initMAX

ISP Alliance 2026

Wazuh pro ISP
Funkce a možnosti

Martin Krupka, initMAX
20. října 2026, Jičín

initMAX

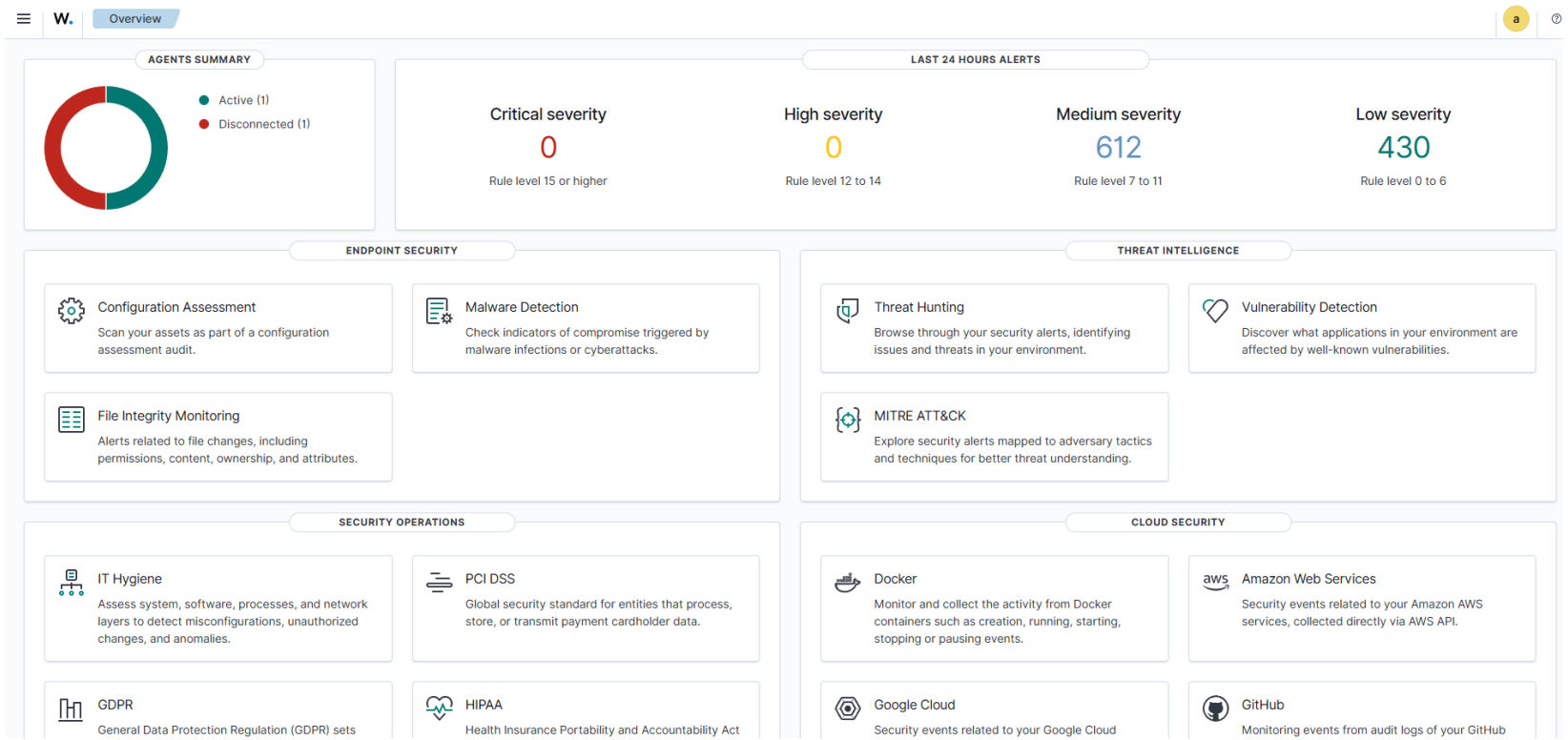
Wazuh v praxi

Bezpečnostní přehled na jednom místě

Wazuh spojuje bezpečnostní události a nálezy ze sledovaných systémů.

Příklad pro ISP

Ranní přehled pro člověka, který má na starosti síť i servery.



Skutečné GUI Wazuh, ukázka výrobce

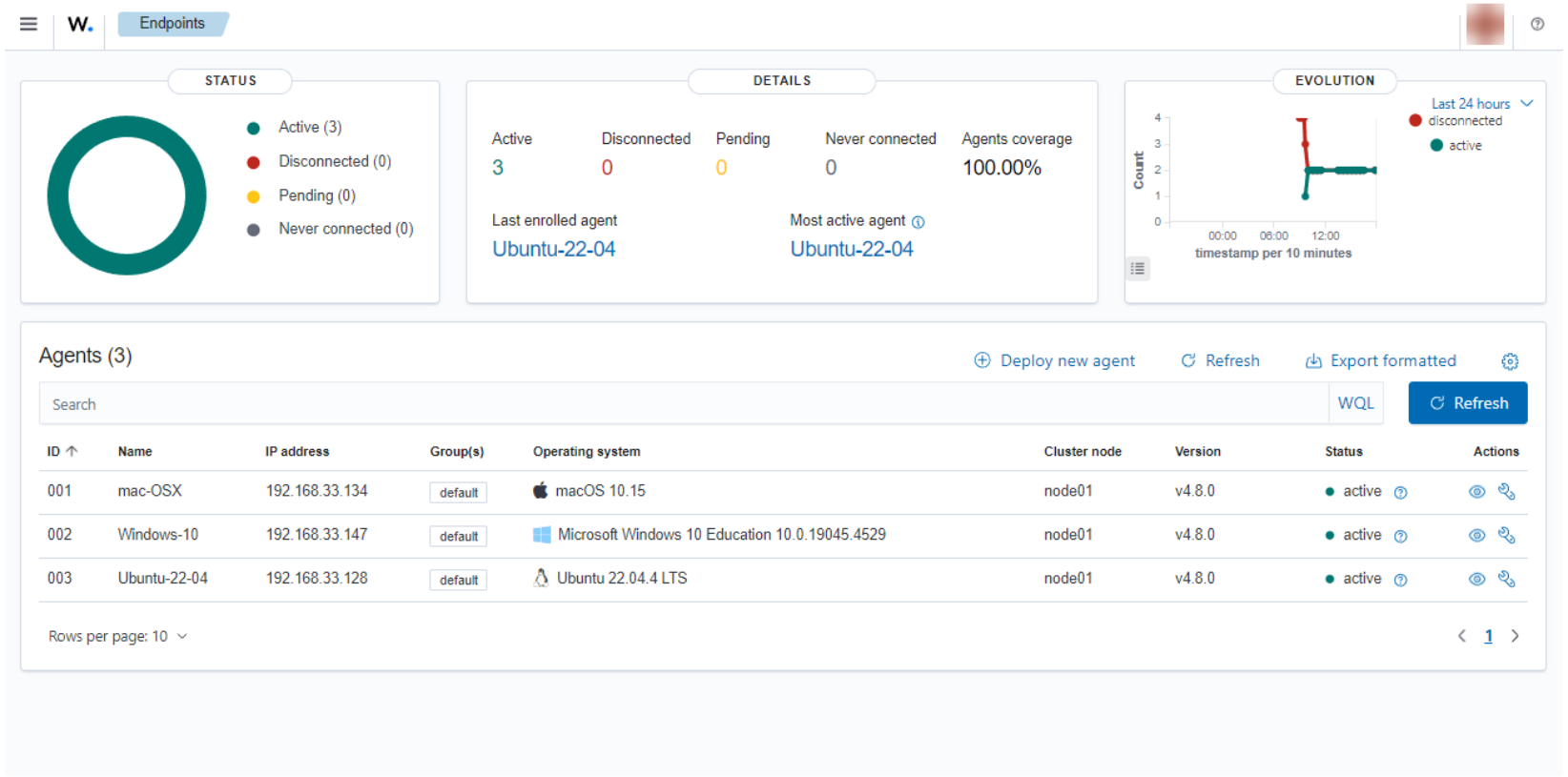
Wazuh v praxi

Pokrytí serverů a pracovních stanic

Přehled registrovaných zařízení a stavu jejich agentů.

Příklad pro ISP

Bastiony, DNS servery, zákaznický portál a notebooky techniků.



