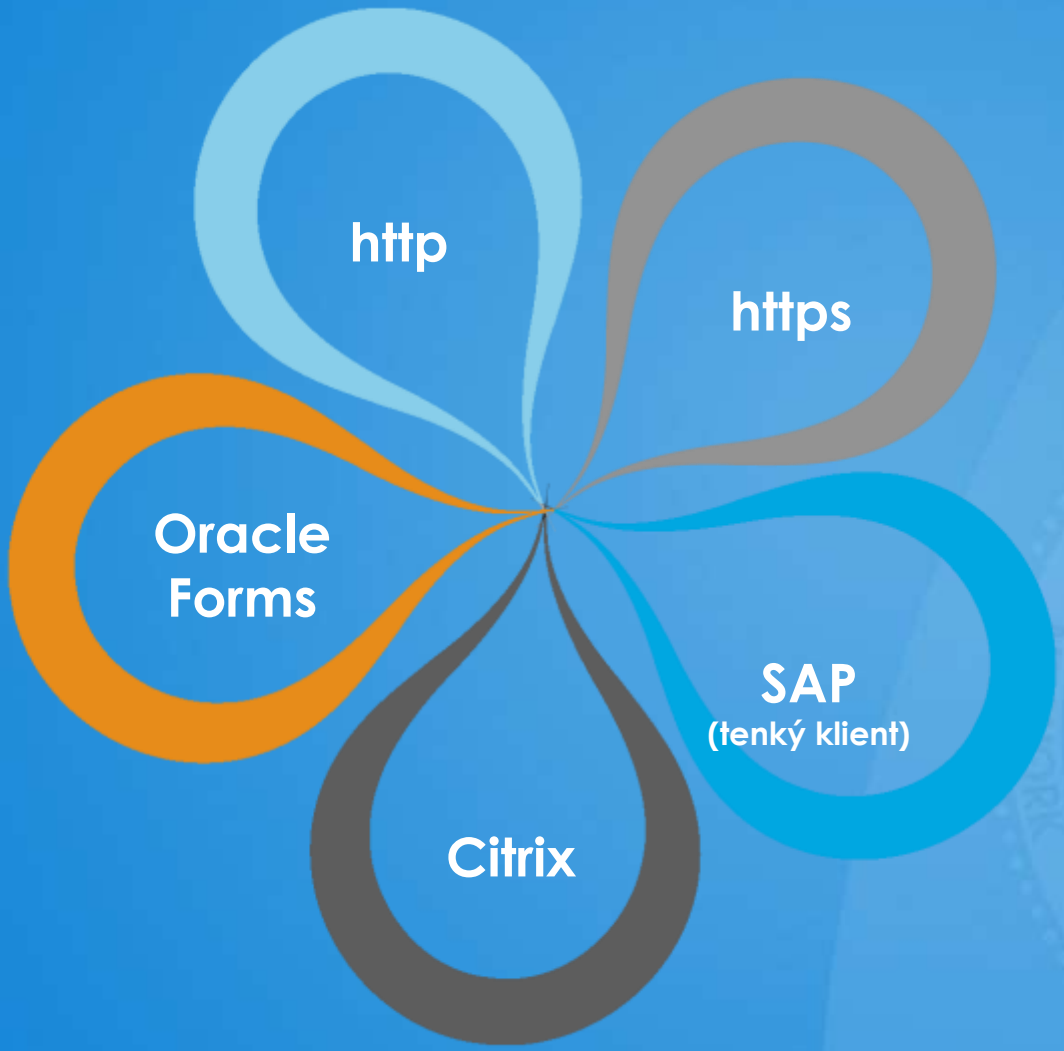


Přínos: identifikovaný zdroj problému, vývoj může odstranit

Metriky

- Počet transakcí
- Doba odezvy aplikace (maximální, průměrná, minimální, případně percentil apod.)
- Počet paralelně přistupujících uživatelů
- Velikost přenášených dat
- Doba přenosu na transportní vrstvě
- Počty a seznam transakcí s překročeným SLA
- Počet výskytů chybových kódů
- Detaily o jednotlivých transakcích (velikosti, doby, IP adresy, Session ID, uživatelské jméno, …)

Co monitoruje BlueFerret



- Zákaznické portály
- Pobočkové aplikace
- Cloud
- Virtuální prostředí

Děkuji za pozornost.

