Auditing, monitoring, logy

Systém bez logů a auditních záznamů je bez paměti – nemůže reagovat na vlivy vnějšího prostředí
Data v systému bez auditních záznamů nemohou být důvěryhodná
Systém, který není monitorován nemůže být spolehlivý

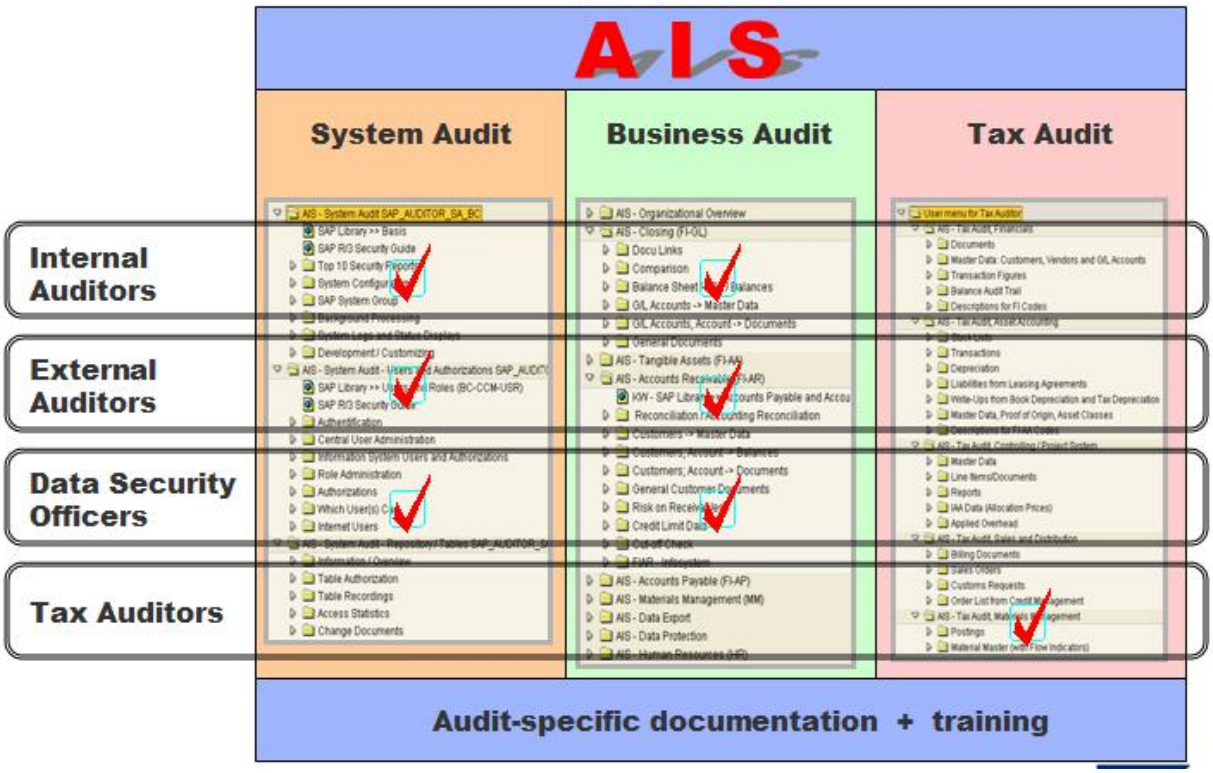
principiálně existují dva druhy logů, které ale společně umožňují zvládat bezpečnostní incidenty:

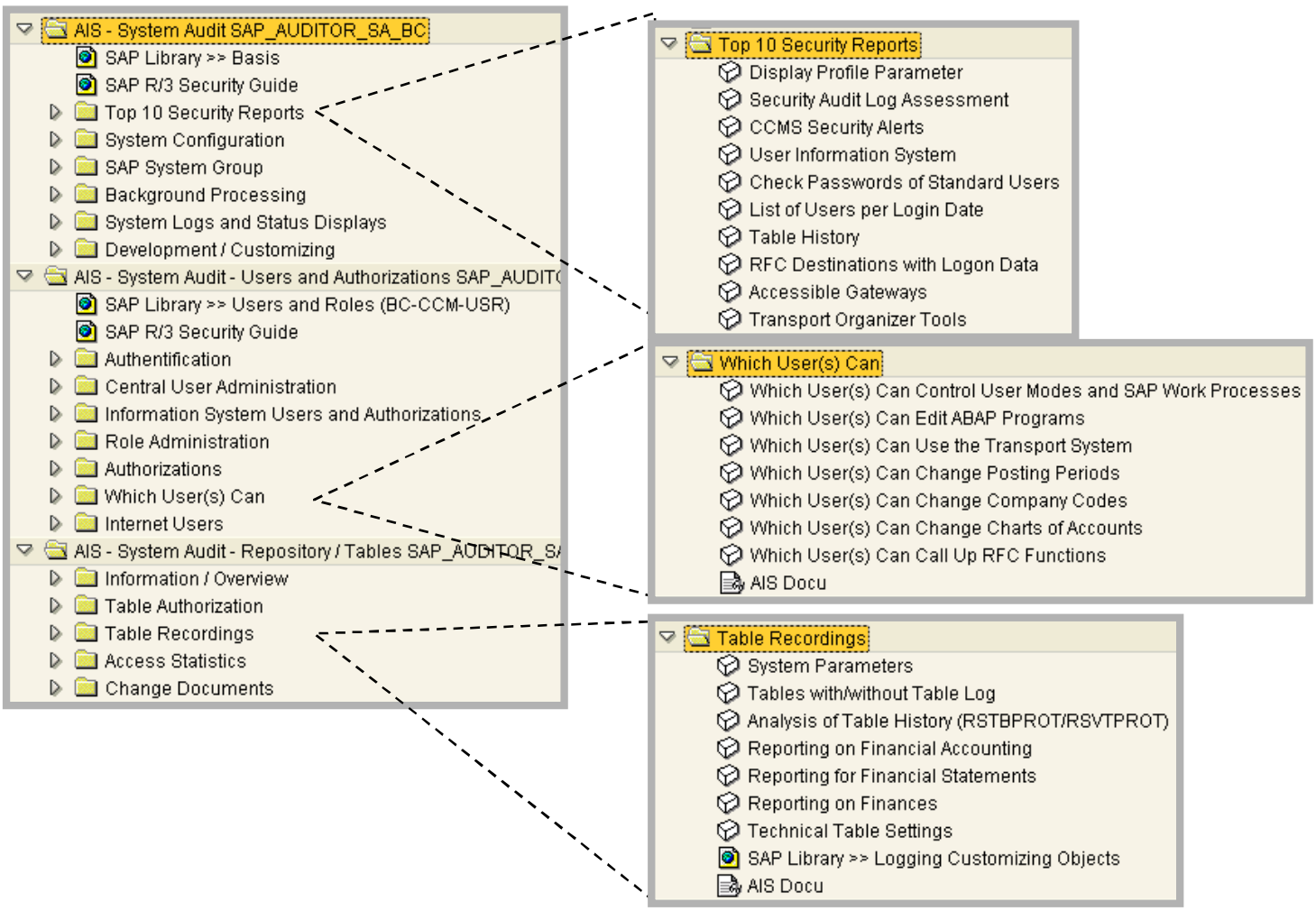
- auditní logy
- provozní logy (redo logy, historie provozních parametrů, ...)

Požadavky na auditní logy:

- zachycení dat důležitých pro detekci připravovaného incidentu
- uchování všech informací pro rekonstrukci průběhu napadení
- spolehlivost informací (tj. “nepřepisovatelnost” logu)
- úplnost logu – tj. že pokrývá všechny operace, které jsou z hlediska bezpečnosti relevantní

Příklad: systémový audit SAP





Požadavky na provozní logy

- úplnost
- odolnost vůči chybám HW - podpora zotavení

Správa logů

Analýza logů
prvním problémem integrace vznikajících logů
musí být soustavná a pravidelná