Skutečné GUI Wazuh, ukázka výrobce

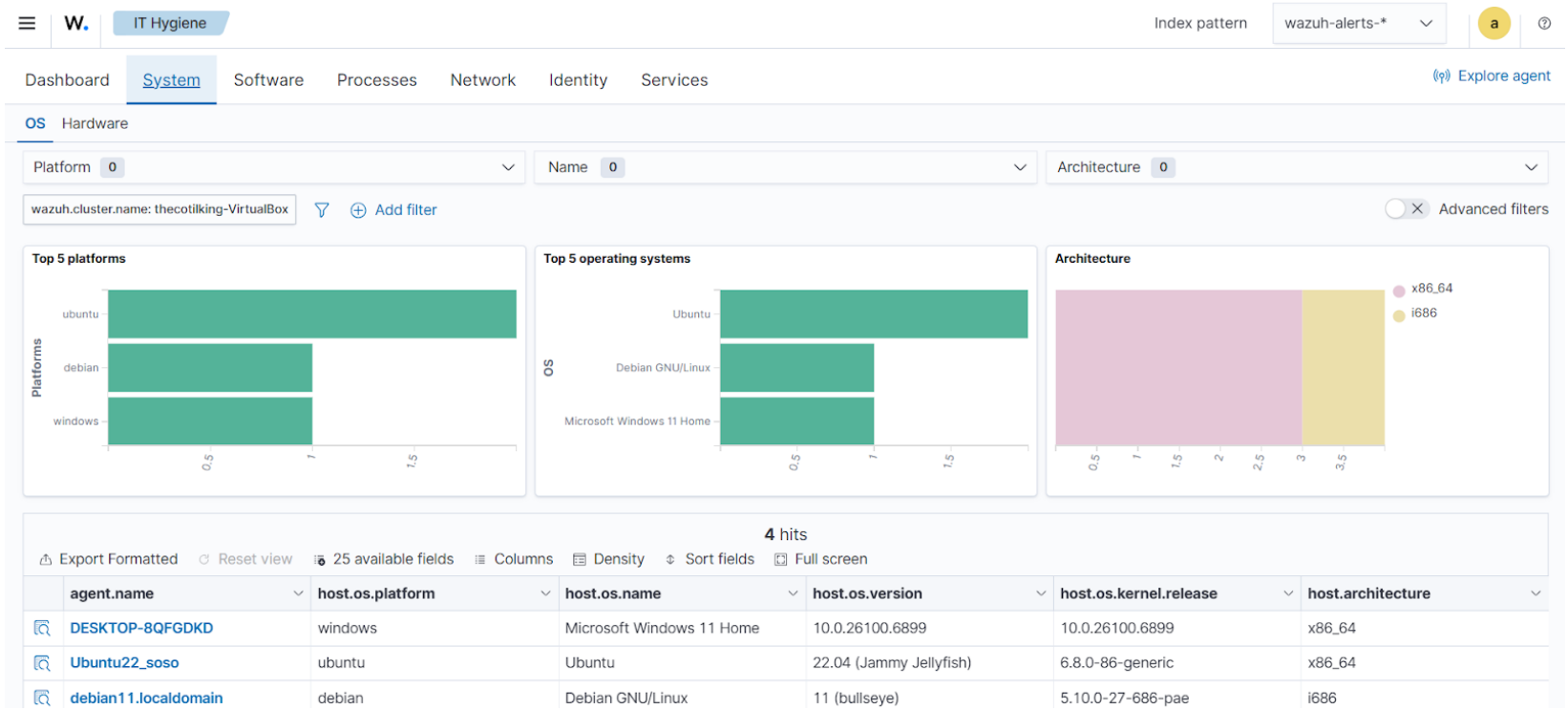
Wazuh v praxi

Inventář systémů

Centrální pohled na operační systémy a hardware.

Příklad pro ISP

Přehled verzí Linuxu na provozních serverech a Windows v kanceláři.



Skutečné GUI Wazuh, ukázka výrobce

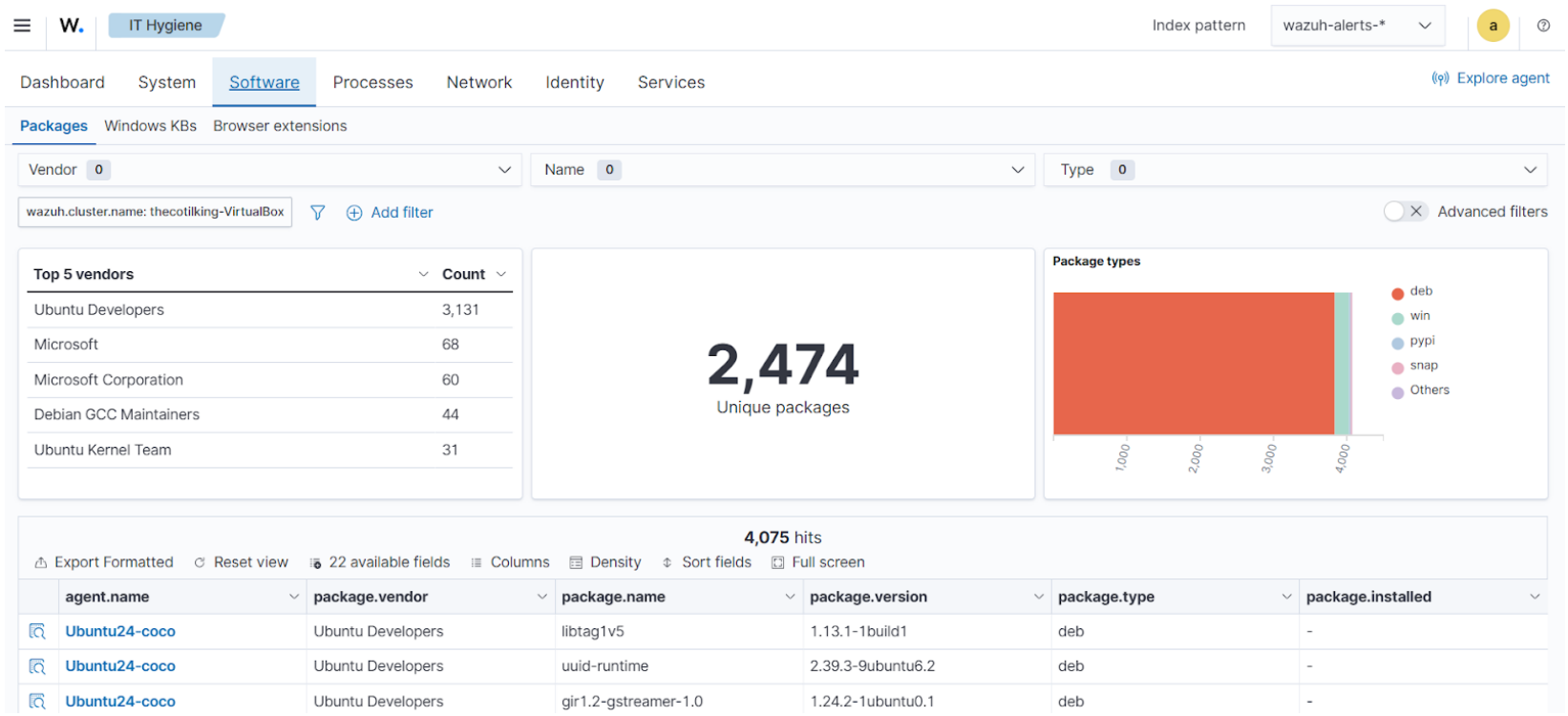
Wazuh v praxi

Instalovaný software

Seznam balíčků a aplikací s vazbou na konkrétní hosty.

Příklad pro ISP

Které naše servery používají konkrétní verzi OpenSSH?



