



ENGAGE

FORTINET ADVANCED PARTNER

Integrator

Microsoft
Partner



Gold Application Development
Gold Cloud Platform
Gold Cloud Productivity
Gold Collaboration and Content
Gold Datacenter

Microsoft
Partner



Gold Messaging
Gold Security
Gold Windows and Devices

Microsoft
Partner



Silver Communications
Silver Data Analytics
Silver Enterprise Mobility Management
Silver Project and Portfolio Management
Silver Small and Midmarket Cloud Solutions

Kybernetická bezpečnost

Jak na řízení zranitelností a bezpečnostních událostí

Ladislav Šolc
Tomáš Polák

Kdo jsme?

Zaměřujeme se na poskytování expertních služeb v oblasti IT již 15 let.

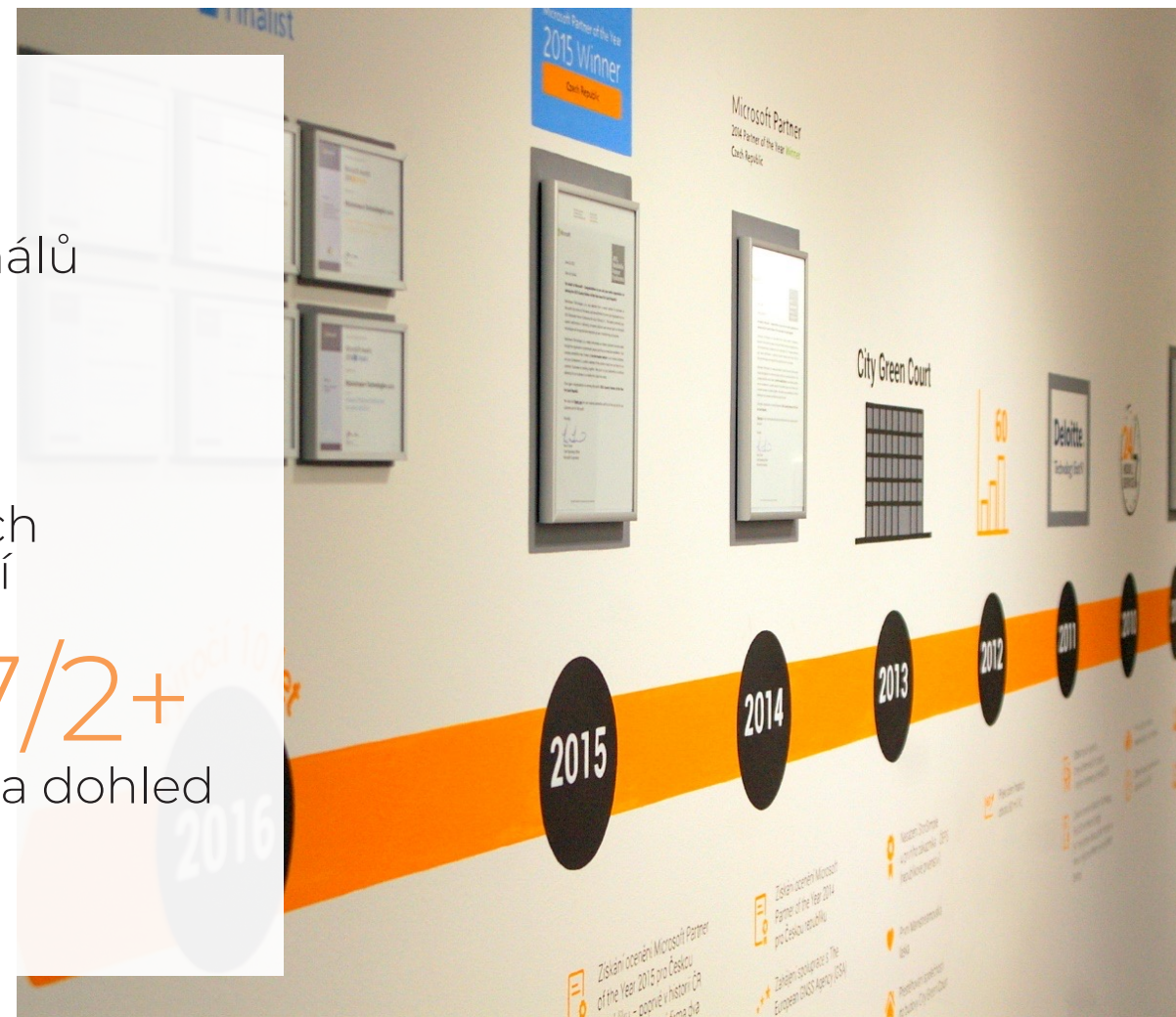
Zákazníkům v souladu s našimi firemními hodnotami nabízíme rychlost, kvalitu a expertní znalost.

Máme prověrky na stupeň TAJNÉ.