Tomáš Mezník

FerretApps s.r.o.

Olšanská 1a

Praha 3

Monitoring a detekce anomálií FlowMon

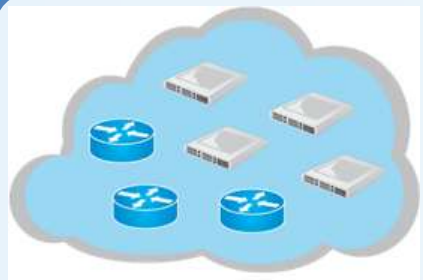
Pavel Minařík

INVEA-TECH, a.s.

minarik@invea.com

Přehled řešení

NSM
NETWORK SECURITY MONITORING CLUSTER



Monitorová provozu datové sítě

Sběr statistik o provozu

Vizualizace a detekce anomálií

Z pohledu uživatele

NSM
NETWORK SECURITY MONITORING CLUSTER

- **Monitorování provozu v síti** (NetFlow/IPFIX)
  - Kompletní viditelnost do dění v síti
  - Real-time a historická data pro LAN & WAN & komunikaci do Internetu
  - Optimalizace správy a provozu sítě
  - Efektivní troubleshooting

- **Bezpečnost datové sítě** (NBA, NBAD)
  - Jediný způsob, jak detekovat pokročilé hrozby
  - Založeno na behaviorální analýze
  - Detekce pokročilého malware, zero-day útoků, podezřelých přenosů dat, změn chování a dalších incidentů

Z pohledu technologie

NSM CLUSTER
NETWORK SECURITY MONITORING CLUSTER

- Monitorování a analýza provozu nové generace
  - Nespoléhá na signatury
  - Funkční i pro šifrovaný provoz
  - Výkon v prostředí 10G

Network Behavior Analysis Update, Gartner

Recommendation

After you have successfully deployed firewalls and intrusion prevention systems with appropriate processes for tuning, analysis and remediation, you should consider NBA to identify network events and behavior that are undetectable using other techniques.

Network Behavior Analysis: Protecting by Predicting and Preventing, Aberdeen Group

Definition

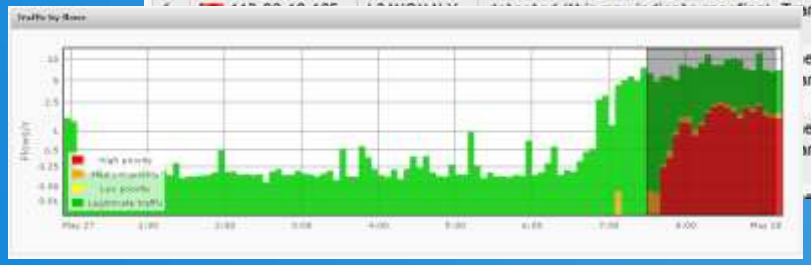
Network Behavior Analysis (NBA) technologies monitor network traffic for unknown or unusual deviations from normal patterns that might indicate the presence of a threat. Commonly used in combination with traditional signature-based approaches to anti-virus, anti-malware, intrusion detection and prevention, and network event management, NBA is especially well-suited for identifying new zero-day exploits and malware for which signatures have not yet been developed.

Několik zajímavých úlovků

DDoS z podvržených adres

- Finanční instituce
- Botnetem infikováno několik stanic
- Podvržené čínské adresy útočí do Vietnamu