Skutečné GUI Wazuh, ukázka výrobce

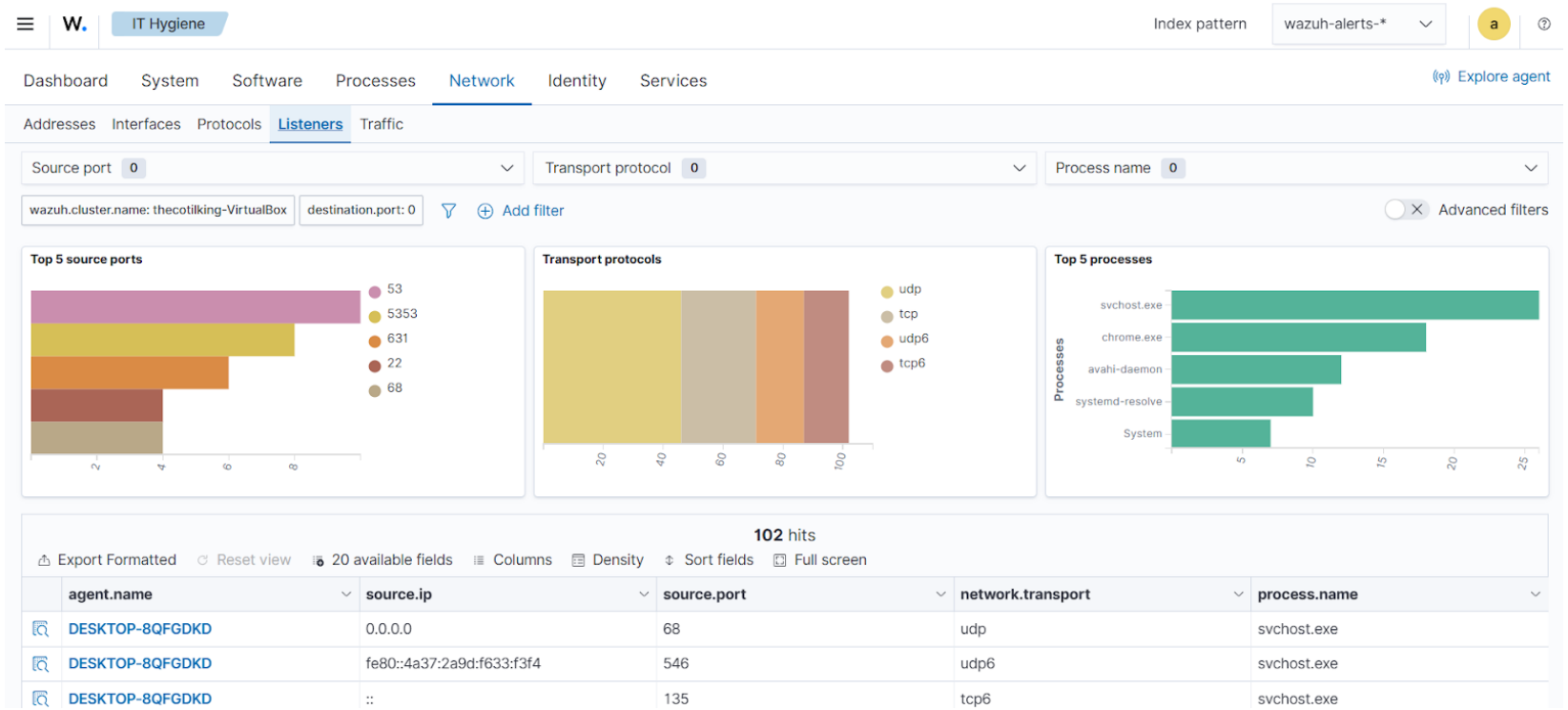
Wazuh v praxi

Služby a síťové porty hostů

Inventář síťových údajů ze sledovaných serverů.

Příklad pro ISP

Kontrola, zda na produkčním DNS serveru neběží další nepotřebná služba.



Skutečné GUI Wazuh, ukázka výrobce

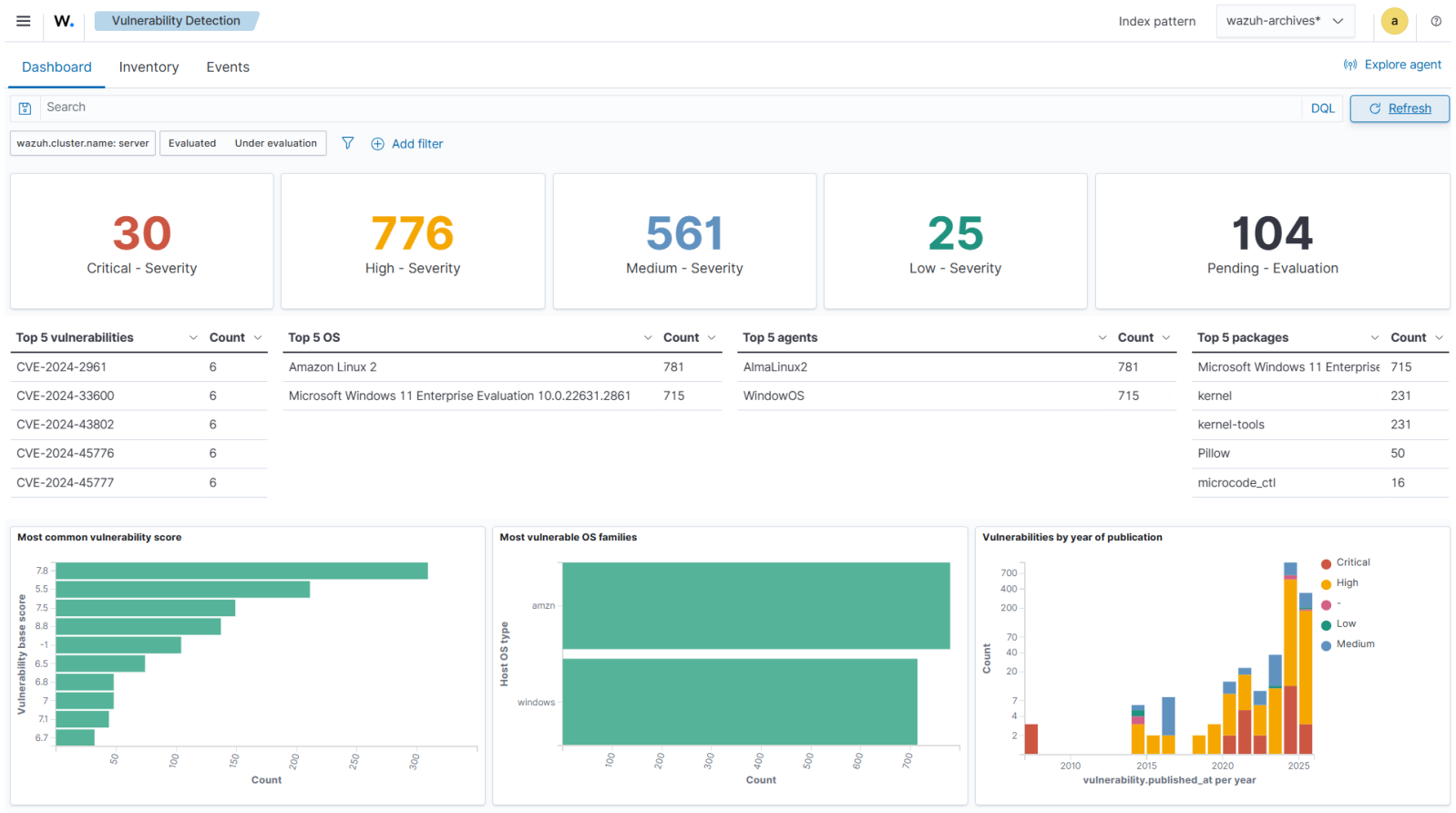
Wazuh v praxi

Přehled zranitelností

Známé bezpečnostní chyby v instalovaném softwaru.

Příklad pro ISP

Příprava oprav na bastionech a serverech dostupných z internetu.



Skutečné GUI Wazuh, ukázka výrobce

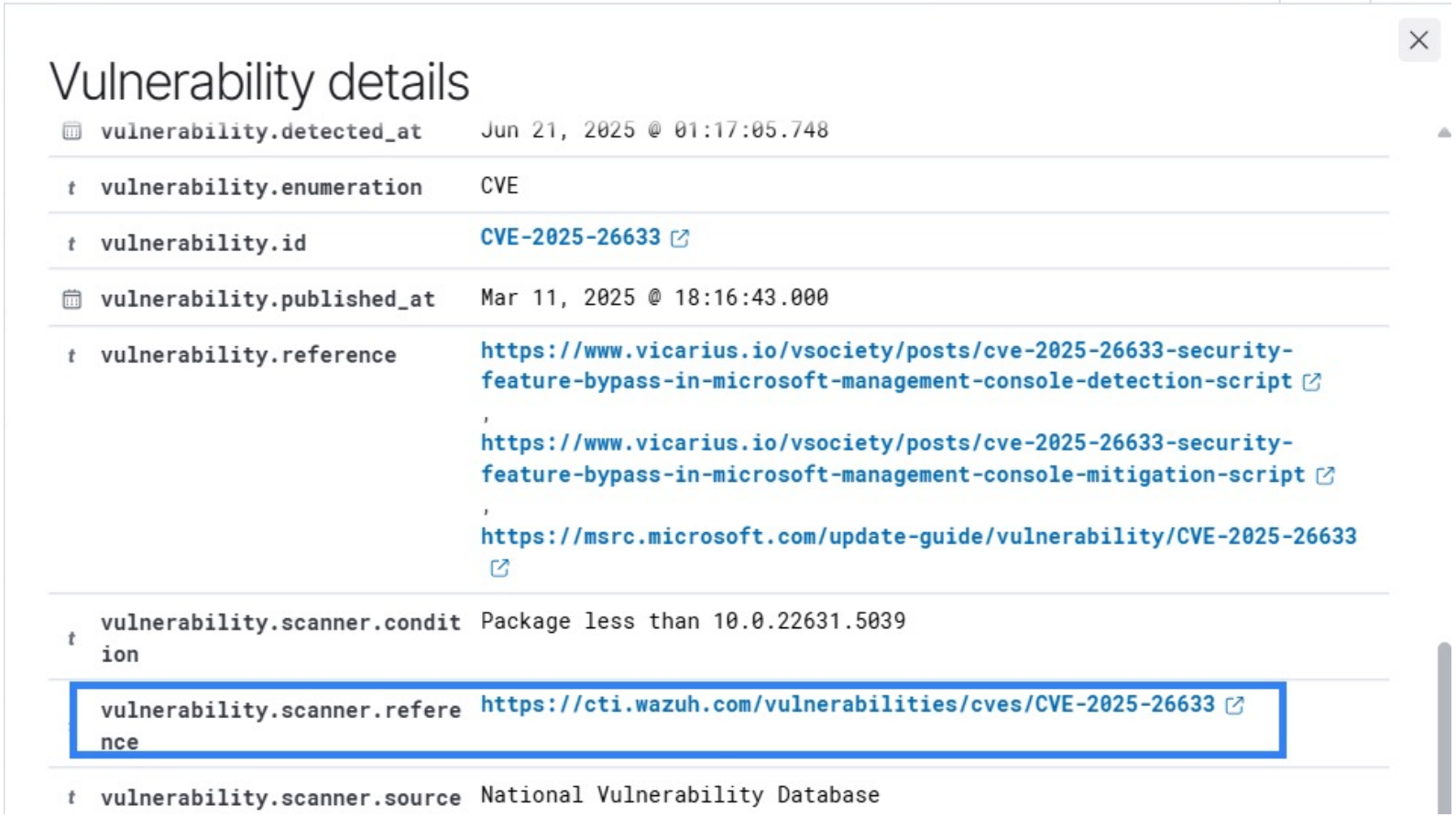
Wazuh v praxi

Detail nálezu a podklady k opravě

Z přehledu otevřeme konkrétní balíček a bezpečnostní chybu.

