

Azure Security Center

Elaborador:	Jonathas P. Pagotto
Orientador:	Maxwel Vitorino Da Silva

**FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte**

P159a PAGOTTO, Jonathas Próspero

Azure Security Center. / Jonathas Próspero Pagotto. – Americana, 2021.

36f.

Relatório técnico (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Maxwell Vitorino da Silva

1 Segurança em sistemas de informação 2. Computação em nuvem I.
SILVA, Maxwell Vitorino da II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518.5

Jonathas Próspero Pagotto

Azure Security Center

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.

Área de concentração: Segurança da Informação

Americana, 10 de Junho de 2021.

Banca Examinadora:

Prof. Maxwell Vitorino da Silva (Presidente)
Mestre
FATEC - Americana

Prof. Alberto Martins Junior (Membro)
Mestre
FATEC - Americana

Prof. Edson Roberto Gasetta (Membro)
Mestre
FATEC - Americana

SUMÁRIO

Banca Examinadora:	3
1 - Objetivo deste documento.....	6
1.1. Justificativa	6
1.2 Metodologia	7
2 - O que é o “Azure Security Center? ”	7
3 - Hardware.....	9
3.1 Infraestrutura Global do Azure.....	10
3.2 O que é um datacenter do Azure?.....	10
3.3 Regiões do Azure	10
3.4 Área Geográfica do Azure	11
4 Rede (Network)	11
4.1 Rede Global do Azure	11
4.2 Gateways de rede regionais do Azure.....	11
4.3 Azure Edge Zones.....	12
5.0 Aplicações	13
5.1 “Privileged Access Management” para Serviços de Domínio do Active Directory.....	13
5.2 Azure Defender	15
5.2.1 Recursos Azure Defender	16
5.3 Azure Defender Key Vault	17
5.4 Azure Sentinel	18
5.4.1 Conectores	19
5.4.2 Pastas de Trabalho – Workbooks.....	20
5.4.3 Análise e Incidentes.....	21
5.4.4 Investigação	22
6 - Fontes Bibliográficas	36

Lista de Figuras

- Figura 1 - Modelo Azure Security Center 7
- Figura 2 - Datacenter Microsoft Arizona EUA 9
- Figura 3 - Rede Mundial Azure 12
- Figura 4 - Microsoft PAM 13
- Figura 5 - Painel Azure Defender 15
- Figura 6 - Azure Defender Key Vault 17
- Figura 7 - Azure Sentinel 18
- Figura 8 - Conectores Azure Defender 19
- Figura 9 - Azure Workbooks 21
- Figura 10 - Azure Incidentes 22
- Figura 11 - Investigação e Timeline 23
- Figura 12 - Impossible Travel 23
- Figura 13 - Encaminhamento suspeito de E-mails 24
- Figura 14 - Conexão Suspeita a um Endereço IP 25
- Figura 15 - Reconhecimento de Mapeamento de Rede 26
- Figura 16 - Um arquivo Malicioso foi detectado 27
- Figura 17 - Propriedades de Login Desconhecidas 28
- Figura 18 - Suspeita de Ataque de Força Bruta 29
- Figura 19 - Atividade Suspeita de Falsificação de Identidade 31
- Figura 20 - Varredura de Porta Horizontal 32
- Figura 21 - NetCat Detectado 32
- Figura 22 - Software Indesejado Bloqueado 33

1 - Objetivo deste documento

A T.I de hoje está migrando em grande parte para a nuvem, incluindo servidores, armazenamento, redes, aplicativos e cargas de trabalho. Com toda essa demanda exigisse uma segurança aplicada.

O Azure possui uma central de segurança usando recomendações da Microsoft. Possui recomendações de requisitos regulatórios ou requisitos de segurança da empresa gerenciando centralmente as políticas de segurança.

O objetivo desse documento é mostrar exemplificando e detalhando opções disponíveis, práticas de bom uso e exemplos práticos utilizados para o Azure Security Center. Com este documento podemos diminuir vulnerabilidades em um projeto destes assim elevando as chances de sucesso na implantação.

1.1. Justificativa

A evolução constante na área de tecnologia da informação alavancou o uso de recursos em Nuvem muito rapidamente. No passado as empresas dependiam muito de servidores locais demandando grande necessidade de equipamentos locais, pessoas qualificadas a gerenciar estes equipamentos e disponibilidade reduzida, pois quase sempre estes ambientes não são redundantes.

Com os recursos em nuvem a demanda por pessoas qualificadas para gerenciar um ambiente local diminuiu, a disponibilidade aumentou e barateou o custo das empresas. Mas com essa disponibilização de recursos na nuvem a segurança surgiu como sendo uma necessidade de primeira.

1.2 Metodologia

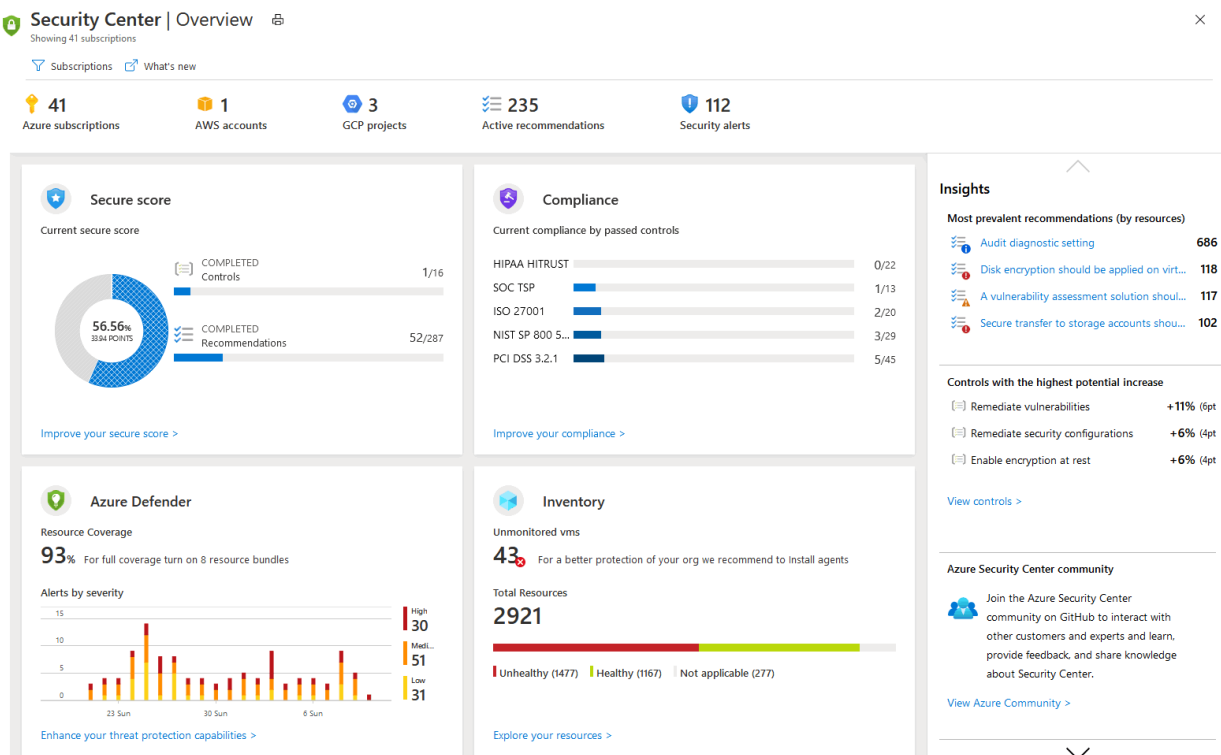
Este projeto fundamenta-se em um relatório técnico, com pesquisas qualitativa, quantitativa e exploratória para coleta e análise de dados coletados na ferramenta mencionada. Trabalho com esta ferramenta há aproximadamente 1 ano e encontro muito pouco material, casos de uso de empresas e usuários brasileiros.

O Objetivo é confrontar as informações adquiridas ao longo do projeto com os conhecimentos teóricos da literatura pesquisada em sites da internet, fórum, casos que encontro no meu dia a dia, opiniões de colegas de trabalho, entre outros, que possibilitam uma interação entre o estudo e a análise do caso.

2 - O que é o “Azure Security Center?”

