net pointers communications

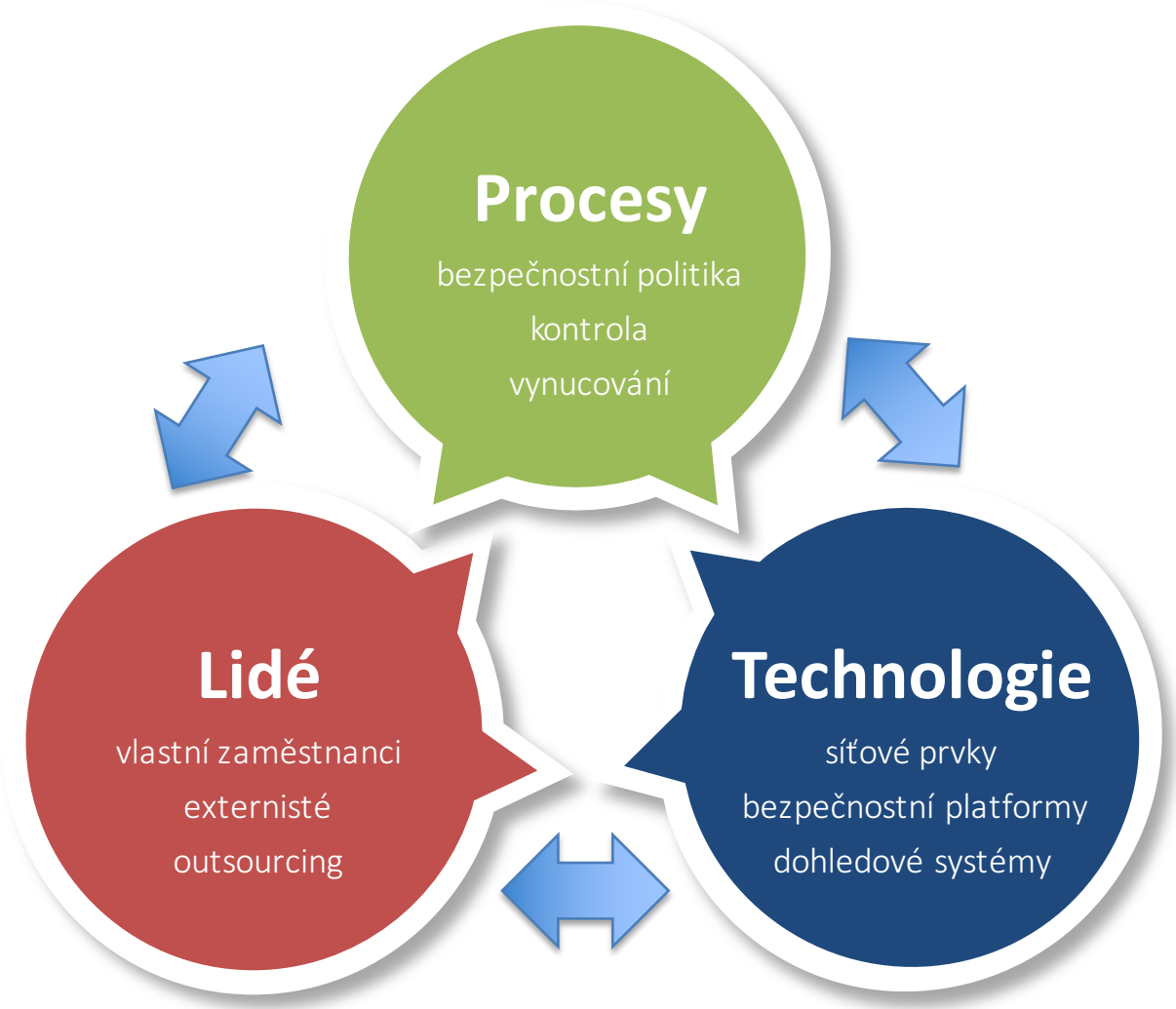
Bezpečnost není o produktech, ale o přístupu a zkušenostech