#	Zdrojová IP	Typ události	Detail	Čas	Zdroj NetFlow dat	Cíle
1	112.90.18.105	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.66 MiB, packets: 65 559.	2013-08-24 07:15:21	localhost	1.52.6.170, 1.52.13.199, 1.52.42.167, 1.52.59.228, 1.52.71.217, 1.52.87.249, 1.52.133.228, 1.52.174.61, 1.52.192.113, 1.52.218.16, ...
2	112.91.30.17	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.37 MiB, packets: 58 379.	2013-08-24 07:15:21	localhost	1.52.54.212, 1.52.109.106, 1.52.167.73, 1.52.184.215, 1.52.191.229, 1.52.218.123, 1.52.220.241, 1.52.238.4, 1.52.241.199, 1.53.8.41, ...
3	121.10.112.17	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.37 MiB, packets: 58 266.	2013-08-24 07:15:21	localhost	1.52.1.176, 1.52.2.100, 1.52.7.105, 1.52.44.162, 1.52.77.224, 1.52.128.196, 1.52.128.214, 1.52.144.204, 1.52.199.183, 1.52.241.170, ...
4	183.61.138.105	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.66 MiB, packets: 65 415.	2013-08-24 07:15:21	localhost	1.52.58.25, 1.52.85.224, 1.52.86.18, 1.52.92.157, 1.52.174.104, 1.52.183.10, 1.52.184.230, 1.52.190.102, 1.52.203.16, 1.52.235.13, ...
5	210.73.221.181	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.36 MiB, packets: 58 086.	2013-08-24 07:15:21	localhost	1.52.28.245, 1.52.44.63, 1.52.112.109, 1.52.143.60, 1.52.177.97, 1.53.40.147, 1.53.58.10, 1.53.89.183, 1.53.122.157, 1.53.221.26, ...
			The traffic not belonging to any internal network was detected:	2013-08-24 05:39:59	localhost	1.52.4.138, 1.52.12.103, 1.52.28.61, 1.52.31.70, 1.52.37.82, 1.52.42.130, 1.52.44.24, 1.52.48.142, 1.52.67.39, 1.52.83.34, ...
			etwork was nsferred:	2013-08-24 03:38:31	localhost	1.52.7.220, 1.52.11.109, 1.52.28.57, 1.52.42.90, 1.52.74.20, 1.52.95.134, 1.52.114.14, 1.52.115.205, 1.52.119.156, 1.52.122.10, ...
			etwork was nsferred:	2013-08-24 03:00:34	localhost	1.52.12.16, 1.52.77.184, 1.52.104.14, 1.52.125.205, 1.52.128.99, 1.52.134.215, 1.52.137.109, 1.52.139.229, 1.52.203.143, 1.52.209.197, ...



Útok na HTTP autentizaci

- Zdravotnictví
- Vedeno z IP adresy v Indonésii
- Pokusy o uhodnutí hesla do phpMyAdmin
- Detaily ze sedmé vrstvy (hostname, URL)

Event details

Type: **Web form attack (HTTPDICT)**
Timestamp: **2014-03-07 21:10:00**
First NetFlow: **2014-03-07 21:09:24**
Event source: **202.61.105.246**
Event source host name: **N/A**
NetFlow source: **CORE**
Probability: **100 %**
False positive: **No**

Detail: **The server (target) has sent the 1.65 KiB file 591 times.**

on IP	Start	Duration	Protocol	Src. port	Dst. port	Trns. B	Packets	Flags	Tos	Src. MAC	Dst. MAC	Src. VLAN	Dst. VLAN	Nbar tag	URL
105.246	2014-03-07 21:09:24.733	0.495	TCP	80	23040	1693	5	.AP.SF	0	a4:ba:db:e0:7e:72	02:17:c5:e0:45:88	0	0	3:80	
255.11	2014-03-07 21:09:24.733	0.495	TCP	23040	80	328	6	.AP.SF	0	02:17:c5:e0:45:88	a4:ba:db:e0:7e:72	0	0	3:80	[redacted].224.15 /phpMyAdmin-2.6.0-rc1/main.php
255.11	2014-03-07 21:09:25.228	0.496	TCP	23050	80	276	5	.AP.SF	0	02:17:c5:e0:45:88	a4:ba:db:e0:7e:72	0	0	3:80	[redacted].224.15 /phpMyAdmin-2.6.0-rc2/main.php
105.246	2014-03-07 21:09:25.229	0.495	TCP	80	23050	1693	5	.AP.SF	0	a4:ba:db:e0:7e:72	02:17:c5:e0:45:88	0	0	3:80	