Na Figura 1 temos o exemplo do Painel Inicial do Azure Security Center:

Figura 1 - Modelo Azure Security Center



Fonte: <https://docs.microsoft.com/pt-br/azure/security-center/security-center-get-started>

A Central de Segurança do Azure é um sistema de gerenciamento de segurança de infraestrutura unificado que fortalece a postura e a proteção de segurança de seus data centers, servidores, workstations e dispositivos móveis e fornece proteção avançada contra ameaças em suas cargas de trabalho híbridas locais e na nuvem, estejam elas em nuvem ou local.

Manter os recursos seguros é um esforço conjunto entre seu provedor de nuvem, o Azure e o cliente. Precisamos verificar se as cargas de trabalho estão seguras ao mudar para a nuvem e, ao mesmo tempo, quando ao ir para *IaaS* (infraestrutura como serviço), há mais responsabilidade do cliente do que havia em *PaaS* (plataforma como serviço) e *SaaS* (software como serviço).

A Central de Segurança do Azure fornece as ferramentas necessárias para proteger sua rede, proteger seus serviços e verificar se você está atualizado quanto à sua postura de segurança, mas demanda bastante conhecimento técnico de quem opera a ferramenta, pois existe inúmeros conectores, regras e *Workloads* disponíveis.

A Central de Segurança do Azure aborda os três desafios de segurança mais urgentes e abordados nos dias de hoje:

- Cargas de trabalho que mudam rapidamente – são tanto um ponto forte quanto um desafio da nuvem. Por um lado, os usuários finais estão capacitados a fazer mais. Por outro, como você garante que os serviços em constante mudança que as pessoas estão usando e criando estejam atualizados com seus padrões de segurança e sigam as melhores práticas de segurança.

- Ataques cada vez mais sofisticados – onde quer que você execute suas cargas de trabalho, os ataques continuam a ficar cada vez mais sofisticados. Nós precisamos proteger as cargas de trabalho de nuvem pública, que são, na verdade, uma carga de trabalho voltada para a Internet que poderá deixá-la ainda mais vulnerável se não seguirmos as melhores práticas de segurança e as atualizações diárias de vulnerabilidades e vazamentos constantes.

- Habilidades de segurança são escassas – o número de alertas de segurança e sistemas de alertas ultrapassa em muito o número de administradores com experiência e preparação necessárias para verificar se seus ambientes estão protegidos.

Permanecer atualizado quanto aos ataques mais recentes é um desafio constante e diário, tornando impossível permanecer em vigor enquanto o mundo de segurança é uma frente em constante mudança.

Para ajudar a nos proteger contra esses desafios, a Central de Segurança fornece ferramentas para:

- Fortalecer a postura de segurança: A Central de Segurança avalia o ambiente e permite que entenda o status dos recursos e se eles são seguros ou não, o nível de criticidade e o que devemos abordar com mais urgência ou não.

- Proteger contra ameaças: a Central de Segurança avalia as cargas de trabalho e gera recomendações de prevenção de ameaças e alertas de segurança.

- Ficar seguro com mais rapidez: Na Central de Segurança, tudo é feito na velocidade da nuvem. Por ser integrada nativamente, a implantação da Central de Segurança é fácil, oferecendo provisionamento automático e proteção com os serviços do Azure. Mas somente a implementação fácil pode causar uma falsa sensação de segurança, pois a ferramenta demanda de mão de obra técnica especializada e atualizada na ferramenta.

3 - Hardware

Por ser uma estrutura totalmente em nuvem a Microsoft possui datacenters ao redor do mundo, na Figura 2 segue uma foto de um dos Datacenters e logo abaixo um resumo de como essa estrutura funciona:

Figura 2 - Datacenter Microsoft Arizona EUA



Fonte: <https://www.datacenterknowledge.com/microsoft/microsoft-build-fifth-massive-western-us-azure-region>

3.1 Infraestrutura Global do Azure

A infraestrutura global do Azure é composta por dois componentes principais: a infraestrutura física e os componentes de rede de conexão. O componente físico é composto por mais de 160 datacenters físicos, organizados em regiões, e está vinculado a uma das maiores redes interconectadas do planeta.

Com a conectividade da rede global do Azure, cada um dos datacenters do Azure fornece alta disponibilidade, baixa latência, escalabilidade e os avanços mais recentes na infraestrutura de nuvem – tudo isso em execução na plataforma do Azure.

Juntos, esses componentes mantêm os dados completamente dentro da rede confiável da Microsoft e o tráfego IP nunca entra na Internet pública. Vemos muito relatos de indisponibilidade de alguns serviços Microsoft, mas nunca da indisponibilidade total de seus serviços, isso mostra a confiabilidade no serviço que oferecem.

3.2 O que é um datacenter do Azure?

Os datacenters do Azure são edifícios físicos exclusivos localizados em todo o mundo que abrigam um enorme grupo de servidores de computador em rede.

3.3 Regiões do Azure

Uma região do Azure é um conjunto de datacenters implantados dentro de um perímetro de latência definida e conectados por meio de uma rede regional dedicada de baixa latência.

Com mais regiões globais do que qualquer outro provedor de nuvem, o Azure dá aos clientes a flexibilidade para implantar aplicativos no local em que eles precisam. Uma região do Azure tem preços e disponibilidade de serviço distintos.

3.4 Área Geográfica do Azure

Uma área geográfica do Azure é um mercado discreto, que normalmente contém pelo menos uma ou mais regiões, que preserva os limites de conformidade e de residência de dados.

As geografias permitem que os clientes com necessidades de conformidade e de residência de dados específicas mantenham seus dados e aplicativos próximos. As geografias são tolerantes a falhas para resistir a falhas completas da região, por meio da sua conexão com a infraestrutura de rede dedicada e de alta capacidade do Azure.

4 Rede (Network)

Nas próximas sessões apresenta-se os métodos e tecnologias aplicadas em seus Datacenters que se aplicam ao Azure:

4.1 Rede Global do Azure

A rede global do Azure refere-se a todos os componentes na rede e é composta pela WAN (rede de longa distância) global da Microsoft, pelos PoPs (pontos de presença), pela fibra e outros.

A WAN (rede de longa distância) global da Microsoft conecta centenas de datacenters em regiões de todo o mundo e oferece alta disponibilidade e capacidade. Com a flexibilidade de responder imediatamente a picos de demanda imprevisíveis, a WAN global é crítica para o fornecimento de uma excelente experiência de serviço de nuvem.

4.2 Gateways de rede regionais do Azure

Os gateways de rede regionais são interconexões de datacenter de hiperescala massivamente paralelas entre datacenters em uma região, sem a necessidade de colocar cada datacenter individual em rede com os outros em uma região.

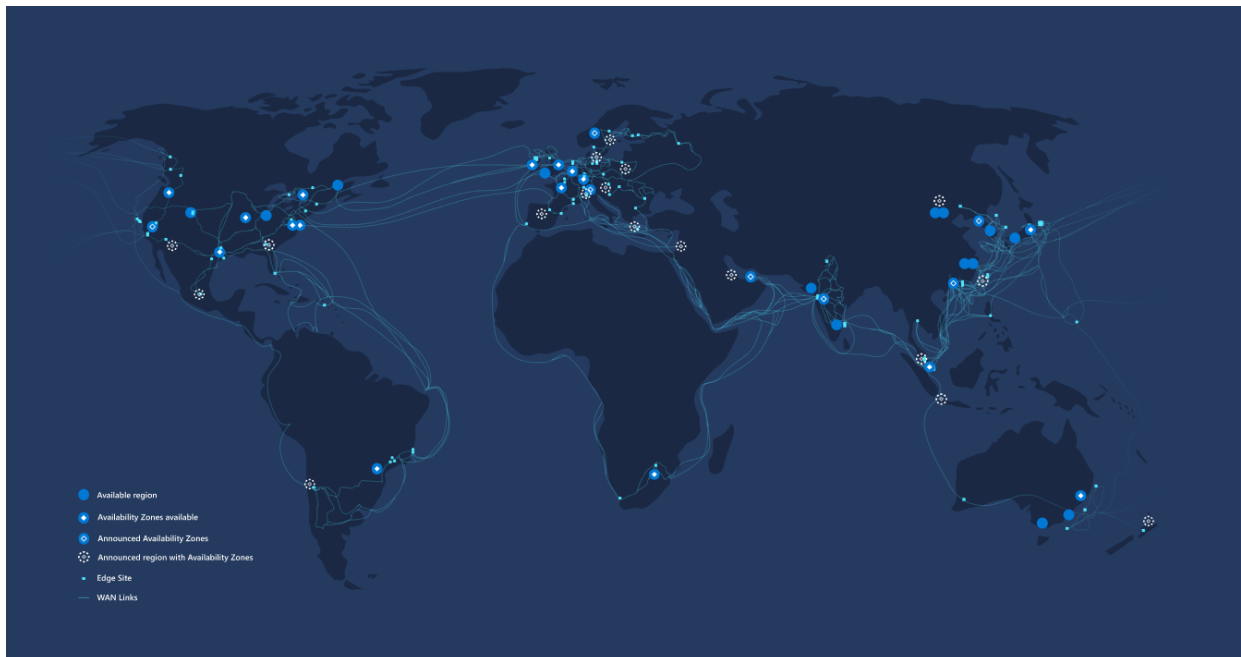
Isso garante que os problemas de conexão em um datacenter não causem problemas na região mais ampla. Isso também permite a adição de novos datacenters sem a necessidade de rotear conexões de rede diretas para cada datacenter existente.

