Máte SIEM pod kontrolou?

5 signálů podle kterých to poznáte

✓	✗
Alerty mají jasného vlastníka a postup řešení.	Alerty se hromadí a nikdo je systematicky nevyhodnocuje.
Počet falešných upozornění postupně klesá.	Stejná chybná upozornění se opakují i týdny po nasazení.
Průběh incidentu dokážete dohledat během několika minut.	Část logů musíte hledat ručně v různých systémech.
Na výpadek sběru logů jste upozorněni automaticky.	O chybějících datech se dozvíte až zpětně.
Pravidla odpovídají aktuálnímu prostředí.	SIEM pracuje se zastaralými nebo neexistujícími systémy.

Ověřte stav svého SIEM

Sbíráme správná data?	Detekujeme a reagujeme?	Jsme připraveni na audit?
Máme centrálně dostupné logy z identity, firewallů, VPN a klíčových serverů?	Máme nastavená pravidla pro nejčastější scénáře útoků a bezpečnostních incidentů?	Dokážeme během několika minut dohledat konkrétní přihlášení nebo změnu v systému?
Ukládají se logy mimo zdrojové systémy?	Má každý typ alertu definovaný postup řešení?	Pravidelně ověřujeme postupy reakce na bezpečnostní incidenty?
Jsou logy chráněny před dodatečnými úpravami nebo smazáním?	Jsme upozorněni na výpadek sběru logů?	Evidujeme a dokumentujeme schválené výjimky z pravidel?
Víme, jaký objem dat logy generují a zda tomu odpovídá kapacita úložiště?	Aktualizujeme pravidelně agenty a kontrolní pravidla?	Máme k dispozici podklady potřebné pro audit nebo kontrolu?
Máme definovaná pravidla pro uchovávání jednotlivých kategorií logů?	Vyhodnocujeme a upravujeme detekční pravidla průběžně?	**Odhalili jste slabá místa?** Napište nám a projdeme to společně. **www.master.cz**