Příklad pro ISP

Správce dostane konkrétní server a balíček, který má prověřit.



Skutečné GUI Wazuh, ukázka výrobce

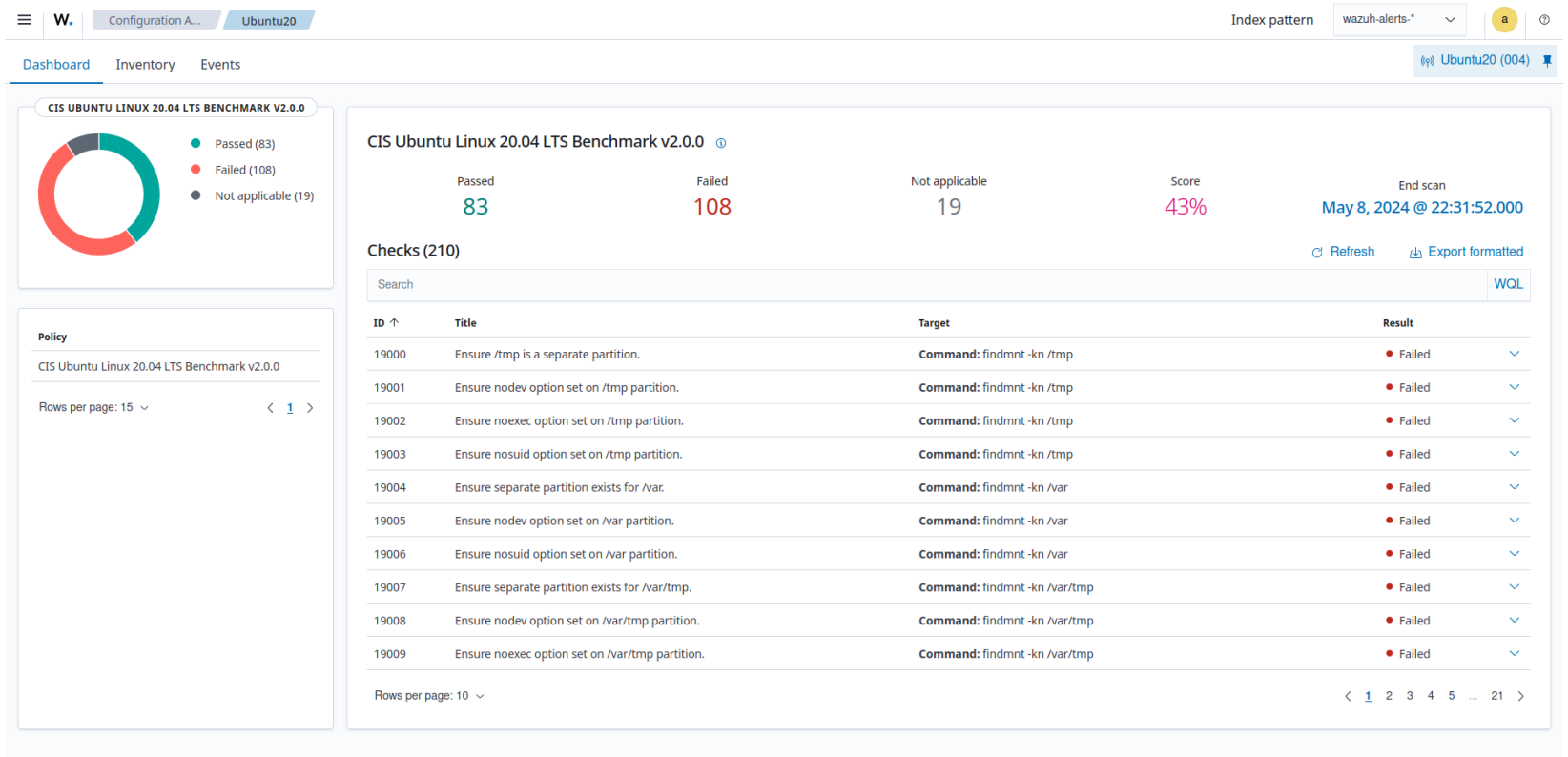
Wazuh v praxi

Kontrola bezpečného nastavení

Pravidelné kontroly konfigurace podle zvolené politiky.

Příklad pro ISP

Kontrola přihlašování a bezpečnostního nastavení provozních serverů.



Skutečné GUI Wazuh, ukázka výrobce

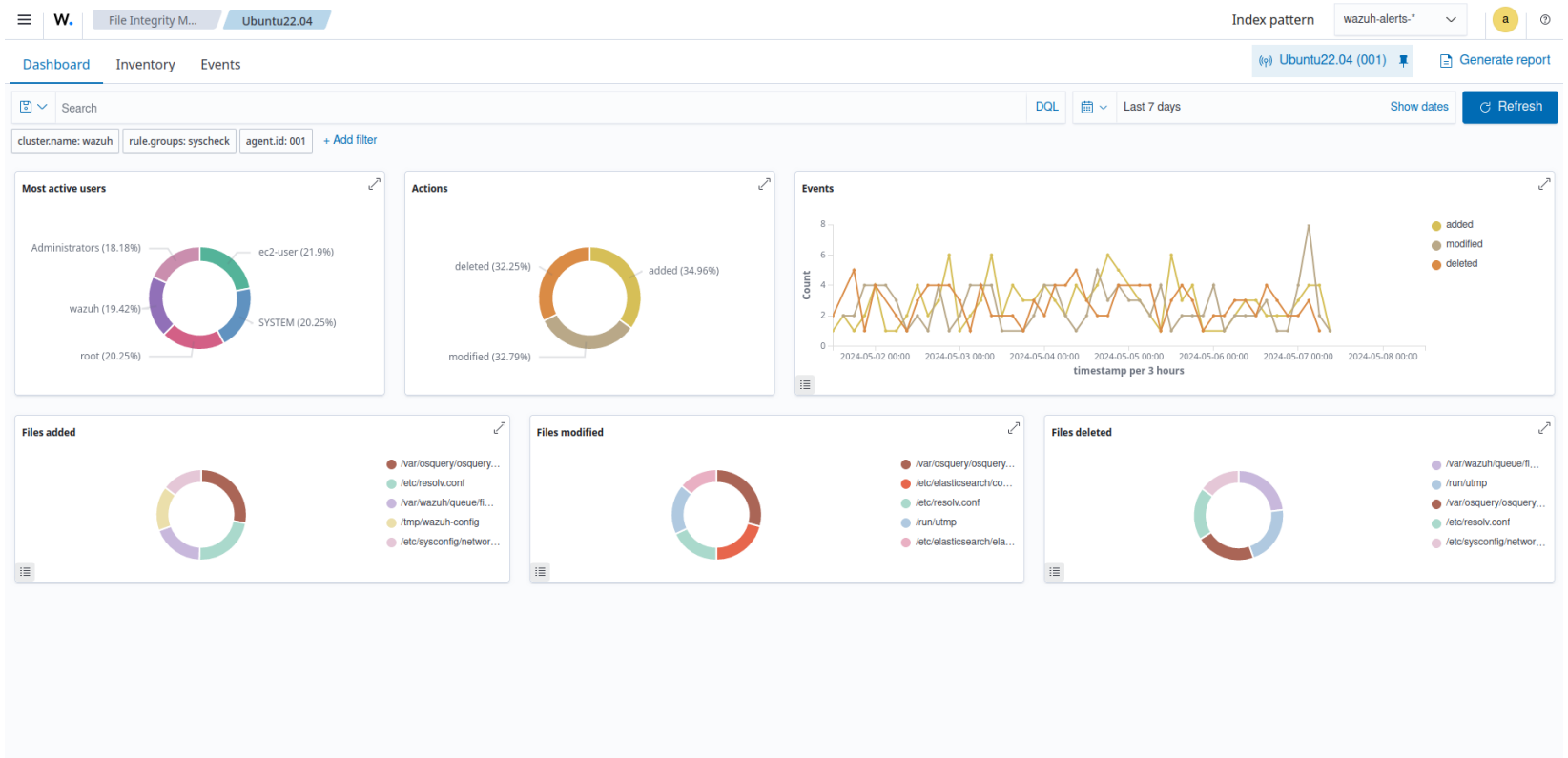
Wazuh v praxi

Změny důležitých souborů

Přehled nových, změněných a odstraněných souborů.