4.3 Azure Edge Zones

Os Azure Edge Zones são extensões de volume do Azure, colocadas em áreas densamente populadas. Os Azure Edge Zones dão suporte a VMs (máquinas virtuais), contêineres e um conjunto selecionado de serviços do Azure que permitem que você execute aplicativos com intensidade de taxa de transferência e sensíveis à latência próxima aos seus usuários finais.

Os Azure Edge Zones fazem parte da rede global da Microsoft e oferecem conectividade segura, confiável e de alta largura de banda entre os aplicativos que estão em execução no Azure Edge Zone (perto do usuário) e um conjunto completo de serviços do Azure em execução nas maiores regiões do Azure. Na Figura 3 vemos toda a rede:

Figura 3 - Rede Mundial Azure



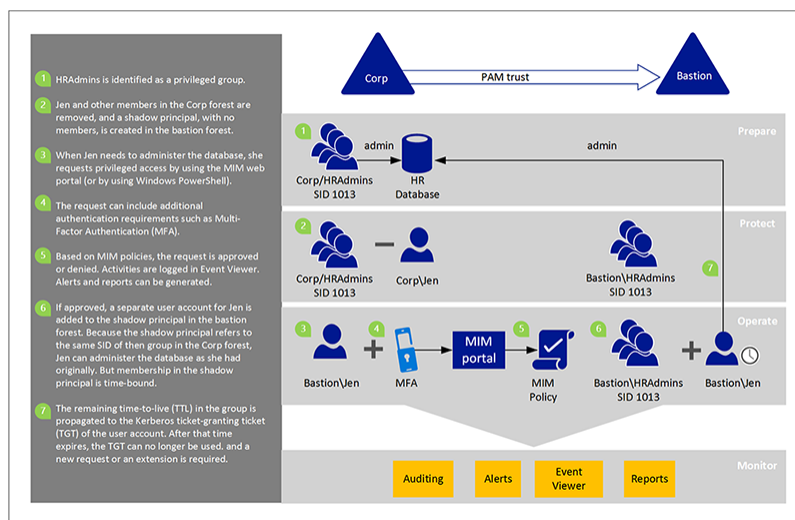
Fonte: <https://docs.microsoft.com/pt-br/azure/networking/microsoft-global-network>

5.0 Aplicações

5.1 “Privileged Access Management” para Serviços de Domínio do Active Directory

Na Figura 4 vemos um painel do PAM:

Figura 4 - Microsoft PAM



Fonte: <https://docs.microsoft.com/pt-br/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services>

O PAM se baseia nas novas funcionalidades do AD DS, particularmente, em relação à autorização e autenticação de contas de domínio, e nas novas funcionalidades do “Microsoft Identity Manager”. O PAM separa as contas privilegiadas de um ambiente existente do “Active Directory”.

Quando uma conta privilegiada precisa ser usada, ela precisa primeiro ser solicitada e, em seguida, aprovada. Após a aprovação, a conta privilegiada recebe a permissão por meio de um grupo principal externo em uma nova floresta em vez da floresta atual do usuário ou aplicativo. O uso dá controle maior à organização, como o controle sobre quando um usuário pode ser um membro de um grupo com privilégios e sobre como o usuário precisa se autenticar.

Essa concessão emite associações a um grupo com limite de tempo, que por sua vez, produzem TGTs (tíquetes de concessão de tíquete) com limite de tempo. Os serviços ou aplicativos baseados no Kerberos poderão respeitar e impor esses TGTs se os aplicativos e serviços existirem nas redes que confiam nas sub redes.

Contas de usuário diárias não precisam ser movidas para uma nova floresta. O mesmo acontece com os computadores, aplicativos e seus grupos. Eles permanecem onde eles estão atualmente, em uma floresta existente. Considere o exemplo de uma organização que trata esses problemas de segurança cibernética hoje, mas não tem planos imediatos para atualizar a infraestrutura de servidor para a próxima versão do Windows Server. Essa organização ainda poderá tirar proveito dessa solução combinada, usando MIM e uma nova floresta; ela poderá também controlar melhor o acesso aos recursos existentes.

O PAM oferece as seguintes vantagens:

Isolamento e controle de privilégios: os usuários não mantêm privilégios em contas que também são usadas para tarefas não privilegiadas, como verificação de e-mail ou navegação na Internet. Os usuários precisam solicitar privilégios. As solicitações são aprovadas ou negadas com base nas políticas do MIM definidas por um administrador do PAM. Até uma solicitação ser aprovada, o acesso privilegiado não estará disponível.

Step-up e proof-up: esses são os novos desafios de autenticação e autorização para ajudar a gerenciar o ciclo de vida de contas administrativas separadas. O usuário pode solicitar a elevação de uma conta administrativa e essa solicitação passa por fluxos de trabalho MIM.

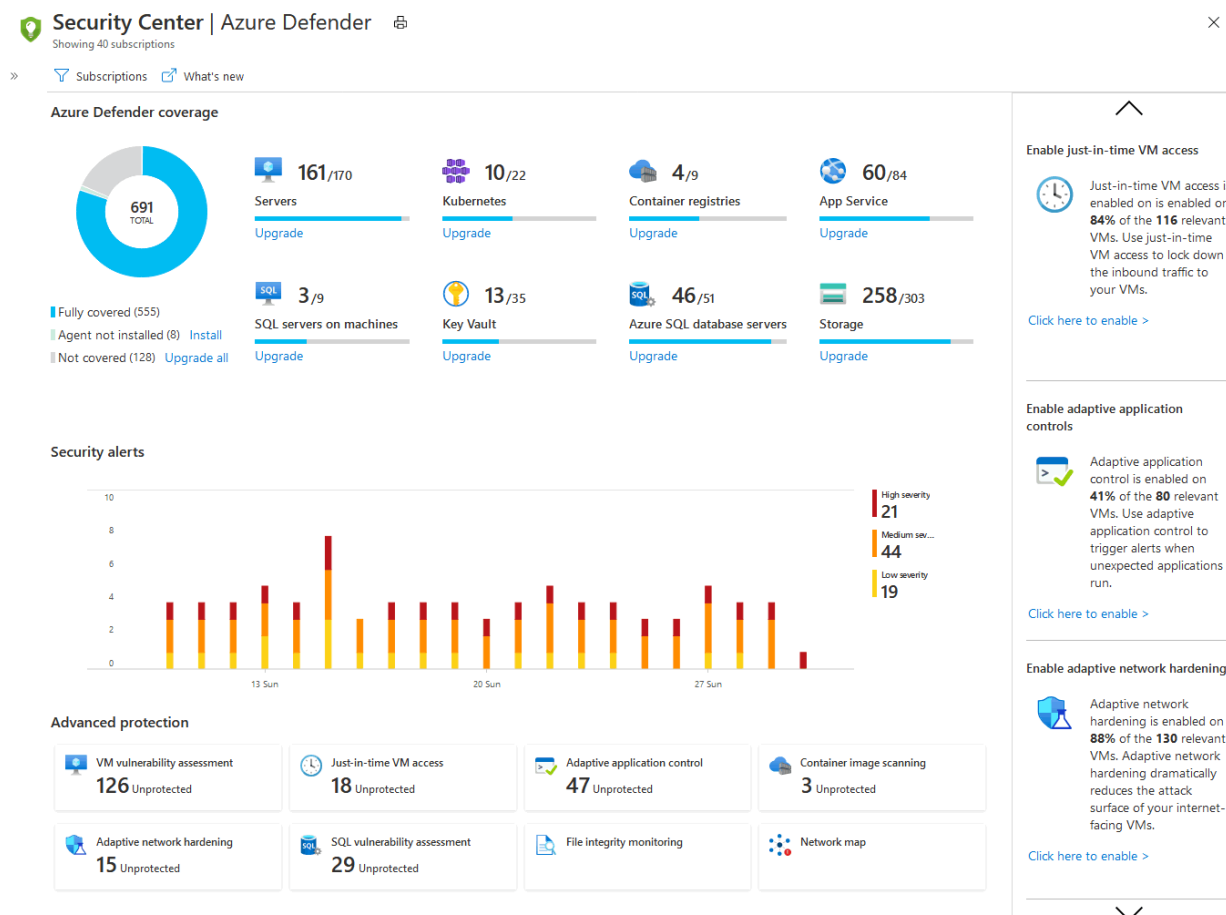
Log adicional: além de fluxos de trabalho internos do MIM, há um log adicional para o PAM que identifica a solicitação, como ela foi autorizada e os eventos que ocorrem após a aprovação.

