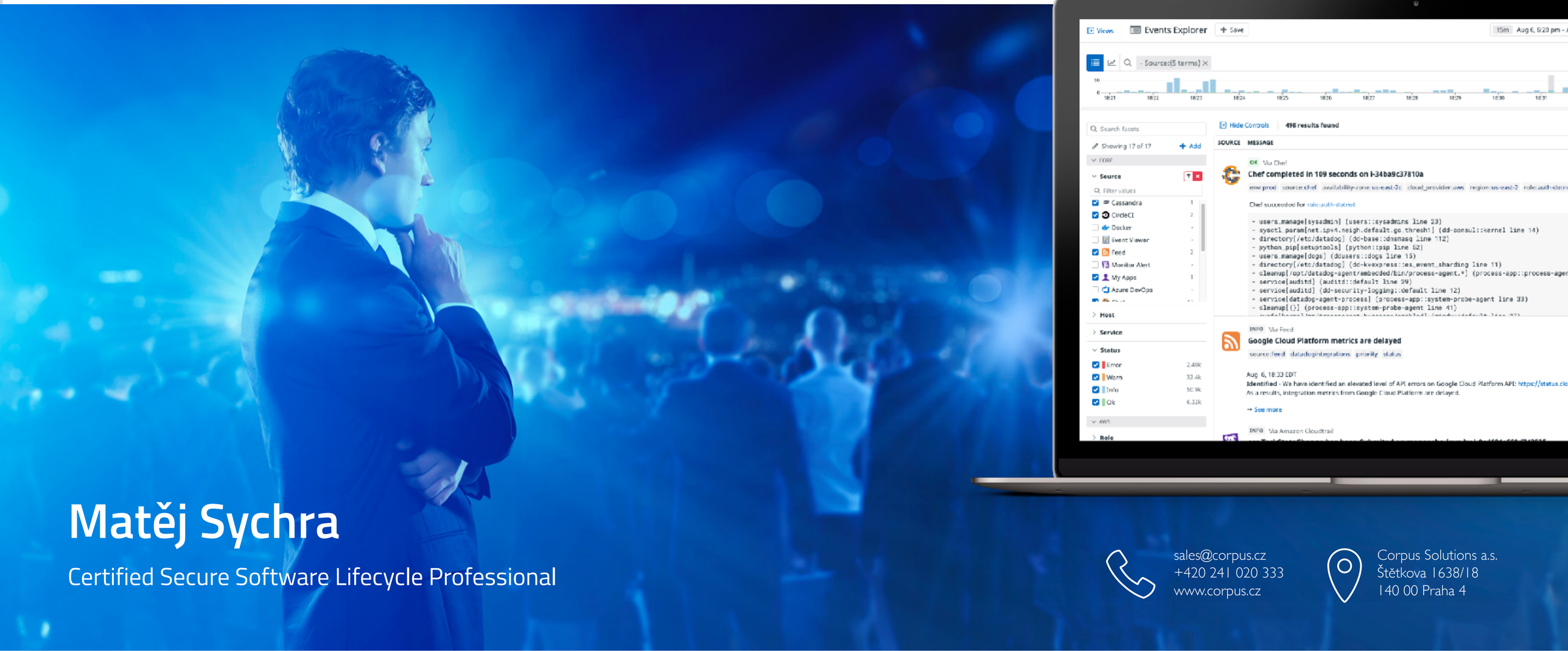
Aplikační bezpečnost vs. SOC

CORPUS SOLUTIONS
CYBERSECURITY EXPERTS

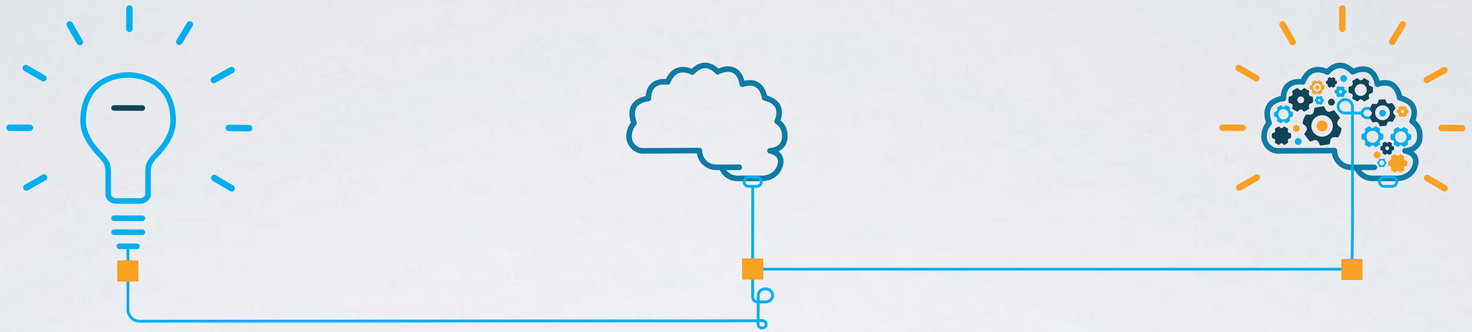


Matěj Sychra

Certified Secure Software Lifecycle Professional

sales@corpus.cz
+420 241 020 333
www.corpus.cz

Corpus Solutions a.s.
Štětkova 1638/18
140 00 Praha 4



Jak na Security Operations Center (SOC) vs. vývoj a provoz softwarových aplikací

Aplikace z pohledu SOC

SITUACE V RÁMCI VÝVOJE A DOHLEDU APLIKACÍ

- Nejvíce kybernetických útoků se statisticky odehrává právě na aplikační vrstvě.
- Náklady na provoz SOC jsou vysoké. SOC musí dobře rozumět prostředí, které chrání.
- Pomáháme upravit procesy bezpečného vývoje tak, aby umožnily efektivní spolupráci v průběhu životního cyklu aplikace.