Martin Půlpán
CEO net.pointers s.r.o.
martin.pulpan@pointers.cz

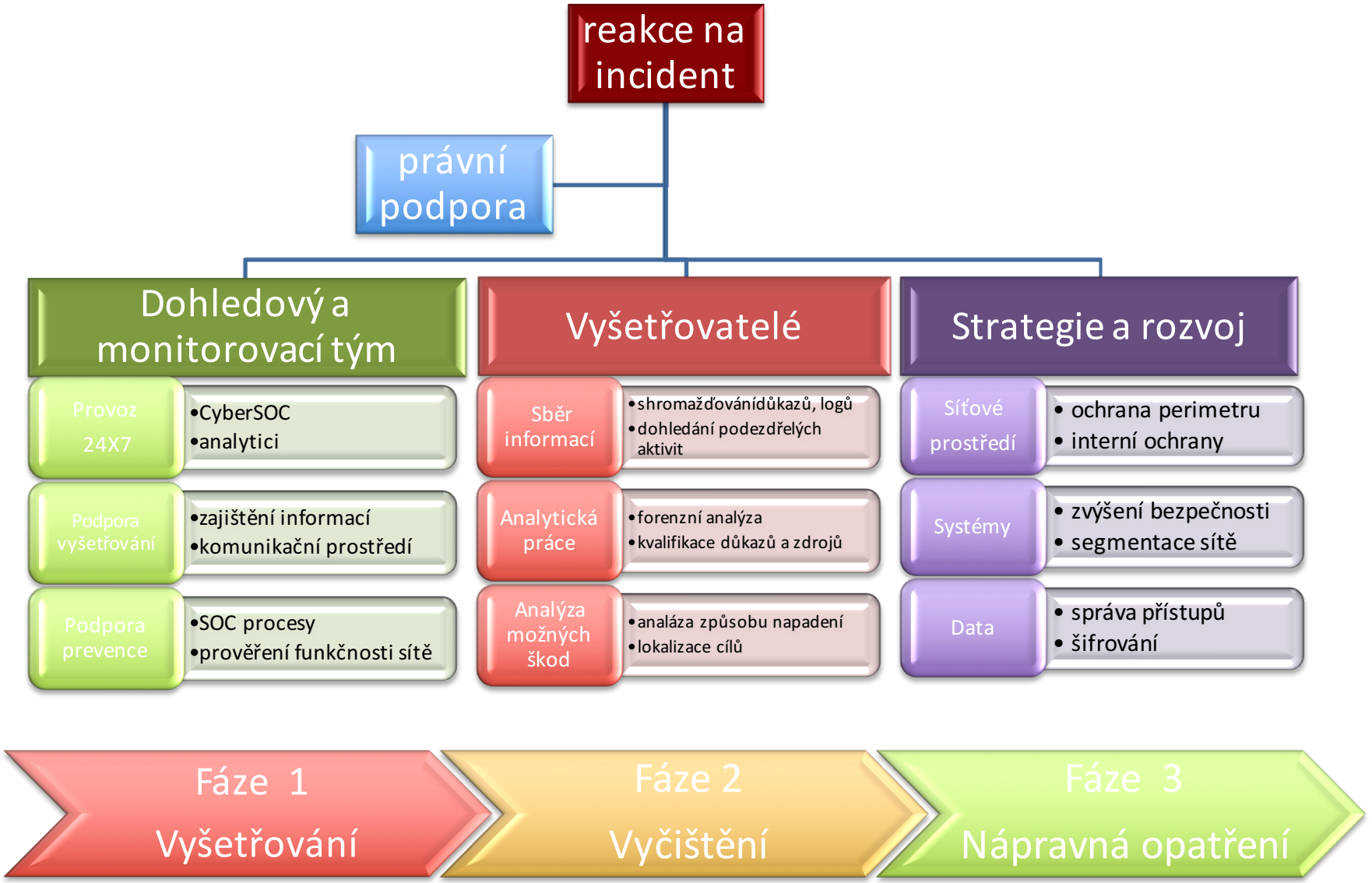
Kdo jsme?

- odborníci na kybernetickou bezpečnost
- největší experti na DDoS ochranu v regionu
  - naše řešení chrání jen v CZ více jak 700Gb/s Internetové konektivity
- specializujeme se na řešení proti APT útokům
  - vizibilita datových toků
  - detekce neznámého malware
  - ochrana citlivých dat
- flexibilita a inovace
- integrace a vlastní vývoj (integrační nástroje, vlastní bezpečnostní platformy)

IT (ne)bezpečnost



Řešení incidentů



Lidé

- stavájící zaměstnanci zakazníka s odbornou podporou partnera
- rozvoj a edukace vašich zaměstnanců
- řešení kapacitních problémů (subdodávka, outsourcing)
- kapacitní plánování IT bezpečnosti
- definice rolí, požadavků, plány osobního rozvoje
- spolupráce na náboru, hledání vhodných lidí

Procesy

- otestování připravenosti (war game)
- hledání problematických míst, zdokonalení systému
- definice a optimalizace procesů IT bezpečnosti
- oddělení neslučitelných funkcí
- definice a optimalizace procesů pro Security Operations Centre (SOC), Computer Security Incident Response Team (CSIRT), Computer Emergency Response Team (CERT)
- kontrola a vynucování bezpečnostních politik

Terminologie

- **SOC (Security Operations Centre)**
  - centrální místo v organizaci, fungující 24x7 a proaktivně sledující stavy IT prvků s cílem eliminovat bezpečnostní rizika
- **CSIRT/CERT (Computer Security Incident Response Team/Computer Emergency Response Team)**
  - team, který řeší v případě potřeby konkrétní bezpečnostní incidenty v počítačových sítích příslušné organizace

Technologie

- nástroje pro dosažení cíle – minimalizace rizik
- audit topologie komunikačních kanálů z pohledu (ne)bezpečnosti
- integrace a propojení IT bezpečnostních systémů
- security BigData

Shrnutí

- pomůžeme vám připravit se na bezpečnostní incident
- naučíme vás co dělat během bezpečnostního incidentu
- pomůžeme vám vyřešit dopady
- jsme partnerem pro dlouhodobou a systematickou prevenci (lidé, procesy, technologie)

Otázky a odpovědi?

Děkuji za pozornost!