SECURITY 2011

19. ročník konference o bezpečnosti v ICT

Kam směřují SIEM systémy,

aneb od logů přes SOC po eGRC

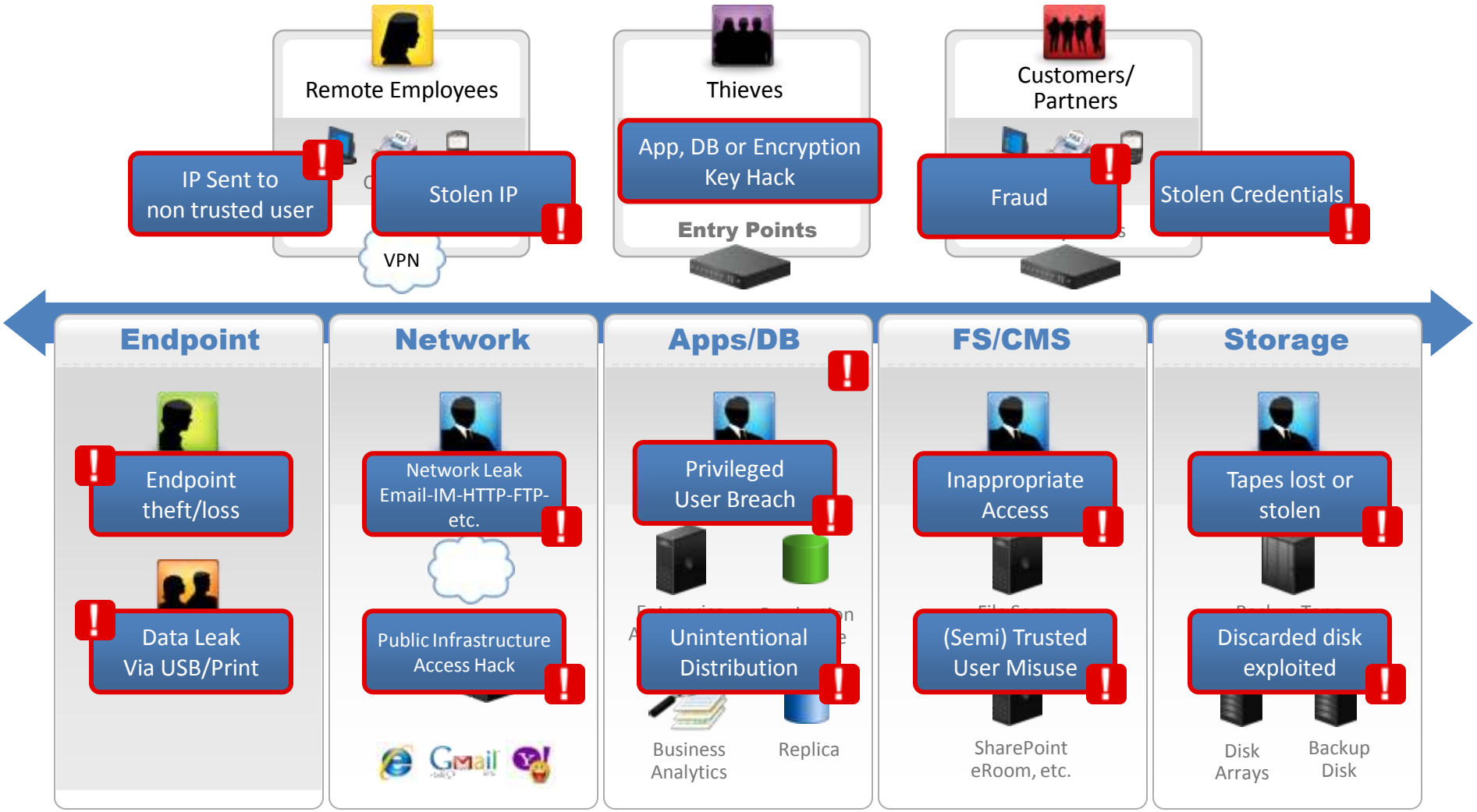
David Matějů

RSA, The Security Division of EMC

Agenda

- Bezpečnostní monitoring
  - Útoky na infrastrukturu
  - Útoky na data a informace
  - Porušení bezpečnostních politik
- Dnešní možnosti monitoringu a analýzy událostí
  - Krok 1: Log Collection
  - Krok 2: SIEM a SOC – Security Information and Event Management a Security Operations Center
  - Krok 3: Integrace s eGRC – Governance, Risk, Compliance
- Shrnutí a výhled