Aplikace z pohledu SOC

SITUACE V RÁMCI VÝVOJE A DOHLEDU APLIKACÍ

Charakteristika SOC/SIEM

- Velká infrastruktura
- Velký objem logů
- Vyžaduje „visibilitu“ do aplikací (logy, terminace SSL)
- Vyžaduje znalost datových toků, umístění dat a stávajících opatření
- Vysoká finanční náročnost nápravy chyb (ve srovnání s vývojem)

Aplikace z pohledu SOC

SITUACE V RÁMCI VÝVOJE A DOHLEDU APLIKACÍ

Nejčastější nedostatky

- Nejsou zmapována rizika aplikací
- Nejsou zavedeny principy bezpečného vývoje
- Nejsou známy skryté zranitelnosti aplikací (dělají se pouze penetrační testy)
- Nejsou jasně definované požadavky na zajištění provozu (využívají se výchozí nastavení)
- Nejsou k dispozici přehledy životních situací aplikace – co má vlastně SOC monitorovat
- Vývojáři nejsou dostatečně vyškoleni v bezpečnostních tématech (např. co ne-/patří do logu)

Aplikace z pohledu SOC

SITUACE V RÁMCI VÝVOJE A DOHLEDU APLIKACÍ

Co s tím?

> Jedinou výhodou obránce proti útočníkovi je znalost prostředí.

SOC z pohledu vývoje

BEZEČNÝ VÝVOJOVÝ A ŽIVOTNÍ CYKLUS APLIKACE

Využití principů bezpečného vývoje (S-SDLC)

- **Modelování hrozeb** – komunikace bezpečnostně relevantních informací napříč týmy, registr rizik a jejich řízení
- **Bezpečnostní code-review** – revize zdrojového kódu z bezpečnostního pohledu
- **Statická analýza** – automatizace v oblasti analýzy bezpečnosti zdrojového kódu
- **Analýza komponent** – tzv. „vulnerability scanning“ na úrovni knihoven a kontejnerů
- **Analýza infrastruktury** – podpora procesů DevSecOps a Continuous Delivery/Deployment

Ukázka zranitelnosti

TEXT4SHELL (CVE-2022-42889)

Text4Shell

Nedávno objevená zranitelnost v knihovně Apache Commons. Přestože tato komponenta je používána v rámci Java/Spring aplikací naprosto běžně, skutečný dopad lze odhalit pouze vhledem do kódu.

- Zranitelná je Apache Commons Text v1.5-1.9 (verze 1.10 je opravená)
- Aplikace musí používat StringSubstitutor
- Aplikace musí akceptovat libovolný vstup řízený útočníkem (používat interpolaci proměnných ${})
- Nelze detekovat pomocí běžných nástrojů OSA/SCA

Ukázka zranitelnosti

TEXT4SHELL (CVE-2022-42889)

http://localhost:8080/vulnerable?requestInput=${script:javascript:java.lang.Runtime.getRuntime().exec('cat /etc/shadow')}

```
@RequestMapping(value = "/vulnerable", method = RequestMethod.GET)
@ResponseBody
public String vulnerable(
  // Výchozí hodnota parametru je použita k demonstraci zranitelnosti
  @RequestParam(defaultValue="${script:javascript:java.lang.Runtime.getRuntime().exec('cat /etc/shadow')}")
  String requestInput
) {
  // Zranitelná metoda importovaná z Apache Commons Text.
  StringSubstitutor interpolator = StringSubstitutor.createInterpolator();

  // Na tomto řádku dojde ke spuštění injektovaného skriptu
  interpolator.replace(requestInput);
```

Efektivní integrace SOC a AppSec

AKTIVITY V OBLASTI BEZPEČNÉHO VÝVOJE A PROVOZU APLIKACÍ

- **Klasifikace** dat a znalost jejich umístění
- **Modelování hrozeb** jako brána v rámci bezpečného vývoje (není model, není release)
- Zjišťování zranitelností v kódu pomocí nástrojů – **SAST/DAST**
- Používání komponent z ověřených zdrojů – **OSA**
- **Automatizace** sledování zranitelností
- **Skenování** během nasazení do provozu (Continuous Integration/Delivery/Deployment)
- **Správné nastavení** prevence a pravidel pro provoz – SIEM
- **Školení vývojářů** – Shift-Left

Děkujeme za pozornost.

CORPUS SOLUTIONS
CYBERSECURITY EXPERTS