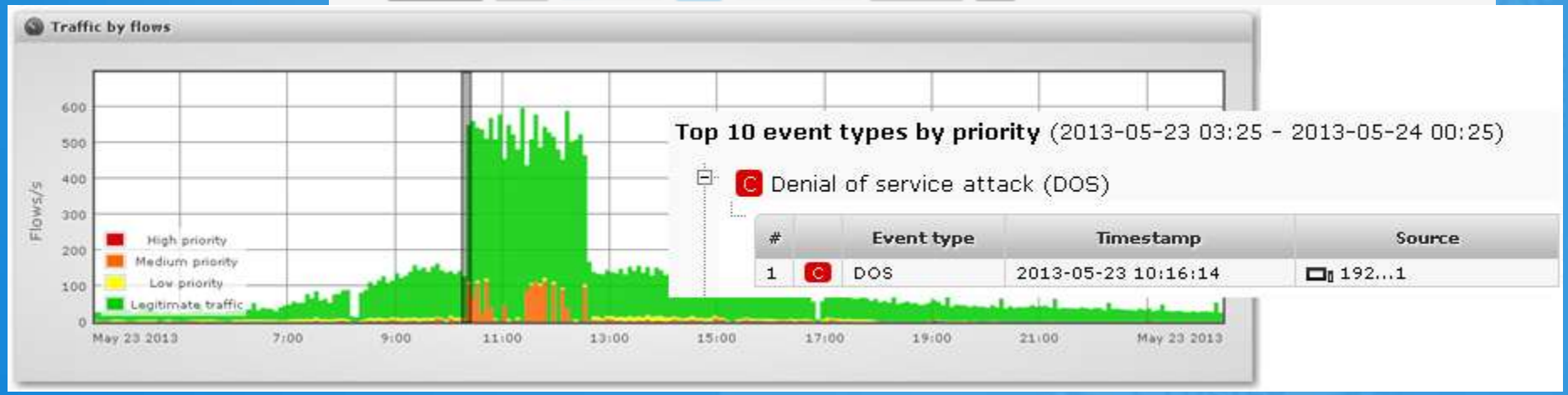
Infikovaná stanice

- Informační technologie
- Botnetem infikovaná stanice z lokální sítě zavlečená do DDoS útoků na Spamhaus

The DDoS That Knocked Spamhaus Offline (And How We Mitigated It)

Published on March 20, 2013 06:26PM by Matthew Prince.