Realita: Stále rostoucí počet útoků

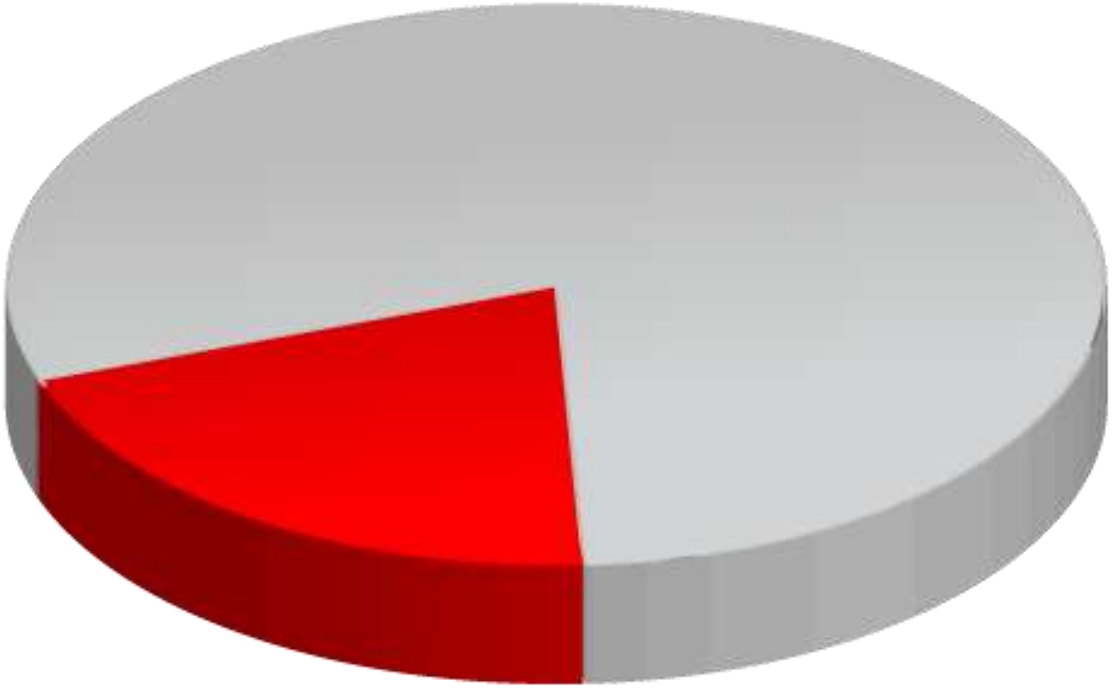


Krok 1: Log Collection Dashboard

Blue Coat - Activity Category by User (Forensic Data) | Investigation (Forensic Data) | SOC - Attack Investigation (Forensic Data) | Excessive Web Surfing Activity (Forensic Data)