Příklad pro ISP

Konfigurace DNS, web zákaznického portálu nebo nastavení SSH.



Skutečné GUI Wazuh, ukázka výrobce

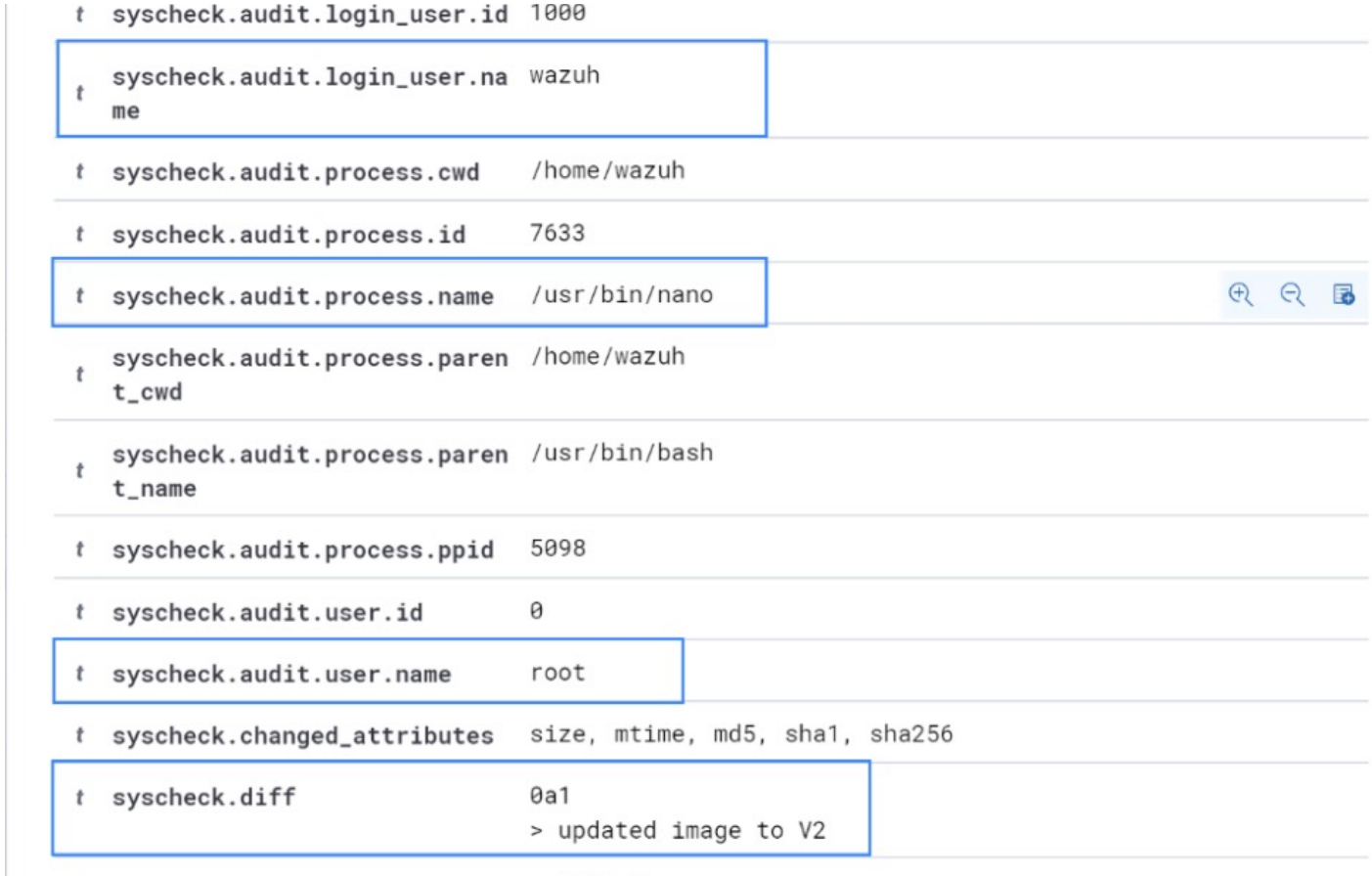
Wazuh v praxi

Kontext změny souboru

Z přehledu otevřeme podrobnosti jedné změny.

Příklad pro ISP

Porovnání změny konfigurace s požadavkem na údržbu.



Skutečné GUI Wazuh, ukázka výrobce

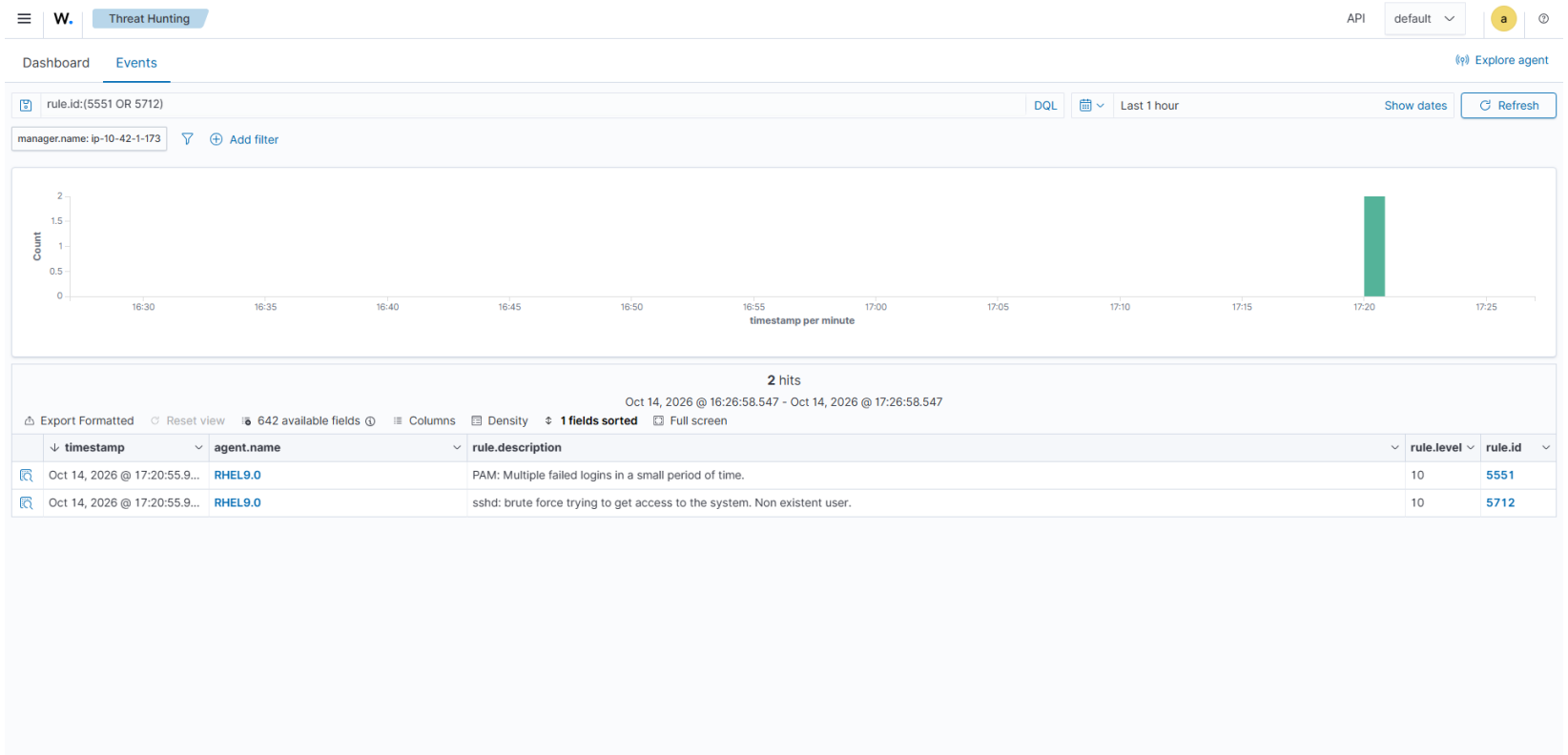
Wazuh v praxi

Přihlašování a opakované pokusy

Přehled neúspěšných i úspěšných přihlášení.

Příklad pro ISP

Noční přístup na bastion nebo vzdálenou plochu správce.