Share 171 Share 71 Like 918 Tweet 465



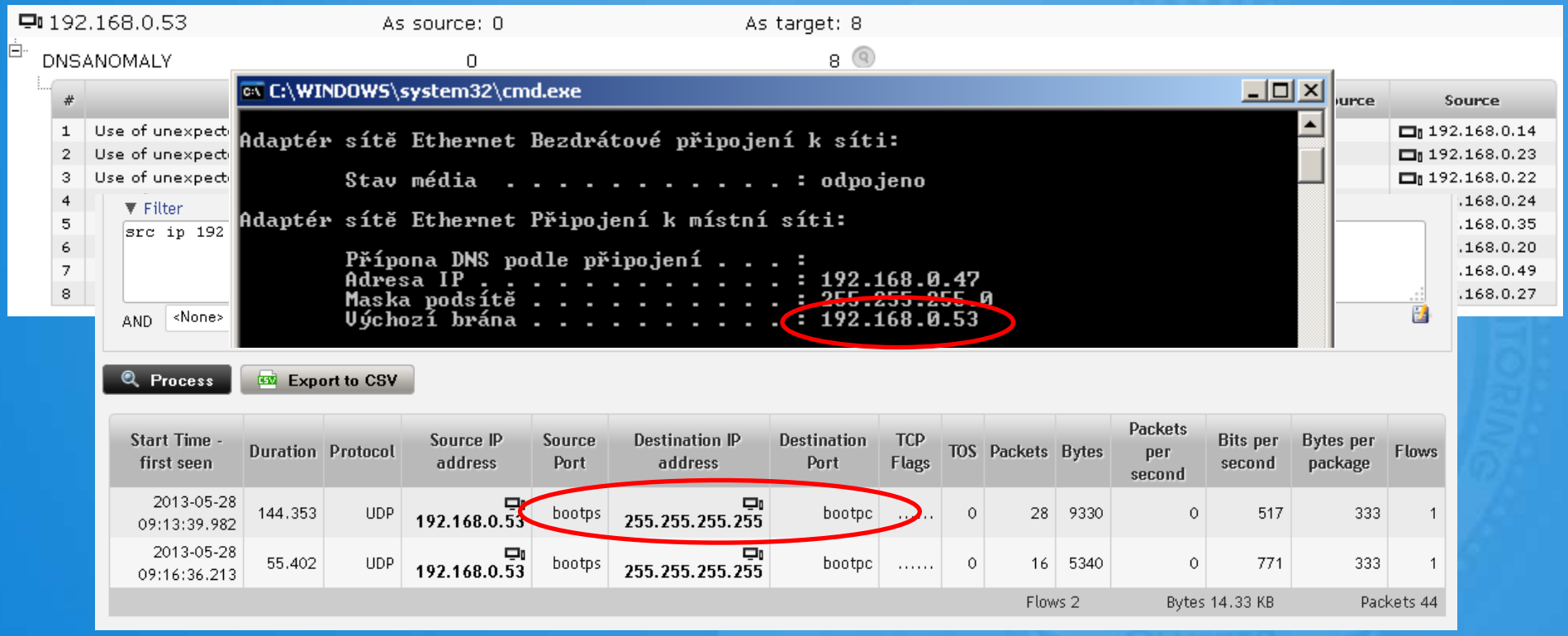
Únik dat

- Obchodní společnost
- Zaměstnanec ve výpovědi
- Uložení interních dokumentů na sdílený disk poskytovaný službou Yahoo
- Zaznamenáno jako pohyb dat z LAN do internetu
- Po prošetření poměrně závažný incident

#	Source	Event type	Detail	Timestamp	Net flow source	Targets
1	10.1.1.84	UPLOAD	Uploaded: 38.83 MiB, downloaded: 0.57 MiB, ports: 80	2012-05-10 11:43:34	localhost	98.136.145.156 (r5.ycpi.vip.ac4.yahoo.net)
2	10.1.1.84	UPLOAD	Uploaded: 243.48 MiB, downloaded: 4.07 MiB, ports: 80	2012-05-10 11:37:19	localhost	98.136.145.156 (r5.ycpi.vip.ac4.yahoo.net)
3	10.1.1.84	UPLOAD	Uploaded: 199.97 MiB, downloaded: 4.49 MiB, ports: 80	2012-05-10 11:33:47	localhost	98.136 United States vip.ac4.yahoo.net)
4	10.1.1.84	UPLOAD	Uploaded: 232.03 MiB, downloaded: 4.38 MiB, ports: 80	2012-05-10 11:28:32	localhost	98.136.145.156 (r5.ycpi.vip.ac4.yahoo.net)
5	10.1.1.84	UPLOAD	Uploaded: 197.11 MiB, downloaded: 3.74 MiB, ports: 80	2012-05-10 11:24:10	localhost	98.136.145.156 (r5.ycpi.vip.ac4.yahoo.net)

Odposlech provozu

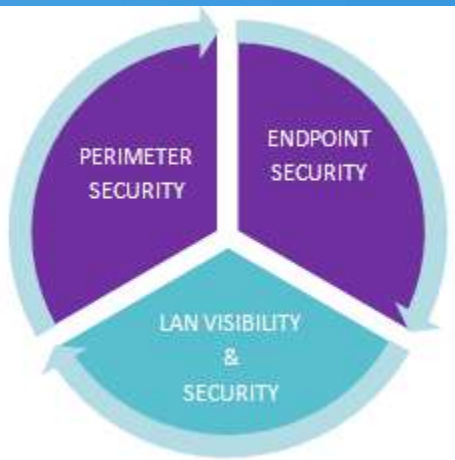
- Služby
- Pokročilý malware přesměroval provoz na infikovanou stanici prostřednictvím DHCP



Shrnutí

Bezpečná infrastruktura

- Perimetr, stanice, LAN
- Bez návazností to nepůjde



BEZPEČNOSTNÍ ODDĚLENÍ

SIEM

Firewall → IDS/IPS → NBA

FlowMon

SÍŤOVÉ ODDĚLENÍ

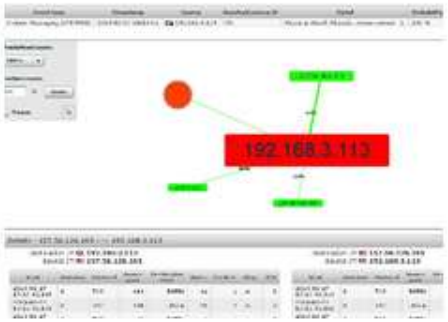
SNMP → Flow monitoring → Paketová analýza

- Kolik paketů, kolik dat
- Základní troubleshooting

- Kdo, s kým, co, jak dlouho
- Efektivní řešení problémů
- Optimalizace sítě
- Sledování trendů, SLA

- Detailní analýza
- Časově velmi náročná
- Na konkrétním místě
- V konkrétním čase

Shrnutí



Děkuji za pozornost.

