COMGUARD

cyber security masters

Případová studie

Zákazník:

IMI Process Automation

Případ:

Zefektivnění a automatizace hardeningu ve společnosti IMI Process Automation

COMGUARD

Informace o zákazníkovi

IMI Process Automation je součástí globální skupiny IMI a specializuje se na návrh a výrobu špičkových průmyslových ventilů a regulačních systémů. Její produkty jsou využívány především v energetice, chemickém průmyslu a dalších kritických odvětvích.

S rozmachem digitalizace průmyslu a kritických infrastruktur narůstají i nároky, které jsou v rámci IMI kladeny na úroveň zabezpečení tohoto předního dodavatele.

GYPTOL Validator

GYTPOL Validator je unikátní nástroj pro detekci a automatizovanou nápravu miskonfigurací. Díky nedostatku efektivnch nástrojů pro zajištění visibility tento typ zranitelnosti běžně uniká pozornosti provozních i bezpečnostních teamů, čímž organizace vystavuje zvýšenému roziku úspěšných útoků.

Hlavní přínosy GYTPOLu

Nepřetržitý dohled nad konfigurační baseline: Nástroj analyzuje konfigurace na úrovni Active Directory, EntraID, Group Policy Objects, Intune politik a koncových zařízení Windows, Windows Server, Linux a MacOS.

Automatizované nápravy: Díky podrobné analýze dokáže GYTPOL u detekovaných miskonfigurací prověřit, zda jejich odstranění nepovede k výpadku systému díky možným dependencím na zranitelné funkci. Opravu následně umožní spustit ze svého rozhraní automatizovanou formou na všech vybraných zařízeních. Není-li v dané situaci automatizace vhodná, poskytne podrobný popis manuálního procesu

Soulad s bezpečnostními standardy: Umožňuje porovnání konfigurací s CIS a NIST benchmarky, což usnadňuje implementaci best practices.

Úspora času: Automatizace oprav šetří čas týmů a umožňuje soustředit se na strategické úkoly.

Výchozí stav

Před implementací GYTPOLu byla oblast hardeningu IT infrastruktury v IMI Process Automation řešena kombinací externích auditů a periodických kontrol, zaměřených zejména na Active Directory (AD). Tyto audity a healthchecky poskytovaly důležitý přehled o bezpečnostním stavu a jejich výstupy vedly k dojmu, že je konfigurační rovina zabezpečení na vysoké úrovni, navzdory vysoké míře komplikovanosti spravovaného prostředí o více než 10 doménách.

Pilotní testování

Gytpol byl zvažován jako alternativa k externím auditům prováděným specializovanými firmami, zejména s ohledem na kontinuální dohled a snažší začlenění do interních procesů.

Po seznámení s platformou v mimoprodukčním prostředí následovalo otestování v serverové infrastruktuře IMI. Nasazení GYTPOLu proběhlo hladce a během několika hodin byl nástroj plně funkční.

Již první analýza při pilotním nasazení na omezený počet zařízení detekovala značné množství problémů, které byly v manuálních procesech detekcí a auditů přehlíženy. Tento stav není u starších domén s více správci nijak výjimečný, díky čemuž je zneužití konfiguračních zranitelností běžným prvkem úpěšných útoků. Jednalo se o:

- Historické konfigurace odpovídající zastaralým standardům.
- Miskonfigurace na úrovni doménových řadičů a serverů, které by správci jen těžko dohledali manuálně.
- Zranitelnosti, které unikly detekci vulnerability managementu- zejména zranitelné instance LOG4J.
- Cleartextová hesla v rámci historických tasků

COMGUARD

Provoz a začlenění GYTPOLu do interních procesů

Kontinuální detekce a možnost snadné zpětné kontroly nápravného procesu z nálezů GYTPOLu udělala další bod pravidelných porad. Díky visibilitě a podrobným informacím k miskonfiguracím se z téměř nemožné proaktivní optimalizace konfigurací stala běžná operativa.

- Historické konfigurace odpovídající zastaralým standardům.
- Karty nálezů zahrnují vše potřebné pro efektivní prioritizaci a delegaci nápravných opatření
- Správci jednotlivých systémů získávají jasně dokumentovaný postup mitigace miskonfigurací a zranitelností, které není vhodné napravit automatizovaně.
- Samotná automatizace za rok využívání napravila více než 500 chyb, bez jakéhokoliv selhání či znefunkčnění systém
- Automatizované opravy jsou aplikovány zejména v oblastech, které by vyžadovaly desítky opakování manuálního procesu na jednotlivých serverech / stanicích

„GYTPOL se ukázal jako velmi efektivní lék na provozní slepotu a bezprostředně po nasazení nám sundal klapky z očí. Vnímám, že řešení operativy a security většině IT týmů nedává prostor se ohlédnout zpátky a důkladně zrevidovat mnohdy dekádu staré a těžko odhalitelné konfigurace, které by mohly působit problémy. Gytpol u nás nahradil cenný pohled externích auditů, které tuto provozní slepotu obcházely, nedokázaly však poskytnout kontinuální náhled a natolik kvalitní výstup s jasnými kroky k nápravám a jejich prioritizaci.“

Libor Navrátil
IT Operations Manager EMEA,
Process Automation

Libor Navrátil zastává pozici IT Operations Managera ve společnosti IMI Process Automation více než 13 let. Jeho bohaté zkušenosti kombinují technický základ se strategickým řízením, podpořené MBA v managementu a kybernetické bezpečnosti. Specializuje se na správu složitých IT infrastruktur, včetně systémové administrace, virtualizace a správy sítí. Svým zaměřením na bezpečnostní protokoly a strategie obnovy po havárii pomáhá sladit IT iniciativy s cíli společnosti, zvyšovat provozní efektivitu a zajišťovat vysokou úroveň kybernetické bezpečnosti.