Fluxos de trabalho personalizáveis: os fluxos de trabalho MIM podem ser configurados para cenários diferentes e vários fluxos de trabalho podem ser usados, com base nos parâmetros do usuário solicitante ou nas funções solicitadas.

5.2 Azure Defender

Na Figura 5 vemos o Painel do Azure Defender:

Figura 5 - Painel Azure Defender



Fonte: <https://docs.microsoft.com/pt-br/azure/security-center/security-center-get-started>

Os recursos da Central de Segurança do Azure abrangem os dois pilares mais amplos da segurança na nuvem:

- GPSN (gerenciamento da postura de segurança na nuvem) – A Central de Segurança está disponível gratuitamente para todos os usuários do Azure. A experiência gratuita inclui recursos de GPSN, como classificação de segurança, detecção de configurações incorretas de segurança em seus computadores do Azure, inventário de ativos e muito mais. Use esses recursos de GPSN para fortalecer sua postura de nuvem híbrida e controlar a conformidade com as políticas internas.

- PCTN (proteção de cargas de trabalho na nuvem) – A PPCTN (plataforma de proteção de cargas de trabalho na nuvem) integrada da Central de Segurança, o Azure Defender, oferece proteção avançada e inteligente para cargas de trabalho e recursos híbridos do Azure.

A habilitação do Azure Defender oferece uma série de recursos de segurança adicionais, conforme descrito nesta página. Além das políticas internas, ao habilitar qualquer plano do Azure Defender, você pode adicionar políticas e iniciativas personalizadas. Você pode adicionar padrões regulatórios, como NIST e Azure CIS, bem como o Azure Security Benchmark para obter uma exibição verdadeiramente personalizada da sua conformidade.

5.2.1 Recursos Azure Defender

O Azure Defender fornece alertas de segurança e proteção avançada contra ameaças para máquinas virtuais, bancos de dados SQL, contêineres, aplicativos Web, sua rede, entre outros.

Quando você habilita o Azure Defender na área Preços e configurações da Central de Segurança do Azure, os seguintes planos do Defender são todos habilitados simultaneamente e fornecem proteções abrangentes para as camadas de computação, dados e serviço do seu ambiente:

- Azure Defender para servidores
- Azure Defender for Serviço de Aplicativo
- Azure Defender para Armazenamento
- Azure Defender para SQL
- Azure Defender para “Kubernetes”
- Azure Defender para registros de contêiner
- Azure Defender para “Key Vault”
- Azure Defender para Resource Manager
- Azure Defender para DNS

5.3 Azure Defender Key Vault

O “Azure Key Vault” é um serviço de nuvem que protege segredos e chaves de criptografia, como certificados, cadeias de conexão e senhas.

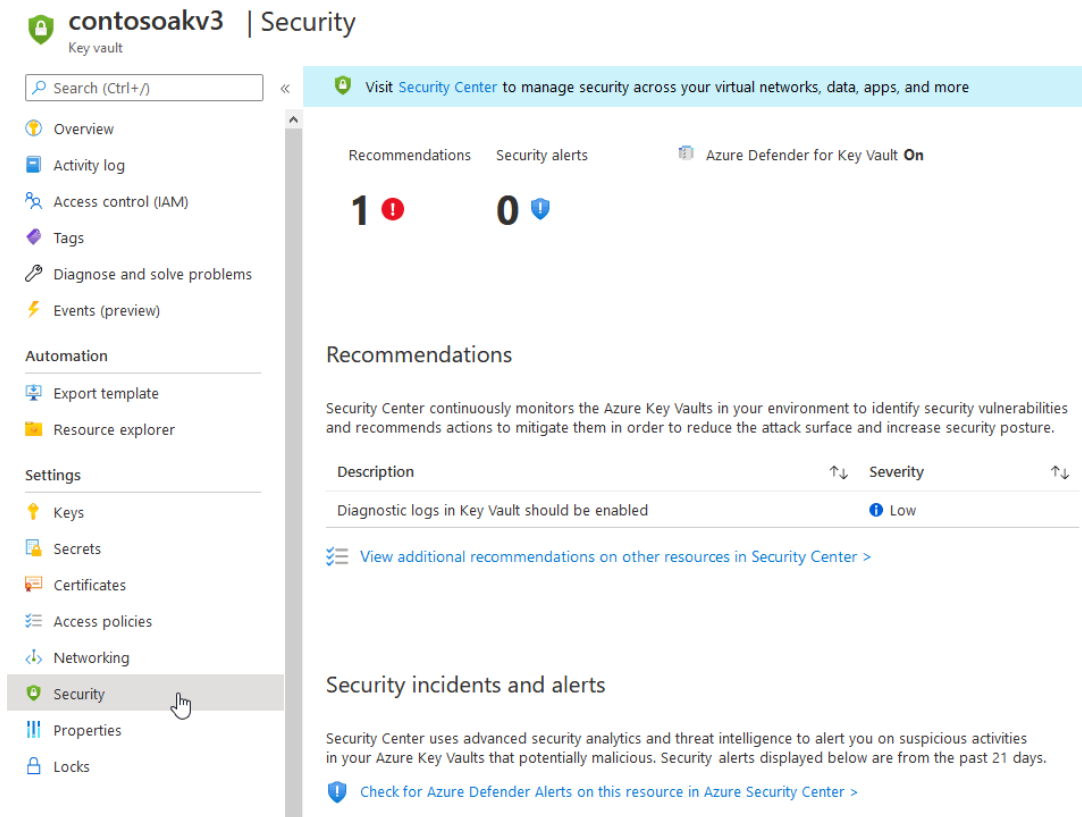
O Azure Defender detecta tentativas incomuns e possivelmente prejudiciais de acessar ou explorar as contas do “Key Vault”. Essa camada de proteção permite que você resolva as ameaças sem ser um especialista em segurança e sem precisar gerenciar sistemas de monitoramento de segurança de terceiros.

Quando ocorrem atividades incomuns, o Azure Defender mostra alertas e opcionalmente, envia alertas por e-mail para os membros relevantes da organização.

Esses alertas incluem detalhes das atividades suspeitas e recomendações sobre como investigar e corrigir ameaças.