Pavel Minařík

INVEA-TECH, a.s.

U Vodárny 2

616 00, Brno

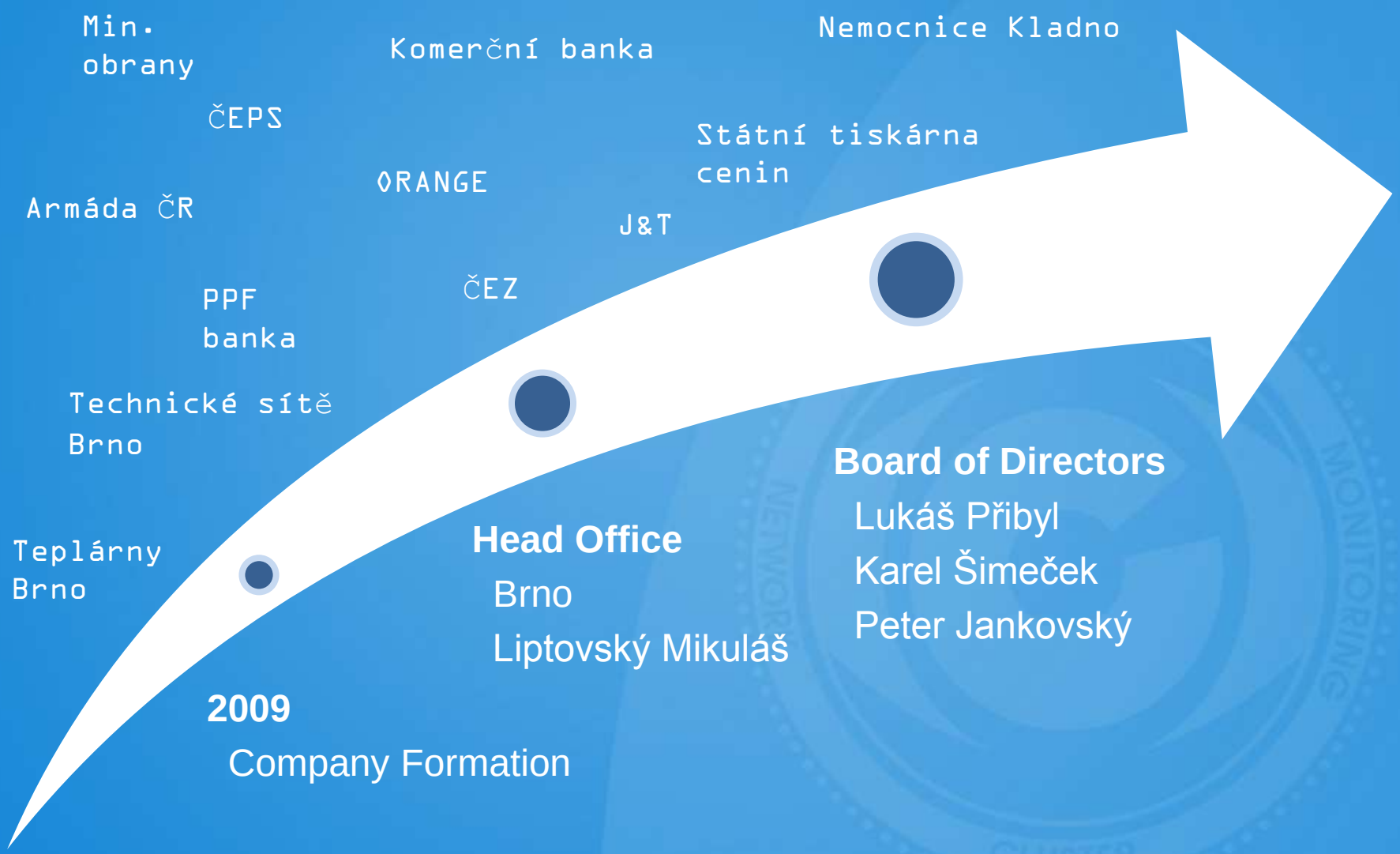
Axenta

Najdi incident v kupě logů

Ing. Lukáš Přibyl, CEO

AXENTA a.s.
+420 724 256 695
pribyl@axenta.cz

AXENTA I.