Skutečné GUI Wazuh, ukázka výrobce

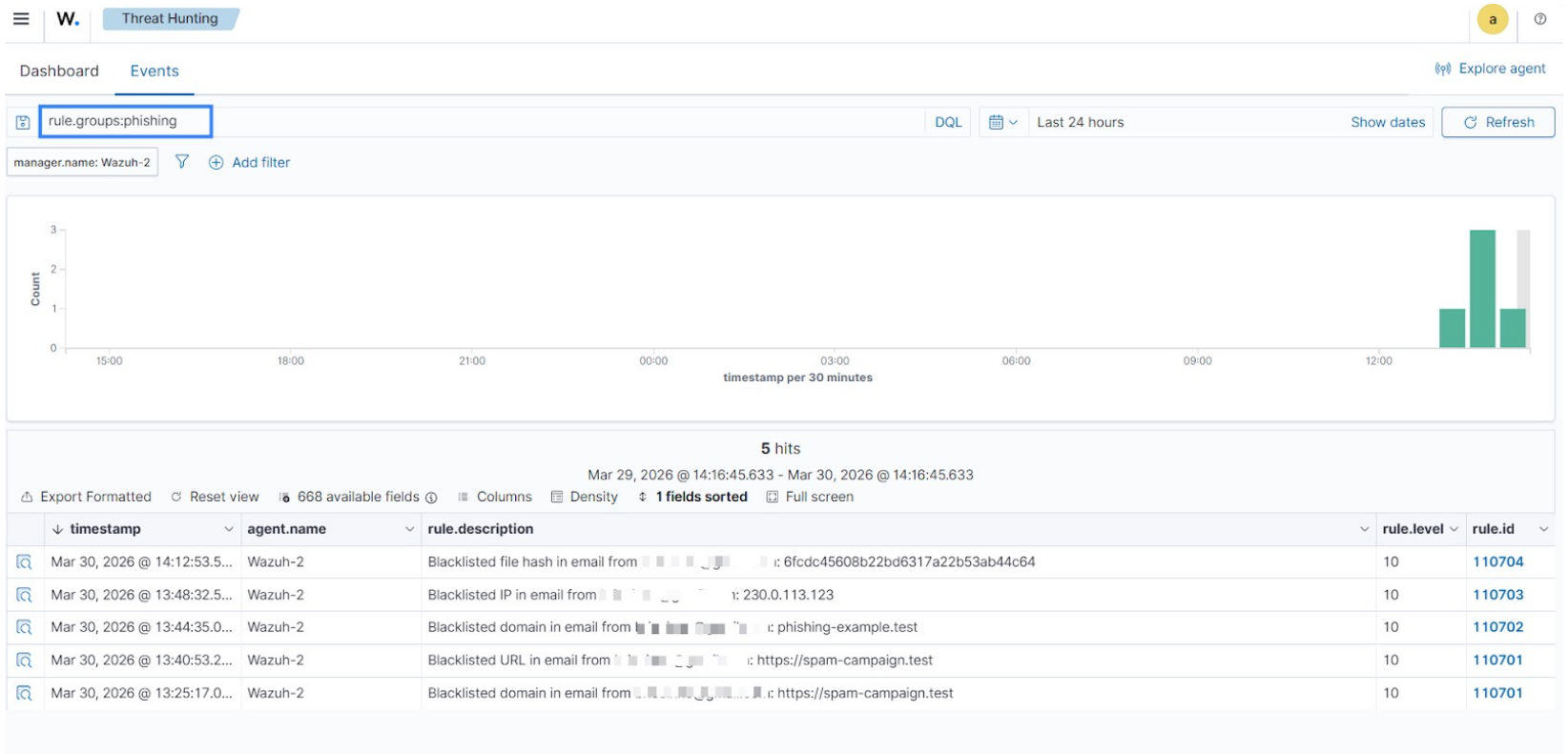
Wazuh v praxi

Hledání souvislostí v událostech

Filtrování bezpečnostních událostí podle otázky operátora.

Příklad pro ISP

Co se na serveru dělo v době, kdy kolega řešil neobvyklý přístup?



Skutečné GUI Wazuh, ukázka výrobce

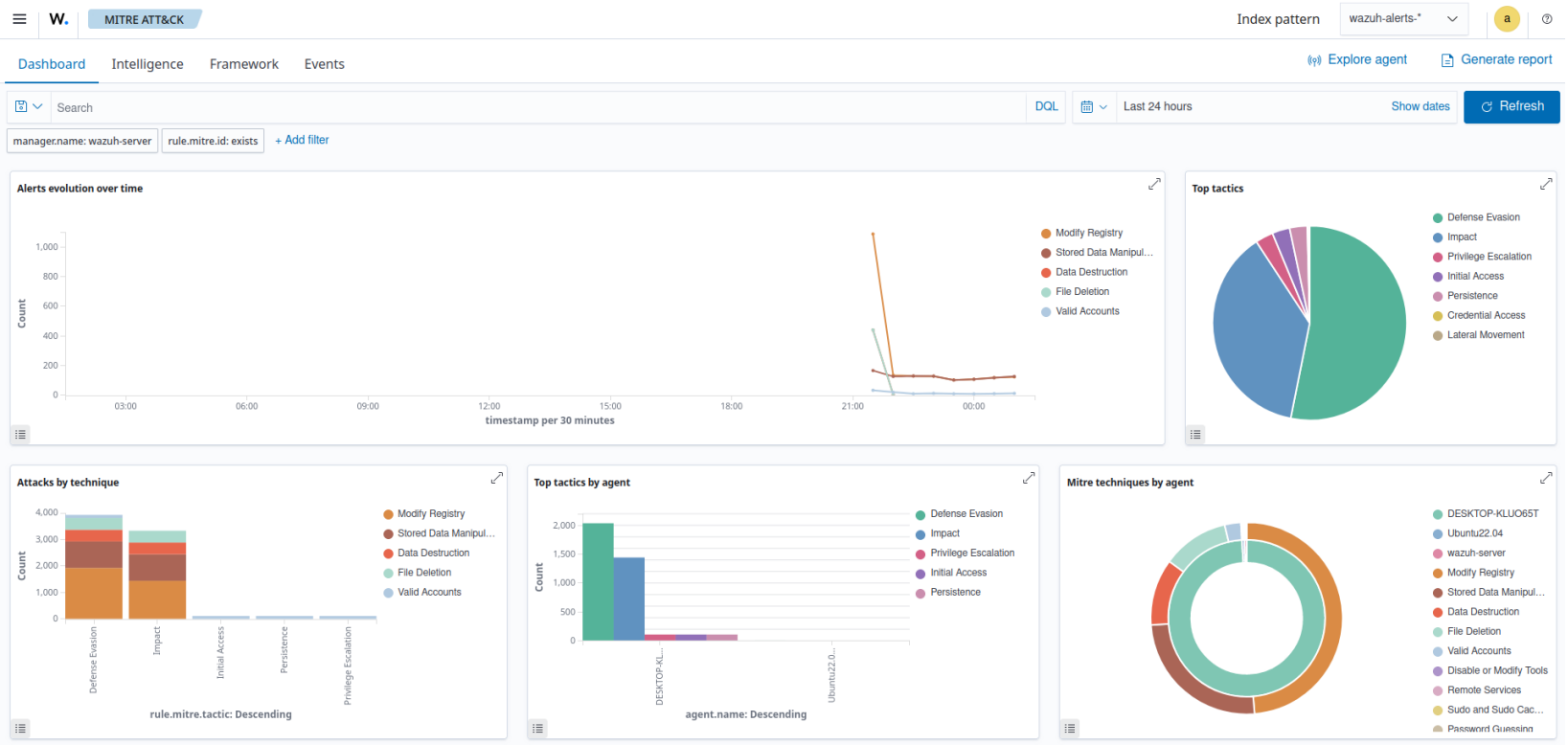
Wazuh v praxi

MITRE ATT&CK v přehledu

Bezpečnostní události v kontextu známých útočných technik.

Příklad pro ISP

Přehled, zda se na stejném hostu objevují různé podezřelé aktivity.