MessageTime	DeviceClassName	DeviceTypeName	EventCategory	Address1	Address2	VID	Action	DeviceAddr...	MessageID
2008-03-23 21:02:17.0	VPN	Nortel VPN Contivity	Attacks.Denial of Service					89.128.98.68	00269
2008-03-23 21:02:42.0	VPN	Nortel VPN Contivity	Attacks.Denial of Service	192.168.224.9				89.128.98.68	00257:04
2008-03-23 21:02:45.0	VPN	Nortel VPN Contivity	Attacks.Access.Modification.Network Based.HTTP				http header ...	89.128.98.68	00175
2008-03-23 21:02:46.0	VPN	Nortel VPN Contivity	Attacks.Access.Modification					89.128.98.68	00309
2008-03-23 21:02:46.0	VPN	Nortel VPN Contivity	Attacks.Access.Modification					89.128.98.68	00152:00
2006-04-11 08:12:45.0	IDS	ISS Realsecure	Attacks.Access.Modification.Network Based.HTTP	194.87.5.82	10.10.50.220	352...		10.10.50.61	HTTP_GetAccess_login
2006-04-11 08:12:45.0	IDS	ISS Realsecure	Attacks.Denial of Service	194.87.5.82	10.10.50.220	231...		10.10.50.61	Cisco_Syslog_DoS
2006-04-11 08:12:47.0	FIREWALL	Netscreen	Attacks.Denial of Service.Bandwidth consumption	194.87.5.82	10.10.50.12			10.10.50.1	00007:14
2006-04-11 08:12:48.0	FIREWALL	Netscreen	Attacks.Malicious Code	10.10.50.1	20.20.20.2		executable p...	10.10.50.1	00400
2006-04-11 08:12:33.0	FIREWALL	Netscreen	Attacks.Access.Modification	209.67.10.10	10.10.50.12			10.10.50.1	00026
2006-04-11 08:12:33.0	FIREWALL	Netscreen	Attacks.Access.Modification	209.67.10.10	10.10.50.12			10.10.50.1	00026
2006-04-11 08:12:49.0	FIREWALL	Netscreen	Attacks.Access	209.67.10.10	10.10.50.10			10.10.50.1	00004:04
2006-04-11 08:12:49.0	FIREWALL	Netscreen	Attacks.Access	209.67.10.10	10.10.50.12			10.10.50.1	00004:05
2006-04-11 08:12:50.0	FIREWALL	Netscreen	Attacks.Access.Modification.TCP/IP	209.67.10.11	10.10.50.12			10.10.50.1	00005:03
2006-04-11 08:12:50.0	FIREWALL	Netscreen	Attacks.Access.Modification.TCP/IP	209.67.10.10	10.10.50.12			10.10.50.1	00005:03
2006-04-11 08:12:50.0	FIREWALL	Netscreen	Attacks.Access.Modification.TCP/IP	209.67.10.12	10.10.50.12			10.10.50.1	00005:04
2006-04-11 08:12:50.0	FIREWALL	Netscreen	Attacks.Denial of Service	209.67.10.100	10.10.50.12			10.10.50.1	00006
2006-04-11 08:12:50.0	FIREWALL	Netscreen	Attacks.Denial of Service	209.67.10.111	10.10.50.12			10.10.50.1	00006
