Čím dříve tým dokáže detekovat útok, tím lépe může reagovat a zotavit se z něj. Ransomware Defender přichází s možností konfigurovat spouštěče událostí na základě vzorců přístupu k datům, které naznačují kybernetický útok. Patří mezi ně detekce pro hromadné mazání dat, hromadné šifrování dat, neoprávněný přístup k síti nebo výrazná odchylka chování uživatele od historického vzoru přístupu k datům a podobně. Tyto události lze zachytit pomocí výstrah a použít je k analýze hlavních příčin porušení zabezpečení. Automatické úlohy lze nastavit tak, aby reagovaly na události naznačující vysokou pravděpodobnost kybernetického útoku, jako je ukončení replikace do kybernetického trezoru nebo odepření přístupu určitým uživatelům, stejně jako pořízení dalších snímků kopie dat z trezoru, do kterých lze nastavit. Uživatelé mohou také aktivovat režim učení, kde se systémy zpřesňují při předpovídání pozitiv.

Režim učení

Umělá inteligence a strojové učení jsou klíčové technologie používané v kybernetické bezpečnosti. Ransomware Defender přichází s režimem učení, který může pomoci vytvořit základní linii bezpečného přístupu. Ta se může lišit od aplikace k aplikaci. Postupem času se systém zpřesňuje v detekci podezřelého chování při přístupu k datům a minimalizuje falešné poplachy.

Whitelisting aplikací

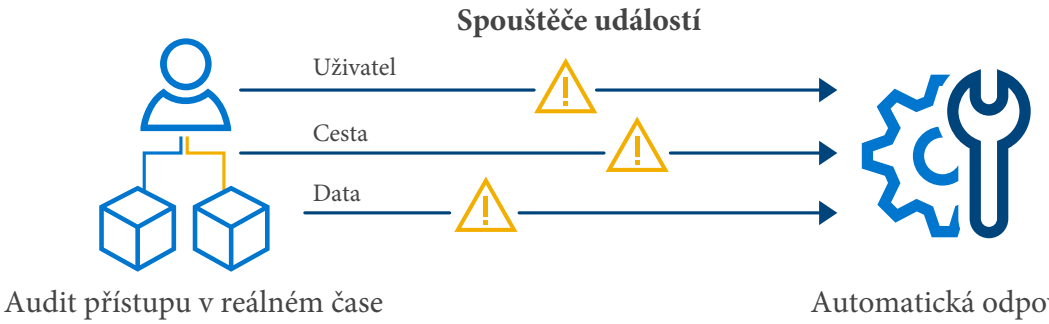
Whitelisting je klíčovou součástí přístupu založeného na nulové důvěře, kdy ověřený seznam aplikací a síťových konfigurací má výhradní přístup k datům. Ran-somware Defender umožňuje správcům zabezpečení vést seznam objektů, uživatelských účtů, IP adres serveru, které mají povolen přístup k určitým datům objektů