Na Figura 6 vemos o painel do “Azure Defender Key Vault”:

Figura 6 - Azure Defender Key Vault

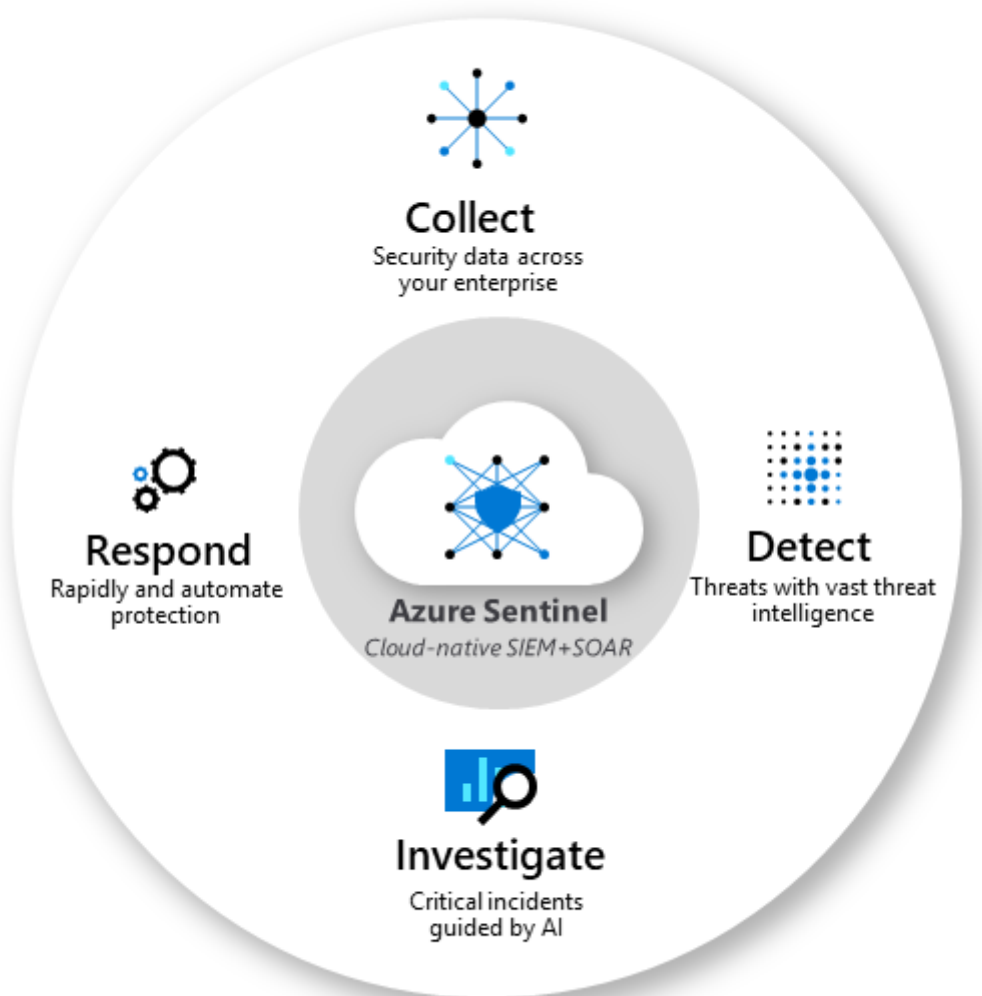


Fonte: <https://docs.microsoft.com/pt-br/azure/security-center/defender-for-key-vault-introduction>

5.4 Azure Sentinel

O Microsoft Azure Sentinel é uma solução escalonável e nativa de nuvem para gerenciamento de eventos e informações de segurança (SIEM) e resposta automatizada de orquestração de segurança (SOAR). O Azure Sentinel oferece análise inteligente de segurança e inteligência contra ameaças em toda a empresa, fornecendo uma única solução para detecção de alertas, visibilidade de ameaças, procura proativa e resposta a ameaças. Na Figura 7 vemos o Azure Sentinel e suas aplicações:

Figura 7 - Azure Sentinel



Fonte: <https://blog.atwork.at/post/Monitor-overview-of-Azure-services>

O Azure Sentinel é a exibição geral da empresa, amenizando o estresse de ataques cada vez mais sofisticados, volumes crescentes de alertas e longos períodos de resolução.

Coletando dados na escala de nuvem de todos os usuários, dispositivos, aplicativos e infraestrutura, local e em nuvens usadas no ambiente.

Detecta ameaças não detectadas antes por outros produtos e minimiza falsos positivos usando a análise e a inteligência contra ameaças incomparáveis da Microsoft.

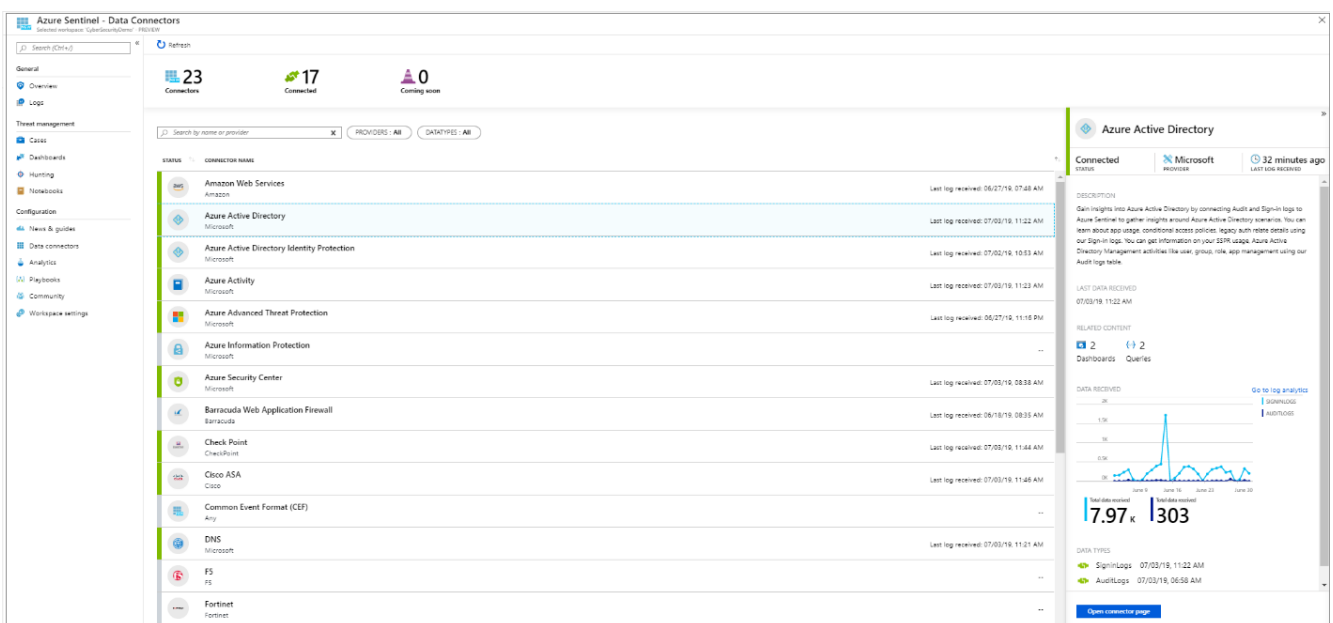
Investiga ameaças com inteligência artificial e busca por atividades suspeitas em escala, acessando anos de trabalho sobre segurança cibernética da Microsoft.

Responde a incidentes de forma rápida com orquestração interna e automação de tarefas comuns.

5.4.1 Conectores

Na Figura 8 vemos um exemplo de conectores que podemos adicionar ao Azure Sentinel:

Figura 8 - Conectores Azure Defender



Fonte: <https://www.cloudfronts.com/create-azure-connector-with-armazure-resource-manager>

configuration/

Para a integração do Azure Sentinel, você precisa primeiro se conectar às suas fontes de segurança. O Azure Sentinel vem com vários conectores para soluções da Microsoft, disponíveis prontamente e fornecendo integração em tempo real, incluindo as soluções do Microsoft 365 Defender (anteriormente conhecido como Proteção contra Ameaças da Microsoft) e fontes do Microsoft 365, incluindo o Office 365, Azure AD, Microsoft

Defender para Identidade (anteriormente, ATP do Azure), Microsoft Cloud App Security e muito mais. Além disso, existem conectores internos no ecossistema de segurança mais amplo para soluções que não são da Microsoft. Você também pode usar formato comum de eventos, Syslog ou API REST para conectar suas fontes de dados ao Azure Sentinel.