2006-04-11 08:12:51.0	FIREWALL	Netscreen	Attacks.Denial of Service.Bandwidth consumption	209.67.10.30	10.10.50.10			10.10.50.1	00007:46
2006-04-11 08:12:51.0	FIREWALL	Netscreen	Attacks.Denial of Service.Bandwidth consumption	209.67.10.10	10.10.50.10			10.10.50.1	00007:46
2006-04-11 08:12:51.0	FIREWALL	Netscreen	Attacks.Access.Modification	209.67.10.10	10.10.50.12			10.10.50.1	00008
2006-04-11 08:12:51.0	FIREWALL	Netscreen	Attacks.Access.Modification	209.67.10.40	10.10.50.22			10.10.50.1	00008
2006-04-11 08:12:51.0	FIREWALL	Netscreen	Attacks.Access.Modification	209.67.10.30	10.10.50.12			10.10.50.1	00008:01
2006-04-11 08:12:52.0	FIREWALL	Netscreen	Attacks.Access.Modification	209.67.10.11	10.10.50.12			10.10.50.1	00009:05
2006-04-11 08:12:52.0	FIREWALL	Netscreen	Attacks.Access.Modification	209.67.10.30	10.10.50.12			10.10.50.1	00009:05
2006-04-11 08:12:52.0	FIREWALL	Netscreen	Attacks.Denial of Service	209.67.10.10	10.10.50.12			10.10.50.1	00010
2006-04-11 08:12:52.0	FIREWALL	Netscreen	Attacks.Denial of Service	209.67.10.10	10.10.50.12			10.10.50.1	00010
2006-04-11 08:12:52.0	FIREWALL	Netscreen	Attacks.Access.Modification.TCP/IP	209.67.10.10	10.10.50.12			10.10.50.1	00011
2006-04-11 08:12:52.0	FIREWALL	Netscreen	Attacks.Access.Modification.TCP/IP	209.67.10.10	10.10.50.12			10.10.50.1	00011
2006-04-11 08:12:53.0	FIREWALL	Netscreen	Attacks.Access.Modification.TCP/IP	209.67.10.10	10.10.50.10			10.10.50.1	00011:02
2006-04-11 08:12:53.0	FIREWALL	Netscreen	Attacks.Access.Modification.TCP/IP	209.67.10.10	10.10.50.12			10.10.50.1	00012:05
2006-04-11 08:12:53.0	FIREWALL	Netscreen	Attacks.Access.Modification.TCP/IP	209.67.10.10	10.10.50.12			10.10.50.1	00012:06
2006-04-11 08:12:53.0	FIREWALL	Netscreen	Attacks.Access.Modification.TCP/IP	209.67.10.10	10.10.50.12			10.10.50.1	00012:06
2006-04-11 08:12:53.0	FIREWALL	Netscreen	Attacks.Access.Modification.TCP/IP	209.67.10.10	10.10.50.12			10.10.50.1	00012:05
2006-04-11 08:12:57.0	FIREWALL	Netscreen	Attacks.Access.Modification	209.67.10.10	10.10.50.12			10.10.50.1	00026
2006-04-11 08:12:57.0	FIREWALL	Netscreen	Attacks.Access.Modification	209.67.10.10	10.10.50.12			10.10.50.1	00026