70+
profesionálů

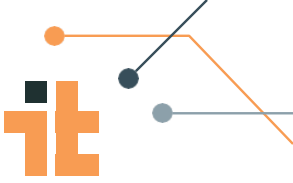
30+
expertních
certifikací

24/7/2+
Podpora a dohled



Kybernetická bezpečnost

Přístup k řešení bezpečnostních výzev



- » Správa zranitelností pod kontrolou
 - » Formou služby na platformě Qualys
- » Sledování zranitelností a aktivit
 - » Být v souladu se ZoKB, GDPR, ISO a těšit se na NÚKIB
 - » Lepide Data Security
- » Stačí otevřít oči
 - » Rychlé zmapování zranitelností, zabezpečení identit
 - » Fortinet CTAP, Qualys, další nástroje
 - » AD Security assessment

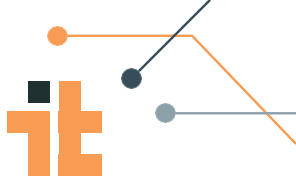
FORTINET



Lepide



Řízení zranitelností jako služba



» Qualys

» Gartner 2020 – nejlepší zákaznická volba pro řízení zranitelností



» Řízená služba správy zranitelností

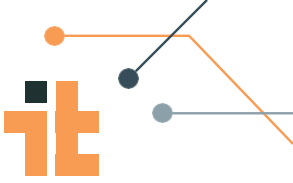
» Detekce chybějících záplat, aktuálních zranitelností a chybné konfigurace

» Online dashboard

» Reporting

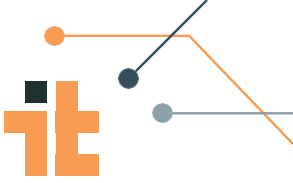
» Odstranění





- » Nasazení služby
 - » Instalace a konfigurace technických prostředků v prostředí zákazníka
 - » Zpřístupnění reportingového portálu
 - » **Workshop:** Stanovení Patch Management procesu
 - » Úvodní inventarizace a klasifikace IT prostředků
 - » Úvodní zpráva o stavu zranitelností
 - » **Workshop:** Expertní posouzení zranitelností

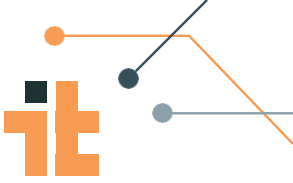




- » Pravidelná detekce a reporting
 - » 24/7 přístup do online dashboardů
 - » Pravidelné skenování IT prostředků
 - » Automatická detekce zranitelností a klasifikace jejich závažnosti
 - » 6x ročně: Reporting a **expertní workshop** nad nálezy a **plán odstraňování**
 - » Proaktivní upozornění na výskyt kritických zranitelností



Řízení zranitelností jako služba

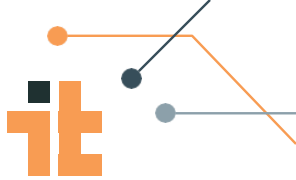


- » Odstraňování zranitelností
 - » 6x ročně: Plán odstraňování zranitelností
 - » Expertní prioritizace zranitelností
 - » Expertní technická spolupráce na nasazení záplat
- » Další součinnost
 - » Technická asistence
 - » Konzultace bezpečnostních expertů



Kybernetická bezpečnost

Lepide Data Security Platform



- » Lepide Data Security Platform (DSP)
 - » Detekce ohrožení zevnitř
 - » Dosažení shody s normami a regulacemi – GDPR
 - » Automatizovaná klasifikace dat
 - » Analýzy chování uživatelů s detekcí anomálií
 - » Detekce změn ve formě auditu
 - » Všechny aktivity správců a dodavatelů

GDPR Reports / All Modifications in Active Directory

Server Name Who Where
Object Path When Criticality
Object Type Operation

Drag a column header here to group by that column

Object Path	Who	When	Operation
User1@saramsoft.on...	karter@sasa	8/27/2020 10:5	Member Ad...
User2@saramsoft.on...	karter@sasa	8/27/2020 10:5	Updated