Min. obrany
ČEPS
Armáda ČR
PPF banka
Technické sítě Brno
Teplárny Brno
Komerční banka
ORANGE
ČEZ
J&T
Státní tiskárna cenin
Nemocnice Kladno
2009
Company Formation
Head Office
Brno
Liptovský Mikuláš
Board of Directors
Lukáš Přibyl
Karel Šimeček
Peter Jankovský

AXENTA II.

NSM
NETWORK SECURITY MONITORING CLUSTER

Analýzy

- Rizik
- Procesů
- Identity Management
- Bezpečnosti informací

Monitoring

- Provozní
- Log Management
- SIEM

ICT bezpečnost

- WAF
- Řízení privilegovaných přístupů
- Školení, uvědomovací kampaně

Naše SIEM reference

NSM
NETWORK SECURITY MONITORING CLUSTER

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Ministerstvo obrany
České republiky

SKUPINA ČEZ

KB

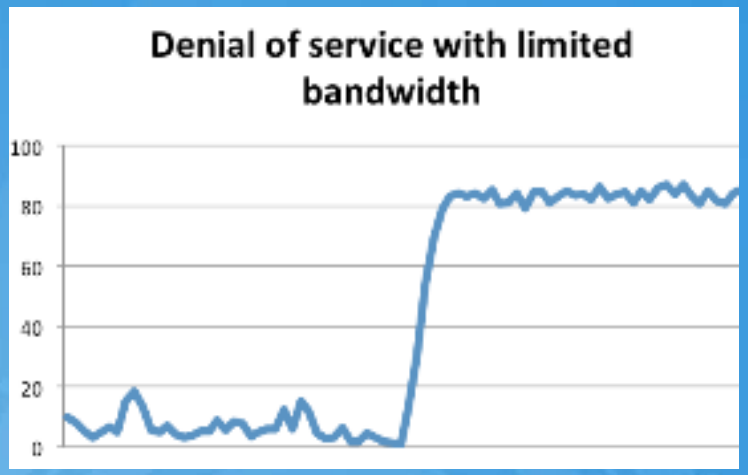
PPF Banka

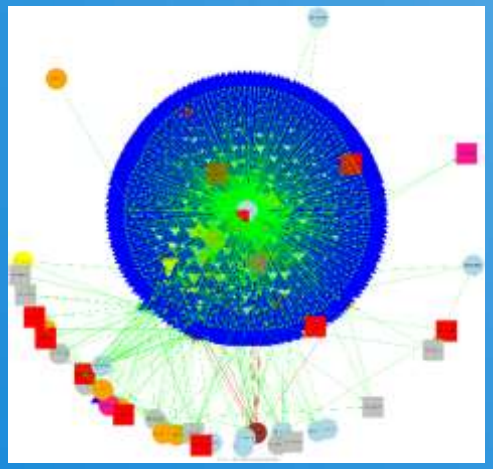
Jak vypadá incident?