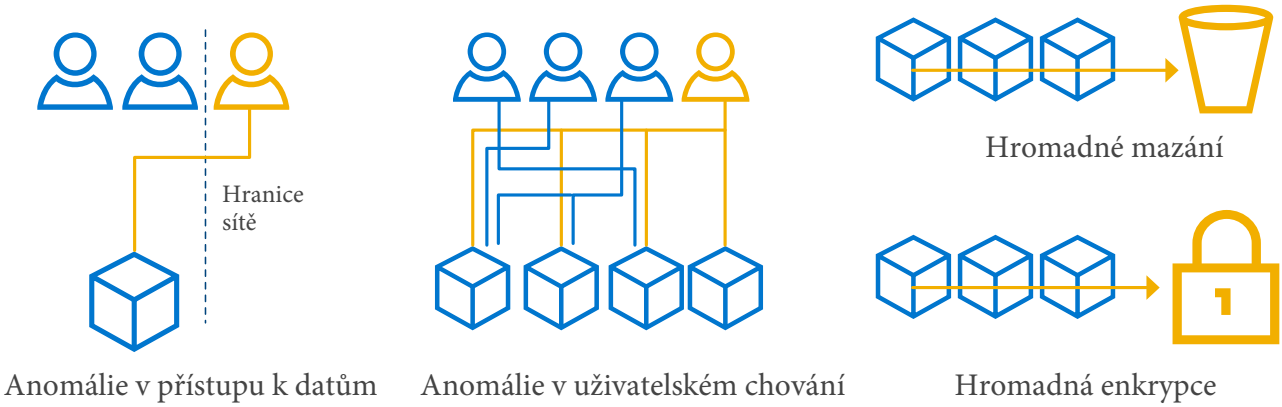
Automatická odpově

Ransomware Defender nabízí řadu možností, jak reagovat na události útoku. Správci jsou upozorněni na neobvyklé chování při přístupu k datům. Systém lze nakonfigurovat tak, aby umožňoval širokou škálu automatických reakcí od pouze monitoru až po okamžité uzamčení uživatele. Integrace API s ECS umožňuje odvolat přístupové klíče, aby se útok zastavil, a urychluje obnovu dat sledováním kompromitovaných objektů, které mohou správci obnovit z předchozích verzí pomocí verzování objektů ECS.

Penetrační testován í s bezpečnostní str áží Security u ard

Penetrační testování je osvědčeným postupem, pokud jde o kontrolu ochrany, která je nastavena proti kybernetickým útokům. Ransomware Defender nabízí automatizované penetrační testování, které zajišťuje funkčnost obrany. Protokoly penetračních testů umožňují správcům snadno zjistit stav bezpečnostních obran a generovat upozornění na neúspěšné penetrační testy.





Obnova provozu a dat

Obnova po kybernetickém útoku zahrnuje identifikaci napadených dat, uživatelských účtů a klientských IP adres, kde útok vznikl. Ransomware Defender poskytuje tyto informace, aby správci mohli umístit úložiště infikovaných objektů a jmenné prostory do karantény. Ransomware Defender poskytuje seznam kompromitovaných objektových dat a S3 bucketů, které umožňují přesnou obnovu dat. To zrychluje dobu obnovy, aby bylo možné systémy znovu zprovoznit a zprovoznit, a zároveň poskytuje post mortem sled událostí, který umožňuje řešit bezpečnostní mezery a chránit prostředí před budoucími útoky. Verze ECS kompatibilní s S3, známá dobrá verze objektových dat může být použita k obnovení postižených dat.

Vnitřní bezpečnostní funkce ECS splňující S3

1. S3 Objektový zámek pro ECS

Dell EMC ECS podporuje uchovávání založené na WORM (jednou zápis, mnoho čtení), počínaje ECS 2.X. Aby byla zajištěna větší kompatibilita s více aplikacemi, ECS nyní podporuje funkci uzamčení objektů (počínaje ECS 3.6.2), která je kompatibilní s možnostmi uzamčení objektů Amazon S3. Objektový zámek je také navržen tak, aby splňoval požadavky na shodu, jako je SEC 17a4(f), FINRA Rule 4511(c) a CFTC Rule 17.

Zámek objektu zabraňuje odstranění verze objektu během uživatelem definované doby uchování. Neměnné objekty S3 jsou chráněny pomocí konfigurace WORM a atributů zachování na úrovni bucketu. Zásady uchovávání jsou definovány pomocí rozhraní S3 API nebo výchozích hodnot na úrovni segmentu. Objekty jsou po dobu uchování uzamčeny a jsou podporovány i scénáře zadržení z důvodu právního omezení.

Click here to learn more about ECS Object lock

2. Správa identity a přístupu S3

ECS Identity and Access Management (IAM) vám umožňuje mít bezpečný přístup ke zdrojům ECS S3. Tato funkce zajišťuje, že každý požadavek na přístup ke zdroji ECS je identifikován, ověřen a autorizován. ECS IAM umožňuje přidávat uživatele, role a skupiny. Můžete také udělit a omezit přístup přidáním zásad k entitám ECS IAM.

Click here to learn more about ECS IAM

3. Verze S3

S3 Versioning na ECS vám umožňuje ponechat více variant objektu ve stejném segmentu, abyste ochránili data a umožnili rychlou obnovu v případě neúmyslné ztráty, včetně nehod, katastrof nebo kybernetických útoků. Pokud je potřeba starší verze verze objektu, můžete ji načíst nebo obnovit na předchozí verzi prostřednictvím rozhraní API ECS S3. Navíc povolením verzování na úrovni segmentu v ECS Object Lock můžete uzamknout verze objektů na konkrétní období uchování (podpora scénářů správy a dodržování předpisů) nebo na neurčito (pro právní blokování).

Click here to learn more about ECS versioning

Získejte více informací o Dell ECS Enterprise Object Storage

Více informací o Dell ECS Platformě

Sledujte Dell Storage na Twitteru

Kontaktujte experty z Dell Technologies
Sales or Support

DELL Technologies