Může ale IT trávit 20% času nad logy?



Když ano, umí pak odpovědět?

- Jsme zabezpečeni?
- Jsme ve shodě s předpisy?
- Kde máme ještě mezery?
- Jak prioritizovat úkoly?

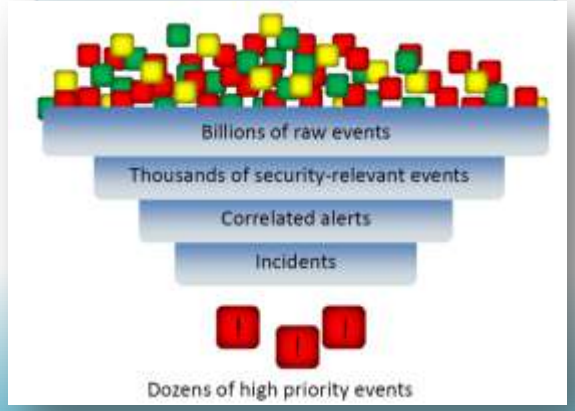
Asi ne. Potřebuje totiž SIEM ...

SIEM supports 3 key aspects of Security Operations

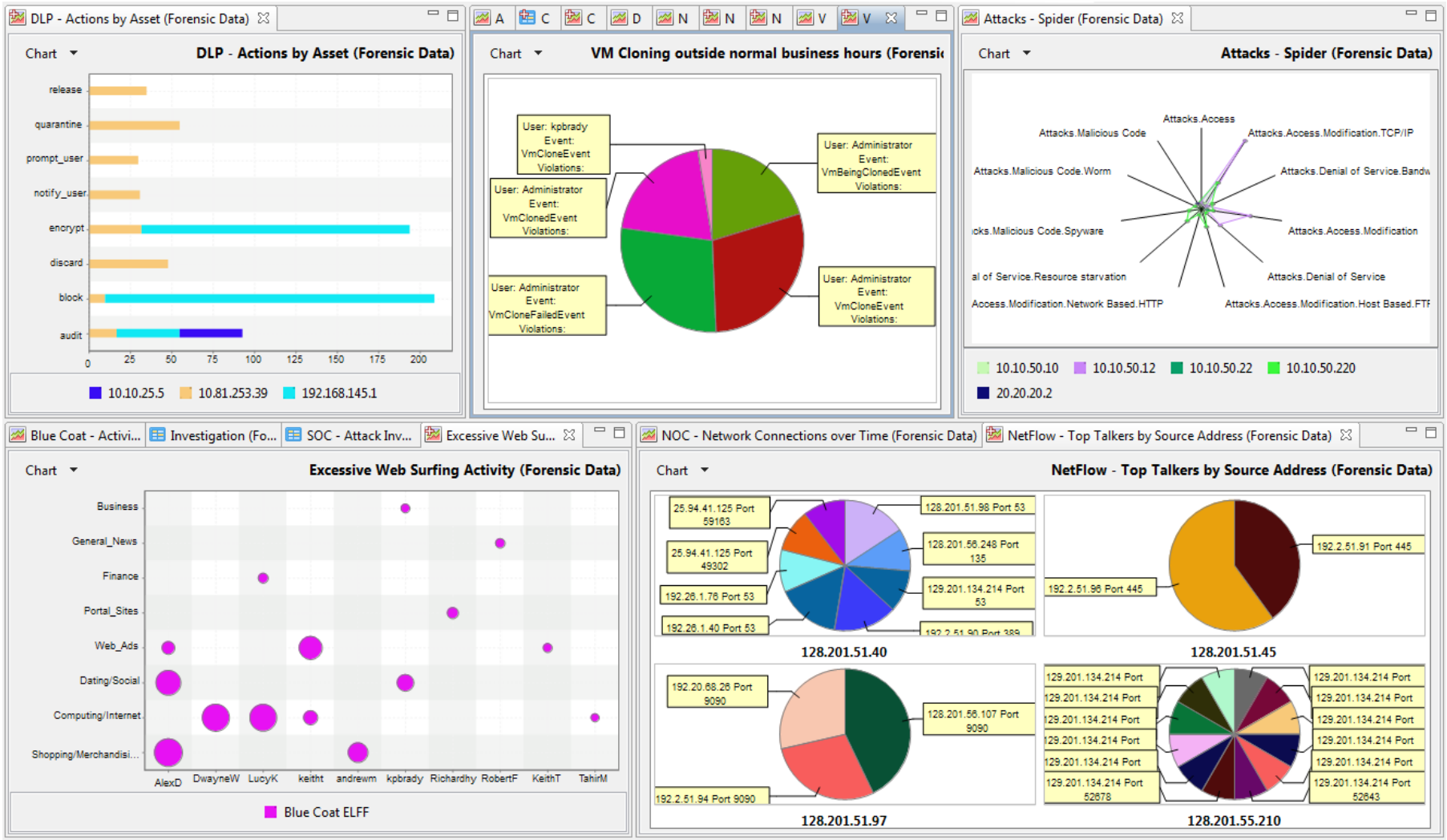
Turn real time events, *e.g. threats*, into actionable data