- prahy (tresholds)
- trendy,
- grupování

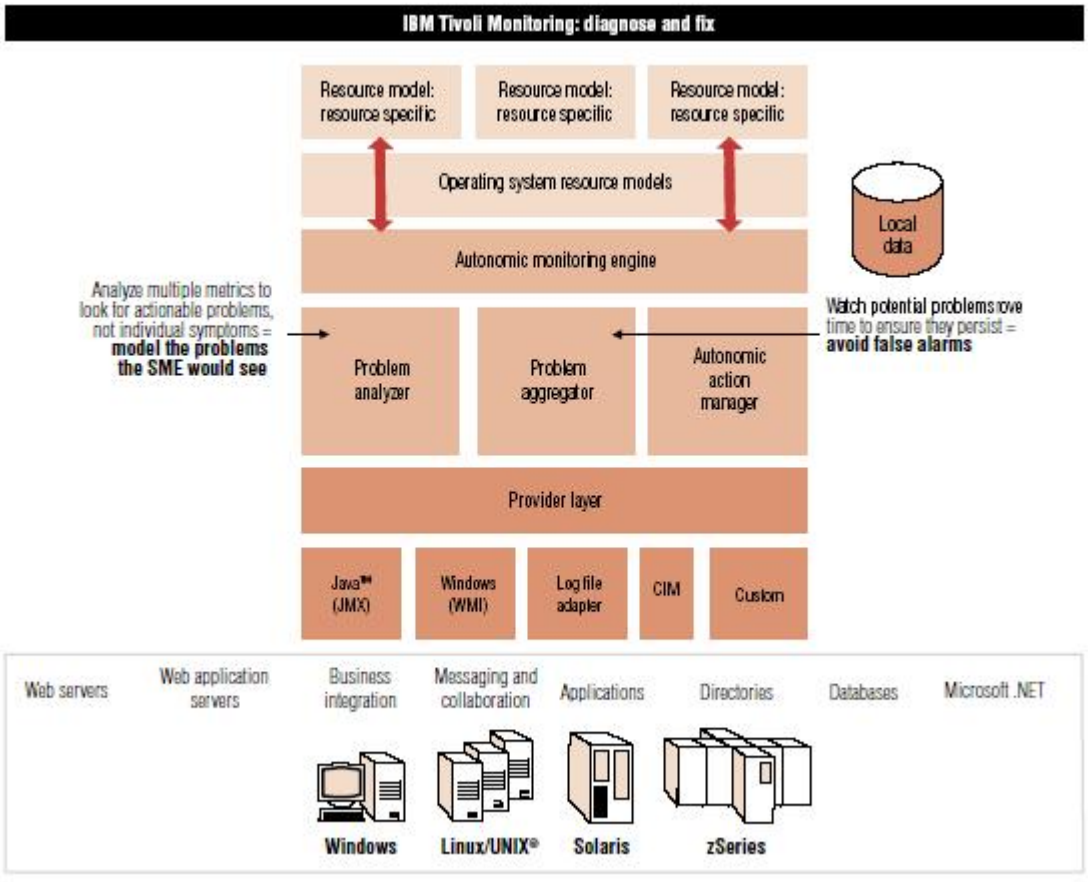
k dispozici celá řada nástrojů na automatizovanou analýzu:

- Security Manager (NetIQ);
- ESM/Security Management System (Symantec);

- Network Security Manager, (Intellitactics);
- Open e-Security Platform (eSecurity);
- Netcool/OMNIbus (Micromuse);
- eTrust (CA);
- Tivoli (IBM);
- NetForensics (netForensics);
- ArcSight (ArcSight);
- Caltarian (RipTech);
- ePolicy Orchestrator (McAfee);
- bv-Control, (BindView);
- Private I Intelligence Suite (OpenSystems).

IDS (intrussion detection system), IPS (... prevention...) systémy – lze detekovat útok před tím, než je skutečně realizován na základě vyhledávání vzorů chování, které charakterizují časné fáze útoku:
port scany
neúspěšné pokusy o příhlášení
zasílání vadných paketů
pokus o spuštění neautorizovaného SW

Příklad komplexního monitoringu “enterprise” úrovně:
IBM Tivoli monitoring



Alerting

proaktivní bezpečnost – systém sám upozorňuje na nebezpečné stavy
rychlá identifikace (potenciálních) problémů
schopnost analyzovat, co se děje, nebo co hrozí