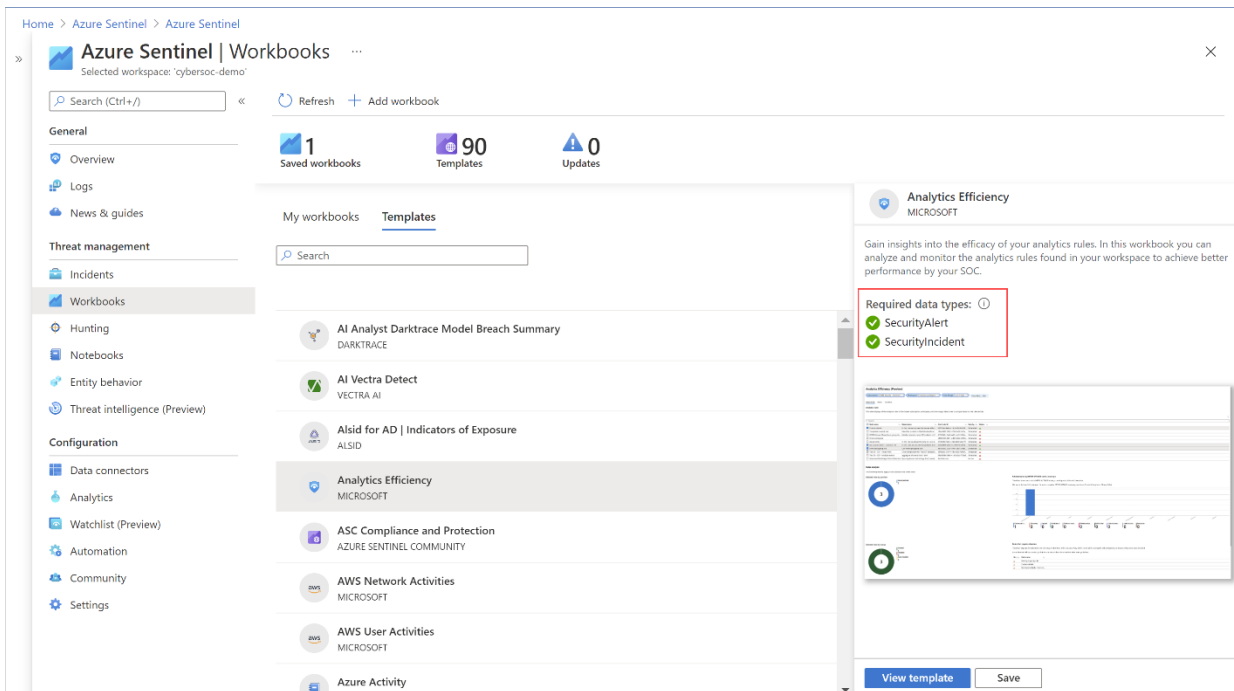
5.4.2 Pastas de Trabalho – Workbooks

Depois de conectar suas fontes de dados ao Azure Sentinel, você poderá monitorar os dados usando a integração do Azure Sentinel às Pastas de Trabalho do Azure Monitor, que oferece versatilidade na criação de pastas de trabalho personalizadas.

Embora as Pastas de Trabalho sejam exibidas de maneiras diferentes no Azure Sentinel, pode ser útil para você ver como Criar relatórios interativos com as Pastas de Trabalho do Azure Monitor. O Azure Sentinel permite que você crie pastas de trabalho personalizadas em seus dados e vem com modelos de pasta de trabalho internos para que você possa obter insights rapidamente em seus dados assim que você conectar uma fonte de dados.

Na Figura 9 vemos exemplos de Templates a serem aplicados no Workbook:

Figura 9 - Azure Wokbooks



Fonte: <https://docs.microsoft.com/pt-pt/azure/sentinel/tutorial-monitor-your-data>

5.4.3 Análise e Incidentes

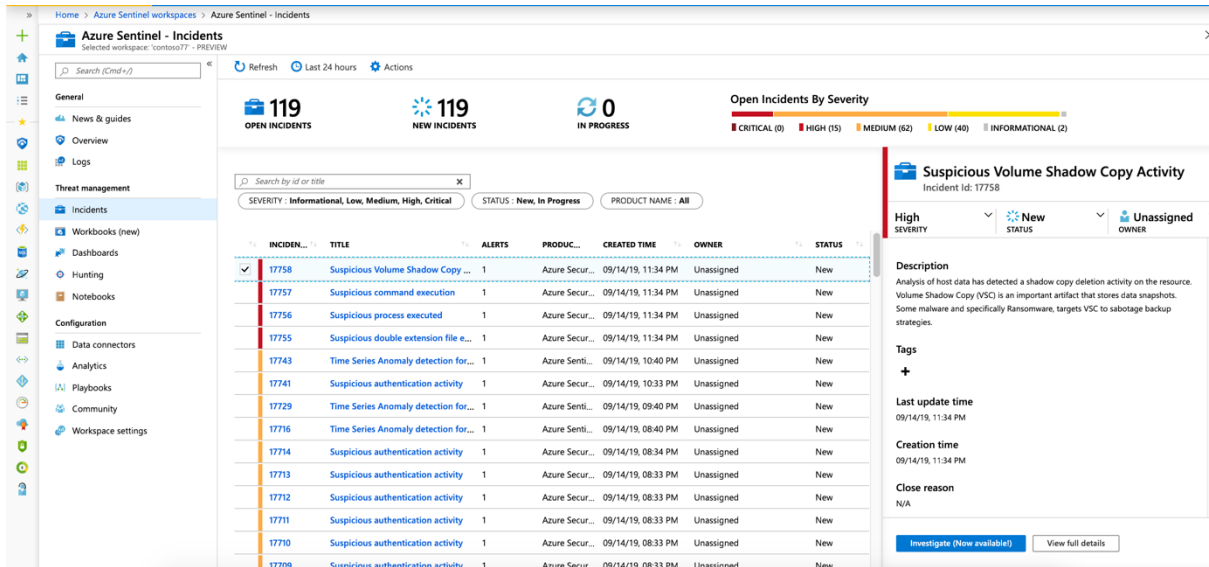
Para ajudar a reduzir o ruído e a minimizar o número de alertas que você precisa examinar e investigar, o Azure Sentinel usa análise para correlacionar os alertas aos incidentes. Incidentes são grupos de alertas relacionados que, juntos, criam uma possível ameaça acionável que você pode investigar e resolver.

Use as regras de correlação internas no estado em que se encontram ou use-as como ponto de partida para criar suas próprias. O Azure Sentinel também fornece regras de aprendizado de máquina para mapear o comportamento da rede e, em seguida, buscar anomalias em todos os seus recursos.

Essas análises ligam os pontos, pois combinam alertas de baixa fidelidade sobre diferentes entidades em possíveis incidentes de segurança de alta fidelidade.

Na Figura 10 vemos um exemplo de incidentes no Azure Sentinel:

Figura 10 - Azure Incidentes



Fonte: <https://docs.microsoft.com/pt-br/azure/sentinel/tutorial-investigate-cases>

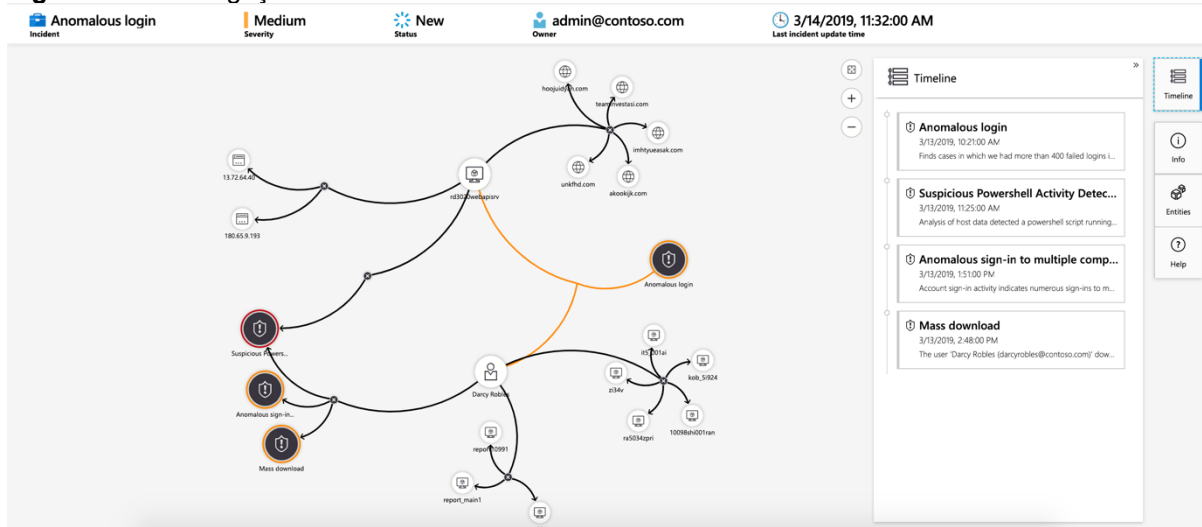
5.4.4 Investigação

Em versão prévia no momento, as ferramentas de investigação profunda do Azure Sentinel ajudam a entender o escopo e a encontrar a causa raiz de uma possível ameaça à segurança.