Create a closed-loop incident handling process

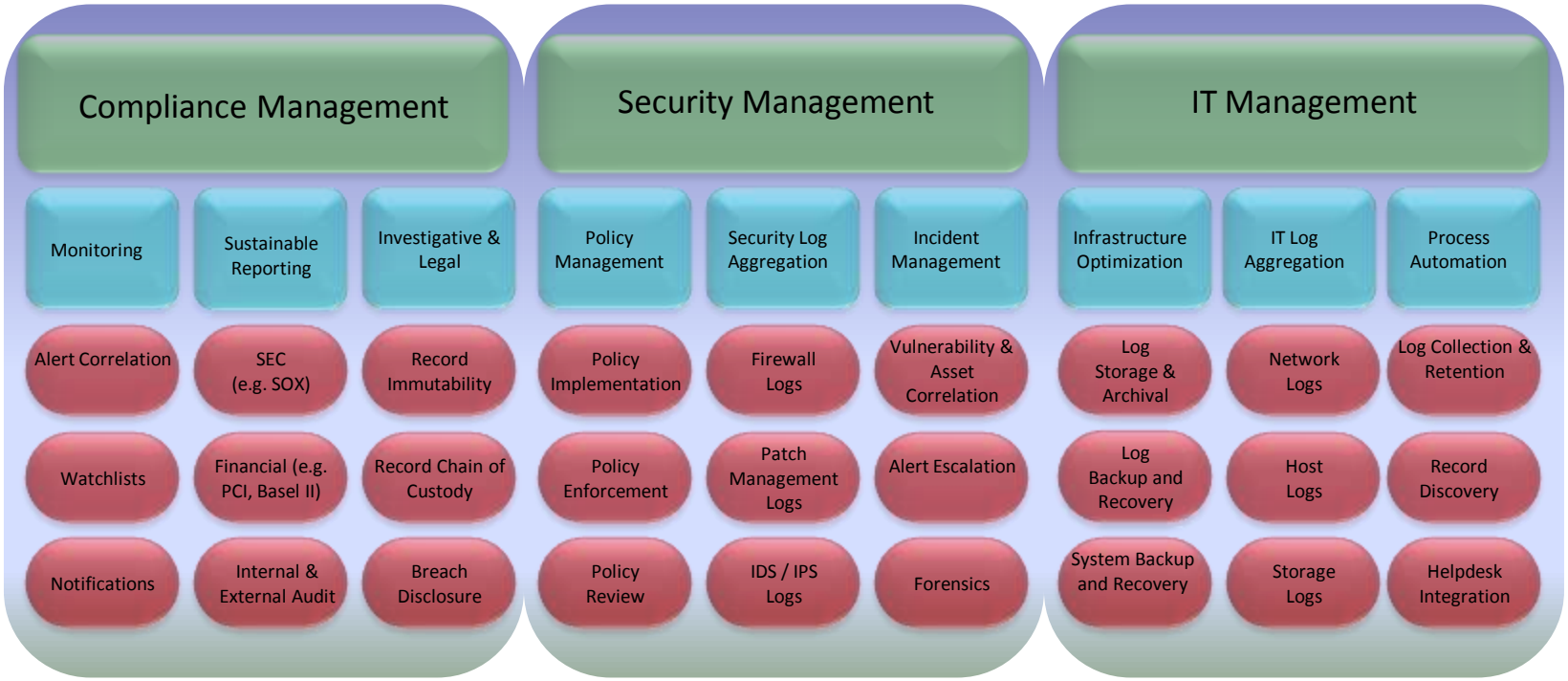
Report on the effectiveness of security management