Co je někde běžný stav, **je jinde incident!**

Reálný stav

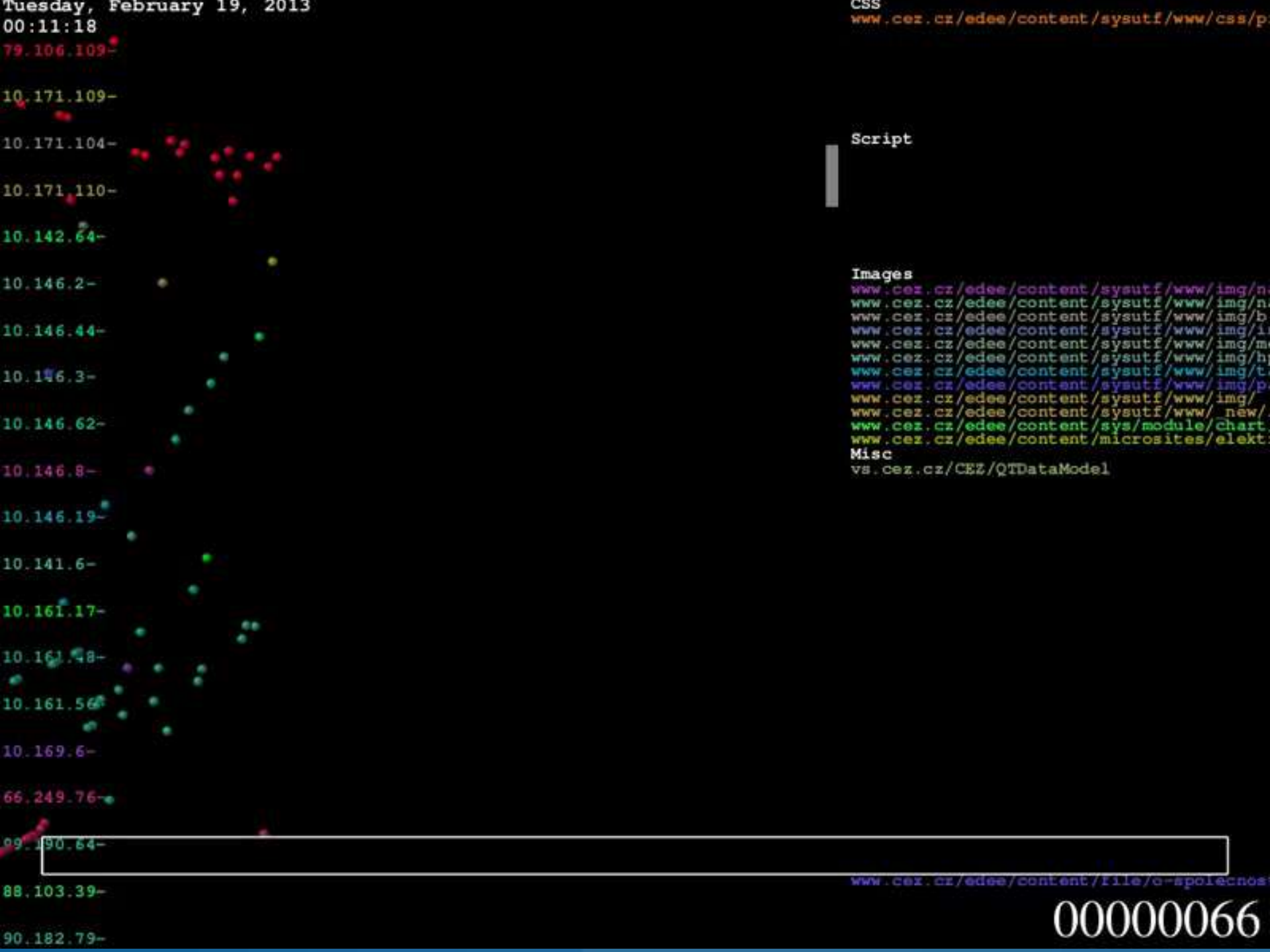
Provozní monitoring





Bezpečnostní monitoring = **SIEM**

Není důležité všechno vidět, ale **je důležité o všem vědět!**


Tuesday, February 19, 2013
00:11:18
79.106.109-
10.171.109-
10.171.104-
10.171.110-
10.142.64-
10.146.2-
10.146.44-
10.146.3-
10.146.62-
10.146.8-
10.146.19-
10.141.6-
10.161.17-
10.161.48-
10.161.56-
10.169.6-
66.249.76-
99.190.64-
88.103.39-
90.182.79-
CSS
www.cez.cz/edee/content/sysutf/www/css/p
Script
Images
www.cez.cz/edee/content/sysutf/www/img/n
www.cez.cz/edee/content/sysutf/www/img/n
www.cez.cz/edee/content/sysutf/www/img/b
www.cez.cz/edee/content/sysutf/www/img/i
www.cez.cz/edee/content/sysutf/www/img/m
www.cez.cz/edee/content/sysutf/www/img/h
www.cez.cz/edee/content/sysutf/www/img/t
www.cez.cz/edee/content/sysutf/www/img/p
www.cez.cz/edee/content/sysutf/www/img/
www.cez.cz/edee/content/sysutf/www/_new/
www.cez.cz/edee/content/sys/module/chart
www.cez.cz/edee/content/microsites/elekt
Misc
vs.cez.cz/CEZ/QTDataModel
www.cez.cz/edee/content/file/o-spolecnos
00000066

Děkuji za pozornost.

Ing. Lukáš Přibyl, CEO

AXENTA a.s.

+420 724 256 695

pribyl@axenta.cz

Rekapitulace celkového konceptu