Skutečné GUI Wazuh, ukázka výrobce

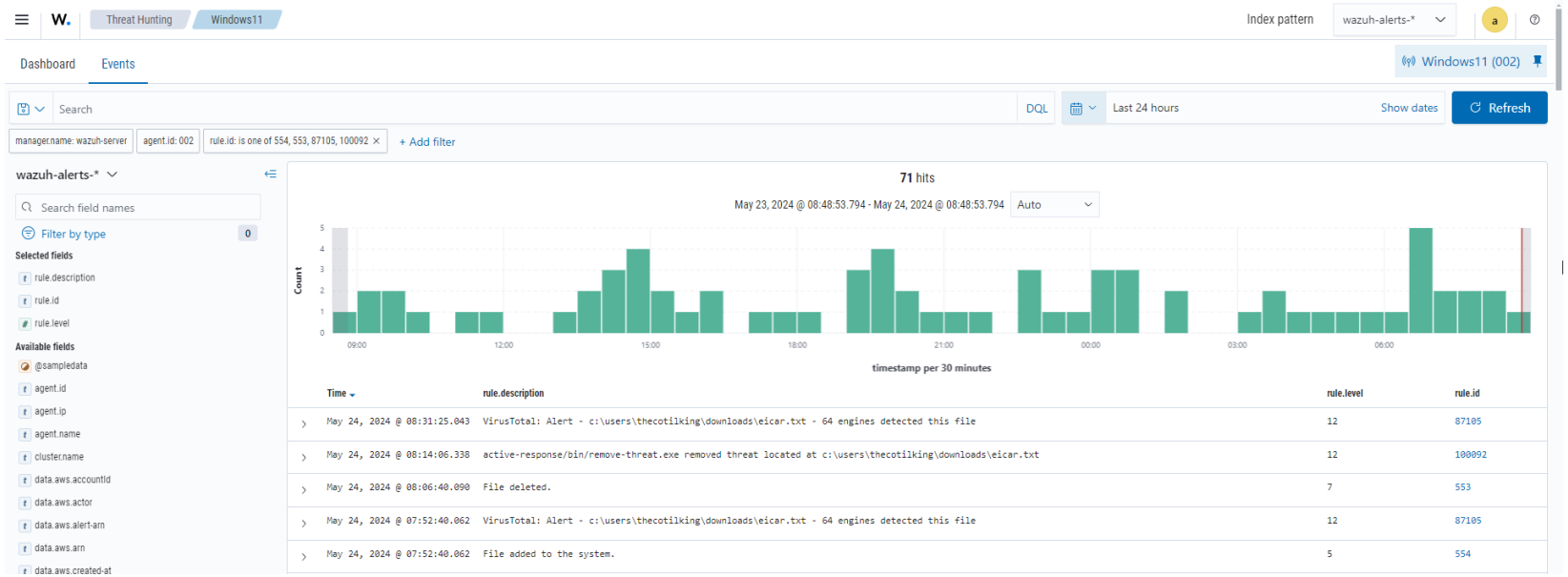
Wazuh v praxi

Malware a podezřelé soubory

Výsledky detekce podezřelých souborů v přehledu událostí.

Příklad pro ISP

Podezřelý soubor na webovém serveru nebo výsledek antiviru na notebooku technika.



Skutečné GUI Wazuh, ukázka výrobce

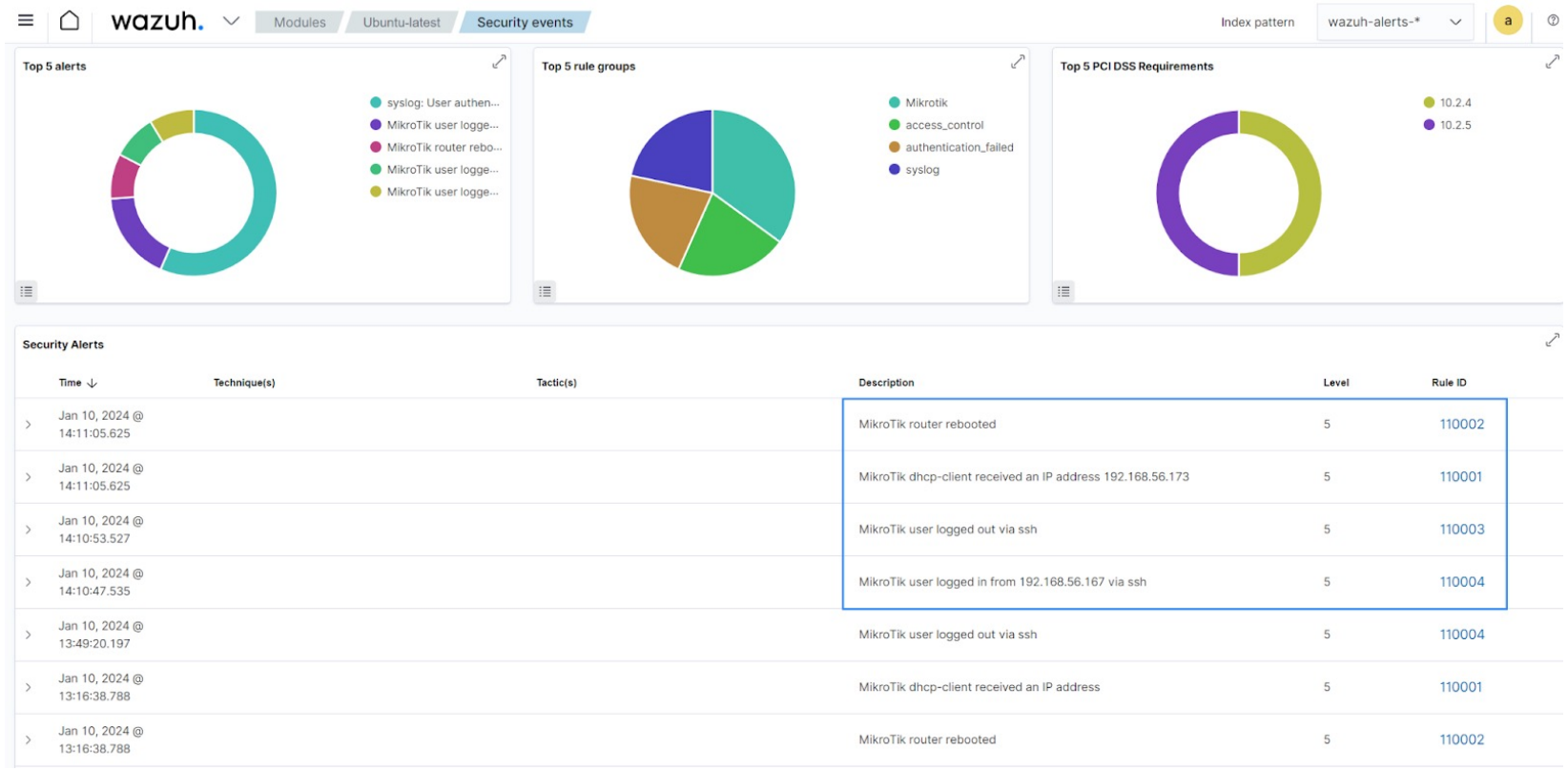
Wazuh v praxi

Logy routerů a firewallů

Síťové události ve stejném prostředí jako logy serverů.

Příklad pro ISP

Přihlášení administrátora na router nebo bezpečnostní událost firewallu.