Over Exposed Data

File Server(s) Owner

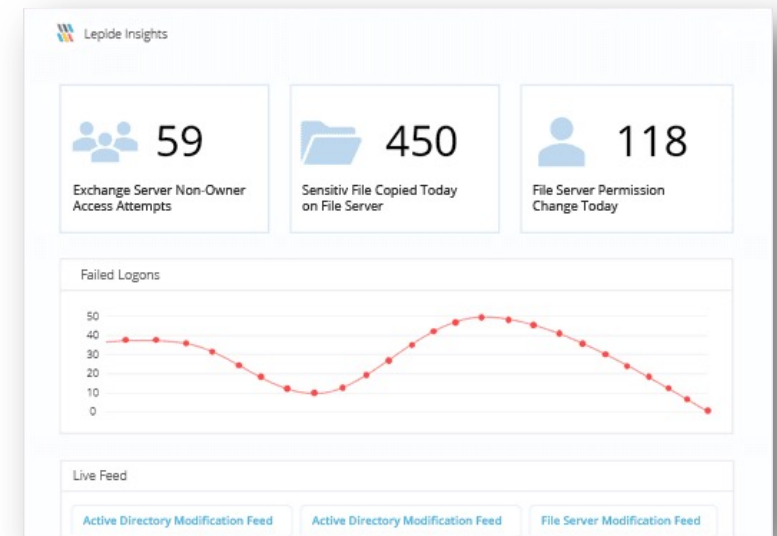
Open Shares – File Server – dmd01

Share Folder	Path	Owner	Open To
Designs	C:\Data\Designs	dmd01\Amins	DMD01\Users
Finance	C:\Data\Finance	dmd01\Amins	DMD01\Users
Sales	C:\Data\Sales	dmd01\Amins	DMD01\Users



Kybernetická bezpečnost Lepide DSP

- » Přednosti a hlavní rysy
 - » Snadný audit a monitoring změn
 - » Sledování dění v IT systémech
 - » Upozornění v reálném čase
 - » Validace nastavení zabezpečení
 - » Přehled o přístupech
 - » Vysoká kontrola nad privilegovanými účty



Lepide Trust interface showing account permissions and file access details.

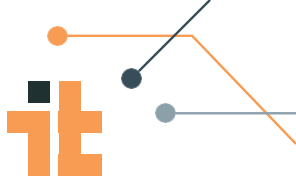
Account (Principal)	Effective Permission	Icon 1	Icon 2	Icon 3	Icon 4
Lpde1\jill	Full Control	✓	✓	✓	✓
Lpde1\Paul	Full Control	✓	✓	✓	✓
Lpde1\Bill	Full Control	✓	✓	✓	✓

Files in Folder : Accounts

File Name	Content Type	Access Count
Clients - Copy (2).txt	Credit Card - Visa + UK Phone	1 + 1 + 1 + 1 + 1
Clients.txt.encrypt	Credit Card	100
Customer details.png	No Sensitive Content	N/A
Database.doc	Credit Card + SSN	100 + 500

Kybernetická bezpečnost

Lepide DSP



» Přednosti a hlavní rysy

» Stovky hotových reportů (300+) pro řadu platforem

» Microsoft AD, souborové servery, SQL, Exchange, GPO, M365 vč. Teams a OneDrive



Active Directory



File Server



Exchange Server



SharePoint Server



SQL Server



Office 365



Azure AD



OneDrive



Amazon S3



MS Teams



Dropbox



G Suite



VMWare

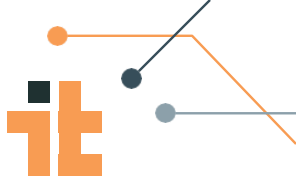


EMC Storage



Kybernetická bezpečnost

Lepide DSP

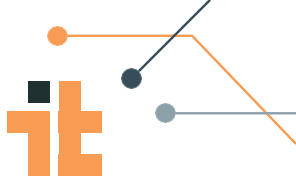


- » Přednosti a hlavní rysy
 - » Stovky hotových reportů (300+) pro řadu platforem
 - » Microsoft AD, souborové servery, SQL, Exchange, GPO, M365 vč. Teams a OneDrive
 - » Auditní data na jednom místě
 - » Možnost vrácení změn – rollback
 - » Automatizované reakce na události
 - » Klasifikace dat a audit GDPR
 - » Základní nasazení v řádu dnů

Permissions on Folder: \\dmd01\Company_Share\Accounts

Account (Principal)	Effective Permission	Folder	File	File	File
Lpde1\Jill	Full Control	✓	✓	✓	✓
Lpde1\Paul	Full Control	✓	✓	✓	✓
Lpde1\Bill	Full Control	✓	✓	✓	✓
Lpde1\Steve	Full Control	✓	✓	✓	✓
Lpde1\Sharon	Full Control	✓	✓	✓	✓
Lpde1\Shelly	Full Control	✓	✓	✓	✓
Lpde1\Philip	Full Control	✓	✓	✓	✓
Lpde1\Danny	Full Control	✓	✓	✓	✓
Lpde1\Aidan	Full Control	✓	✓	✓	✓





» Jednorázové zmapování zranitelností

- » Kontrola zabezpečení identit AD (AD Security Healthcheck)
- » Síťový sken zranitelností - Qualys
- » Výsledná podrobná zpráva
- » Pracnost do dvou týdnů
- » Cena do 250.000 Kč

» Jednorázová analýza síťového provozu

- » Zapůjčení Fortinet firewallu
- » Analýza emailového provozu
- » Analýza návštěvnosti internetu
- » Výsledná podrobná zpráva
- » Pracnost do dvou týdnů
- » Cena do 50.000 Kč

» Více podrobností, ukázky výstupů, demo a další informace

- » Dejte nám prosím vizitky