Você pode escolher uma entidade no gráfico interativo para fazer perguntas interessantes para uma entidade específica, além de fazer uma busca detalhada nessa entidade e em suas conexões para chegar à causa raiz da ameaça.

Na Figura 11 vemos um exemplo de investigação e a Timeline do evento ocorrido:

Figura 11 - Investigação e Timeline



Fonte: <https://docs.microsoft.com/pt-br/azure/sentinel/tutorial-investigate-cases>

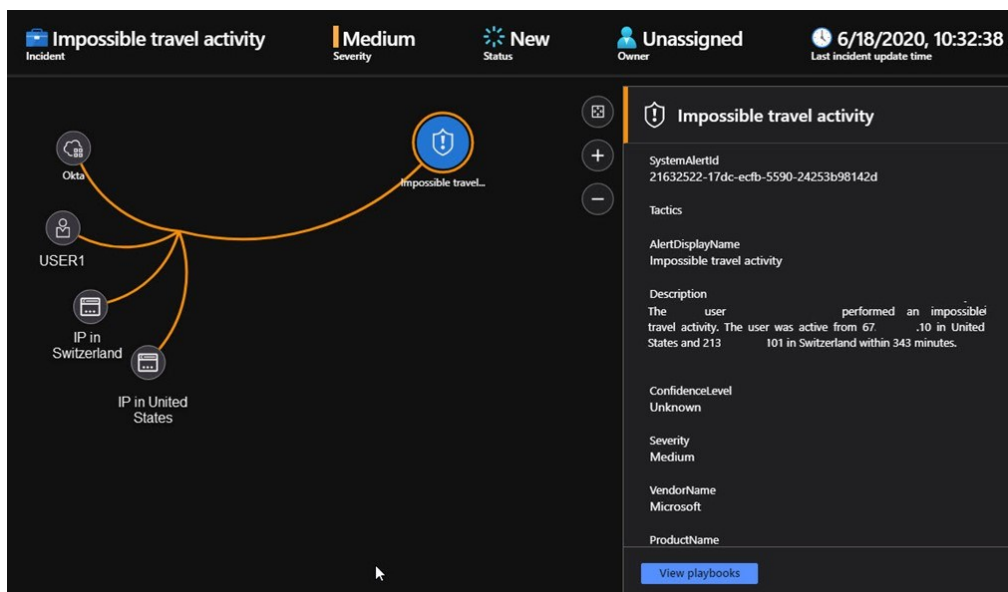
6 - Uso Prático

6.1 – Incidentes de Rotina

“Impossible Travel” – Viagem Impossível

Na Figura 12 vemos um exemplo de Viagem impossível:

Figura 12 - Impossible Travel



Fonte: <https://blog.johnjoyner.net/sso-is-your-doorkeeper-watch-it-with-azure-sentinel/>

Este incidente identifica duas entradas provenientes de locais geograficamente distantes, em que pelo menos um dos locais também pode ser atípico para o usuário, dado o comportamento passado.

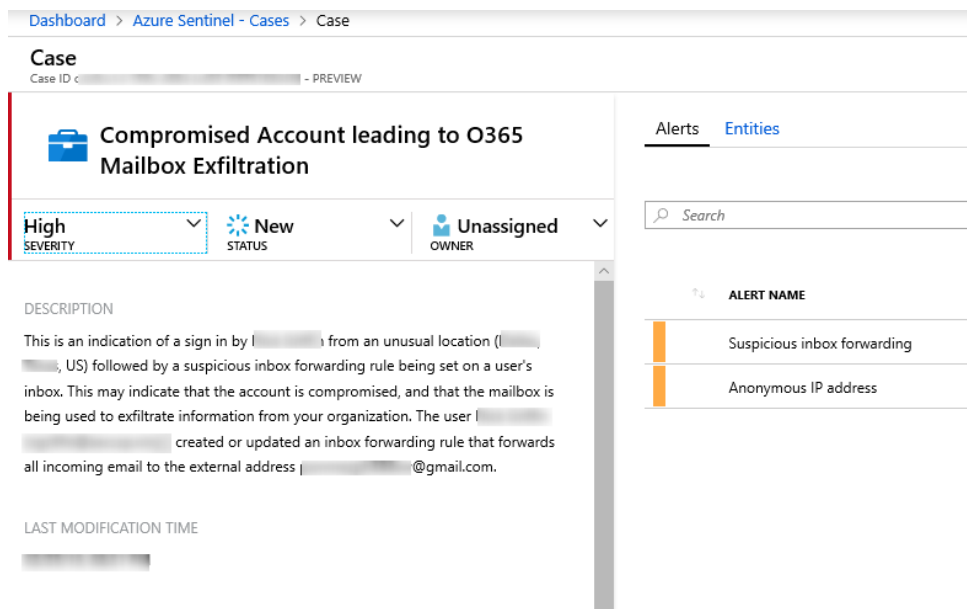
Entre muitos outros fatores, esse algoritmo de aprendizado de máquina leva em consideração o tempo entre as duas entradas e o tempo que seria necessário para o usuário ir do primeiro até o segundo local, indicando que um usuário diferente está usando as mesmas credenciais.

Muitas vezes encontramos falsos positivos pois usuários usam VPN's em que simulam IP's de outras localidades. Este Incidente é muito útil para detectar contas vazadas ou contas comprometidas. Vemos muitos alertas vindos da Nigéria, Itália e Rússia que são provenientes de contas que foram comprometidas.

Encaminhamento suspeito da caixa de entrada

Na Figura 13 vemos um exemplo de incidente de encaminhamento suspeito de e-mails:

Figura 13 - Encaminhamento suspeito de E-mails



The screenshot shows the Azure Sentinel interface for a specific case. The breadcrumb navigation at the top reads 'Dashboard > Azure Sentinel - Cases > Case'. Below this, the case title is 'Compromised Account leading to O365 Mailbox Exfiltration'. The alert severity is 'High', the status is 'New', and the owner is 'Unassigned'. A search bar is visible on the right side of the alert details. The description of the alert states: 'This is an indication of a sign in by [redacted] from an unusual location ([redacted], US) followed by a suspicious inbox forwarding rule being set on a user's inbox. This may indicate that the account is compromised, and that the mailbox is being used to exfiltrate information from your organization. The user [redacted] created or updated an inbox forwarding rule that forwards all incoming email to the external address [redacted]@gmail.com.' The 'ALERT NAME' section on the right lists two related alerts: 'Suspicious inbox forwarding' and 'Anonymous IP address'.

Fonte: <https://techdailychronicle.com/advanced-multistage-attack-detection%E2%80%8A-%E2%80%8Areal-machine-learning-for-the-real-world/>

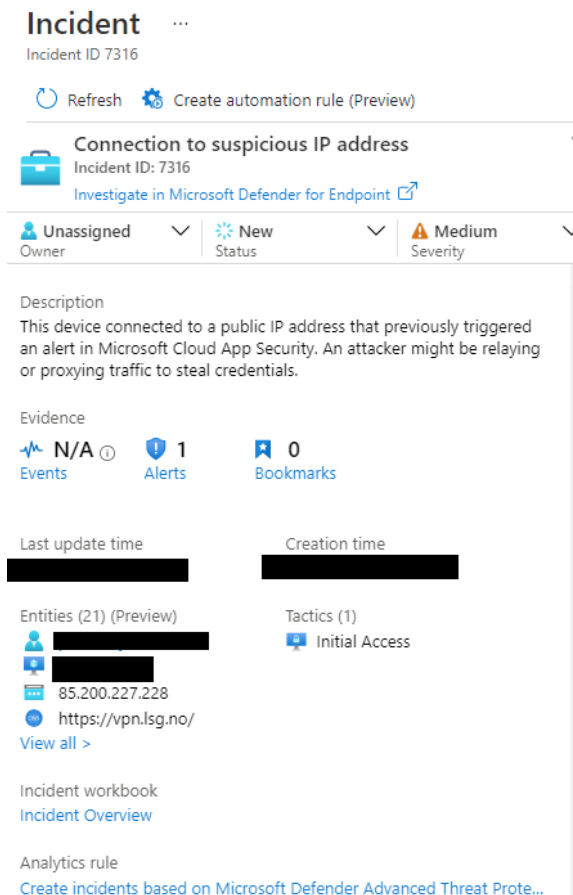
Essa detecção é descoberta pelo MCAS (Microsoft Cloud App Security). Essa detecção procura regras de encaminhamento de e-mail suspeito, por exemplo, se um usuário criou uma regra de caixa de entrada que encaminha uma cópia de todos os e-mails para um endereço externo.