Skutečné GUI Wazuh, ukázka integrace MikroTik od výrobce

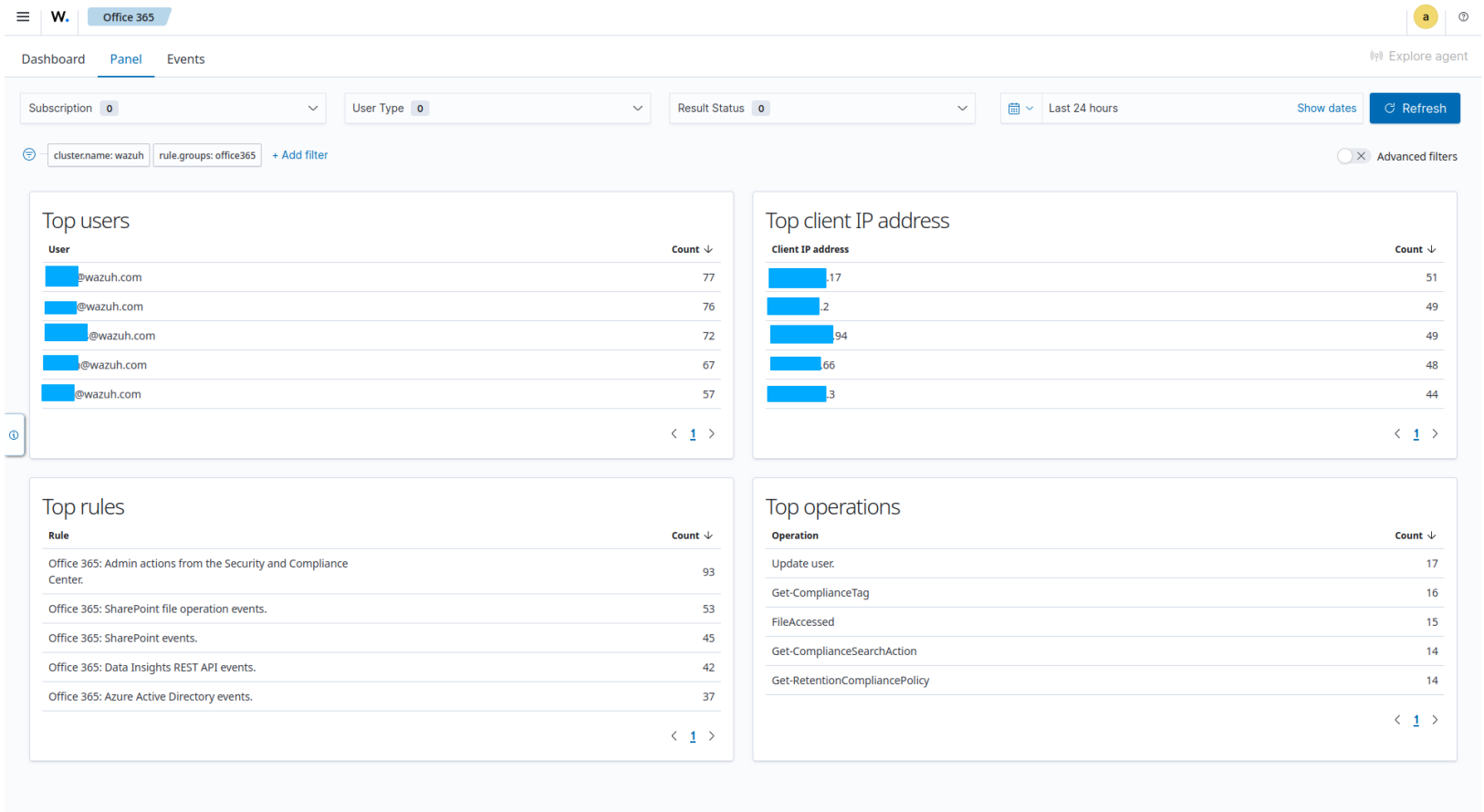
Wazuh v praxi

Cloud a Microsoft 365

Auditní události z připojených cloudových služeb.

Příklad pro ISP

Prověření neobvyklé administrátorské změny ve firemním Microsoft 365.



Skutečné GUI Wazuh, ukázka výrobce

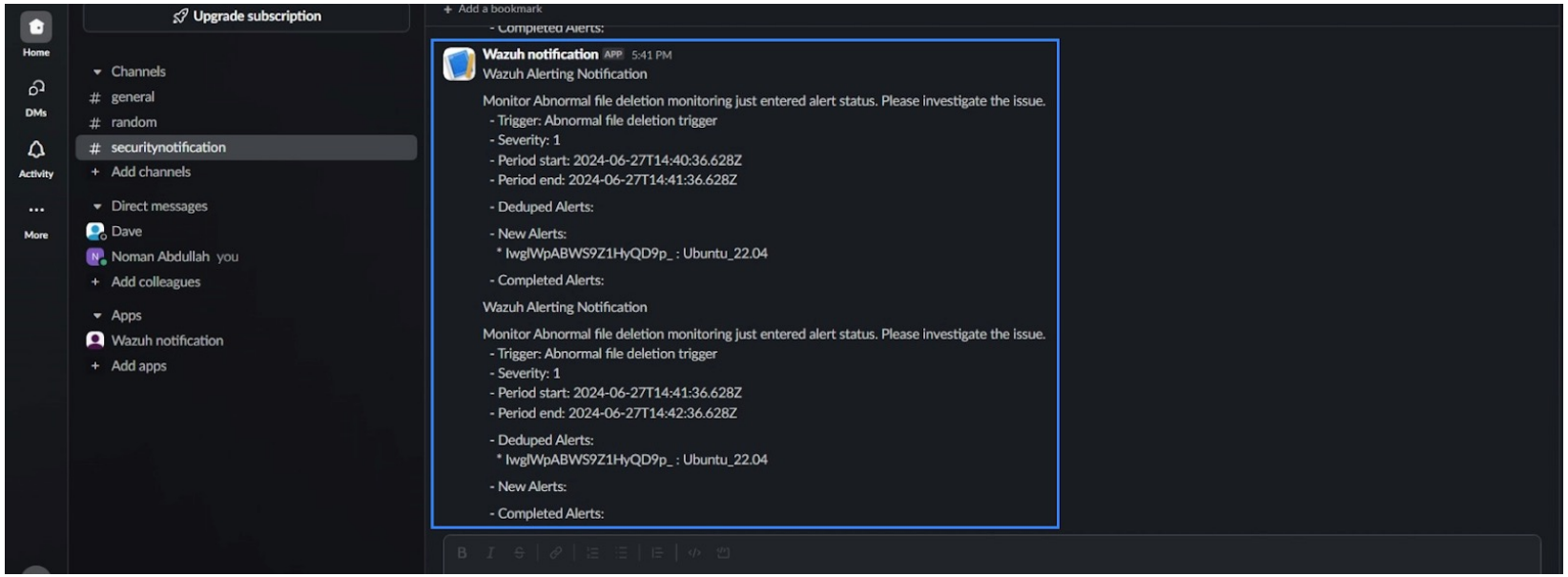
Wazuh v praxi

Upozornění pro obsluhu

Vybraná upozornění lze doručit do týmového chatu.

Příklad pro ISP

Zpráva pohotovosti při hromadném mazání souborů na serveru.



Skutečné GUI Slack, ukázka notifikací Wazuh od výrobce

Wazuh v praxi

Předem připravená reakce

Vybraná detekce může spustit nakonfigurovaný zásah.

Příklad pro ISP

Dočasné zablokování zdrojové adresy při opakovaných pokusech o SSH přístup.



Skutečné GUI Wazuh, ukázka výrobce

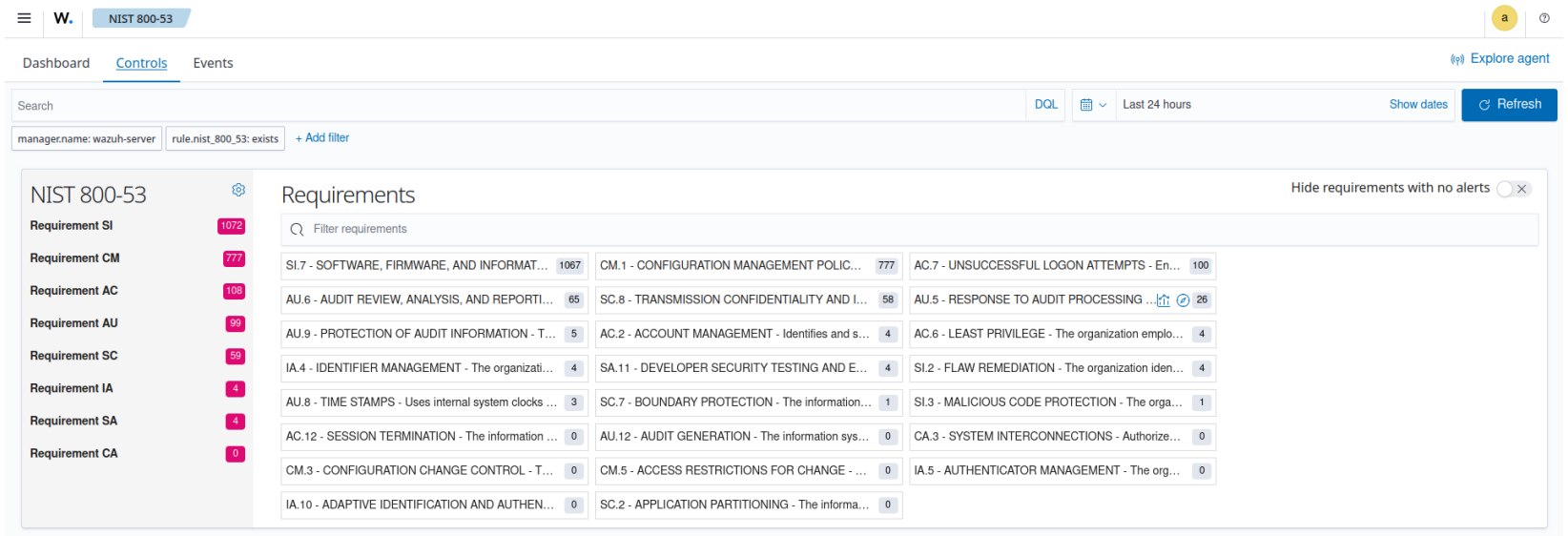
Wazuh v praxi

Podklady pro audit a kontroly

Přehled událostí a výsledků podle vybraného rámce.

Příklad pro ISP

Pravidelný přehled pro vedení nebo podklady při bezpečnostním auditu.



Skutečné GUI Wazuh, ukázka výrobce

Wazuh, využití v provozu

První nasazení u menšího ISP

První zdroje

Bastion, DNS, zákaznický portál a jeden síťový prvek.

První výstupy

Přístupy, změny konfigurace a přehled zranitelností.

Obsluha

Určený člověk, dohoda o upozornění a ověření výsledku.

Pozvánka od initMAX

initMAX

Další ukázky a Wazuh v praxi

Webináře

Praktické ukázky
a záznamy.
Zdarma online.

Termíny a záznamy

Školení

Wazuh v praxi.
Laboratorní cvičení
a konkrétní postupy.

Kurzy a termíny

Konzultace

Váš problém,
pilot nebo návrh
řešení.

Domluvit konzultaci

Dotazy

www.initmax.cz