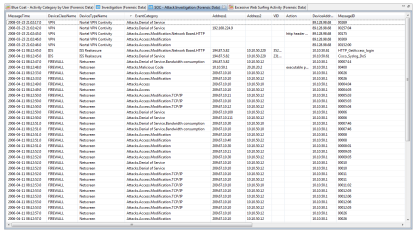
Krok 2: SIEM/SOC Dashboard

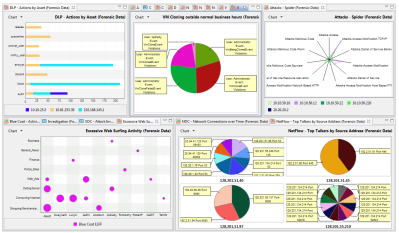


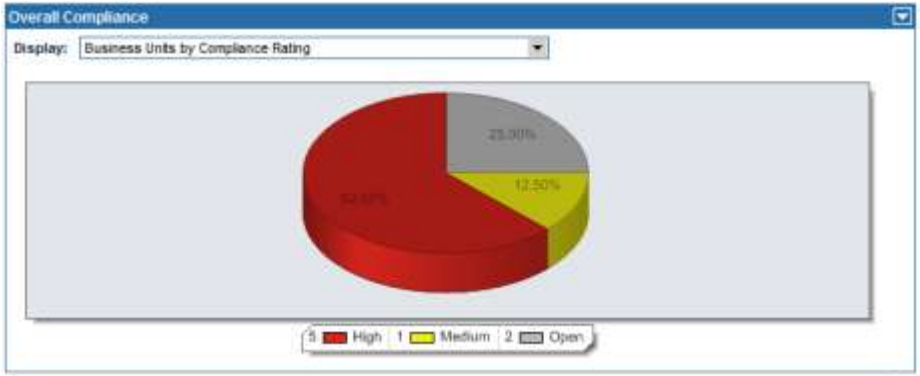
Možnosti současných SIEM

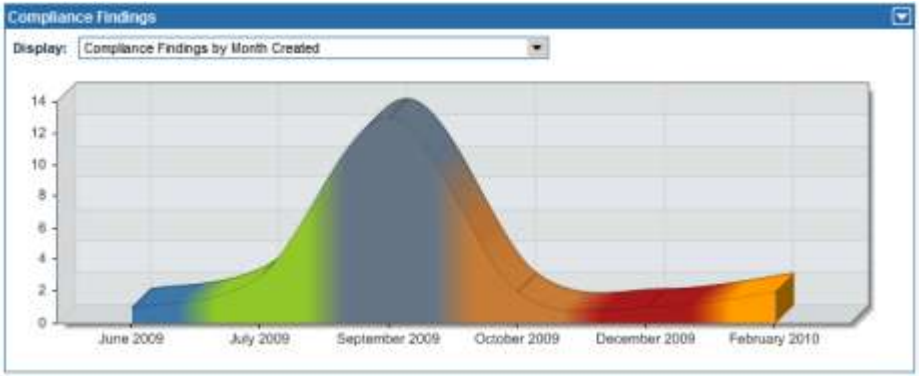


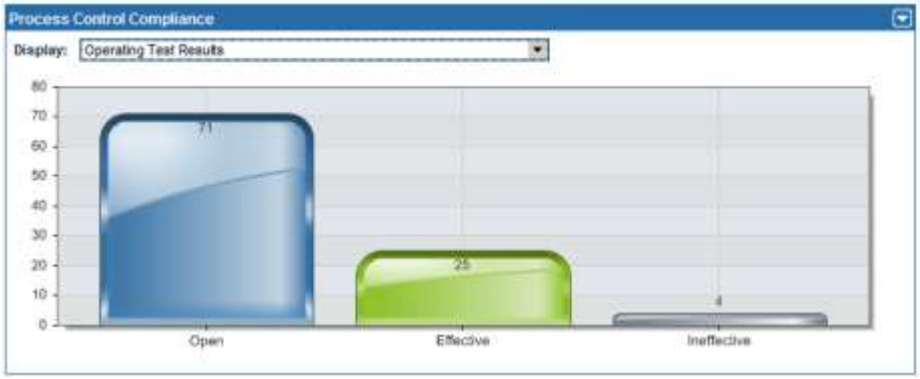
Krok 3: Integrace s eGRC

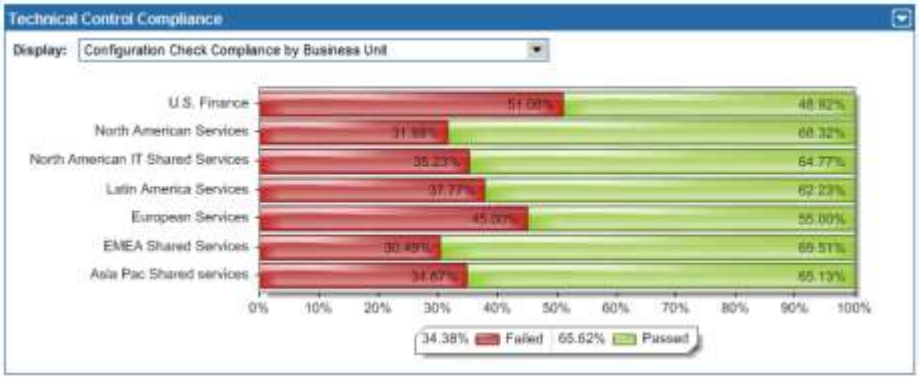












eGRC umí zodpovědět ...

- Je celé moje snažení efektivní?
- Podporuji klíčové procesy podniku?

Shrnutí

- Pouhý sběr logů (log collection) zdaleka nestačí na smysluplný monitoring.
- SIEM s možnostmi SOC je pro většinu středních institucí dostačující.
- Velké firmy využijí navíc eGRC pro integraci SOC do celkového obchodního a procesního pohledu.
- SIEM, SOC a eGRC se budou stále více integrovat -> balíková řešení.

SECURITY 2011

19. ročník konference o bezpečnosti v ICT

Děkuji za pozornost.

David Matějů

RSA, The Security Division of EMC

david.mateju@rsa.com