Essa detecção analisa o ambiente e dispara alertas quando regras suspeitas que excluem ou movem mensagens ou pastas são definidas na caixa de entrada de um usuário. Isso pode indicar que a conta de usuário está comprometida, que as mensagens foram ocultadas de forma intencional e que a caixa de correio está sendo usada para enviar spam e malware em sua organização.

“Connection to suspicious IP address”

Na Figura 14 vemos um exemplo de incidente “Conexão suspeita a um endereço IP”:

Figura 14 - Conexão Suspeita a um Endereço IP



The screenshot displays the Microsoft Defender for Endpoint interface for an incident. At the top, it shows 'Incident ID 7316' and options to 'Refresh' or 'Create automation rule (Preview)'. The incident title is 'Connection to suspicious IP address' with a sub-title 'Incident ID: 7316' and a link to 'Investigate in Microsoft Defender for Endpoint'. Below this, there are filters for 'Owner' (Unassigned), 'Status' (New), and 'Severity' (Medium). The 'Description' section states: 'This device connected to a public IP address that previously triggered an alert in Microsoft Cloud App Security. An attacker might be relaying or proxying traffic to steal credentials.' The 'Evidence' section shows 'N/A' for Events, '1' for Alerts, and '0' for Bookmarks. There are fields for 'Last update time' and 'Creation time', both of which are redacted with black boxes. The 'Entities (21) (Preview)' section lists a user, a device, the IP address '85.200.227.228', and the URL 'https://vpn.lsg.no/'. The 'Tactics (1)' section shows 'Initial Access'. At the bottom, there is an 'Incident workbook' link to 'Incident Overview' and an 'Analytics rule' section with a link to 'Create incidents based on Microsoft Defender Advanced Threat Prote...'

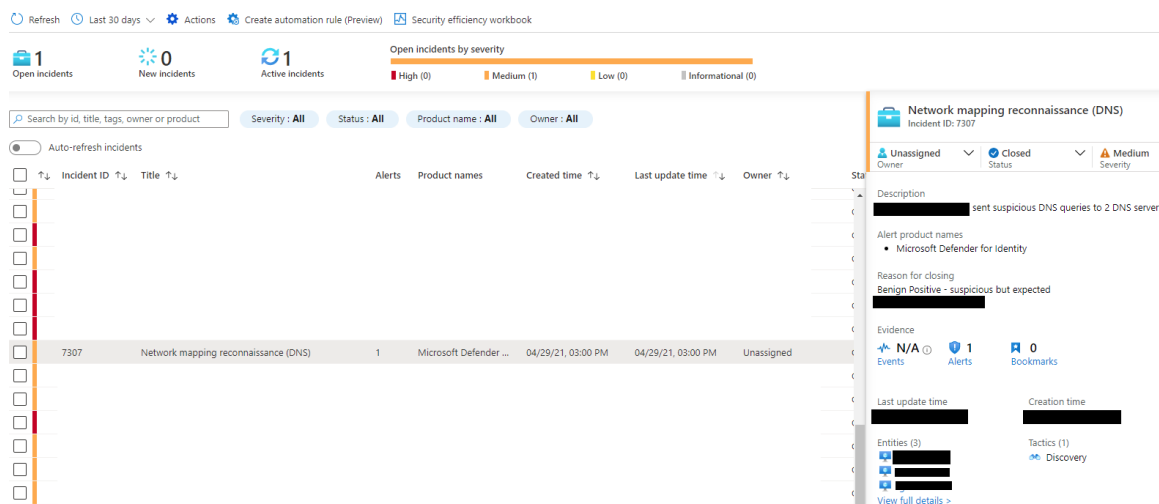
Fonte: Próprio Autor

Este dispositivo se conectou a um endereço IP público que acionou anteriormente um alerta no Microsoft Cloud App Security. Um invasor pode estar retransmitindo ou proxy de tráfego para roubar credenciais.

Network Mapping Reconnaissance (DNS) – Reconhecimento de Mapeamento de Rede

Na Figura 15 vemos um exemplo de incidente “Reconhecimento de Mapeamento de Rede”:

Figura 15 - Reconhecimento de Mapeamento de Rede



Fonte: Próprio Autor

O servidor DNS contém um mapa de todos os computadores, endereços IP e serviços em sua rede. Essas informações são usadas pelos invasores para mapear sua estrutura de rede e visar computadores interessantes para etapas posteriores no ataque.

Há vários tipos de consulta no protocolo DNS. Esse alerta de segurança do Defender para Identidade detecta solicitações suspeitas, seja em solicitações que usam uma AXFR (transferência) proveniente de servidores não DNS ou naquelas que usam um número excessivo de solicitações.

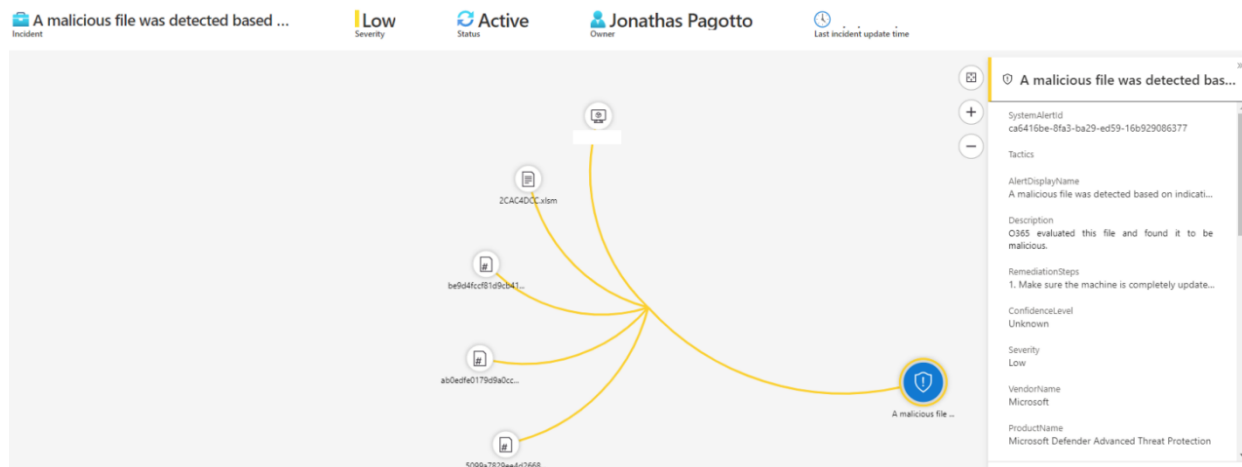
Procure usuários que estavam conectados no mesmo período em que a atividade ocorreu, pois eles também podem estar comprometidos.

Redefina suas senhas e habilite a MFA ou, se você tiver configurado as políticas relevantes de usuário de alto risco no Azure Active Directory Identity Protection, poderá usar a ação Confirmar usuário comprometido no portal do Cloud App Security.

“A malicious file was detected based on indication provided by O365” – Um Arquivo Malicioso foi detectado com uma indicação do O365.

Na Figura 16 vemos um exemplo de Arquivo Malicioso detectado:

Figura 16 - Um arquivo Malicioso foi detectado



Fonte: Próprio Autor

Alerta bastante comum mostrando que o malware foi previamente observado e bloqueado em uma organização protegida pelo ATP do Office 365 que integra com o Azure Sentinel.

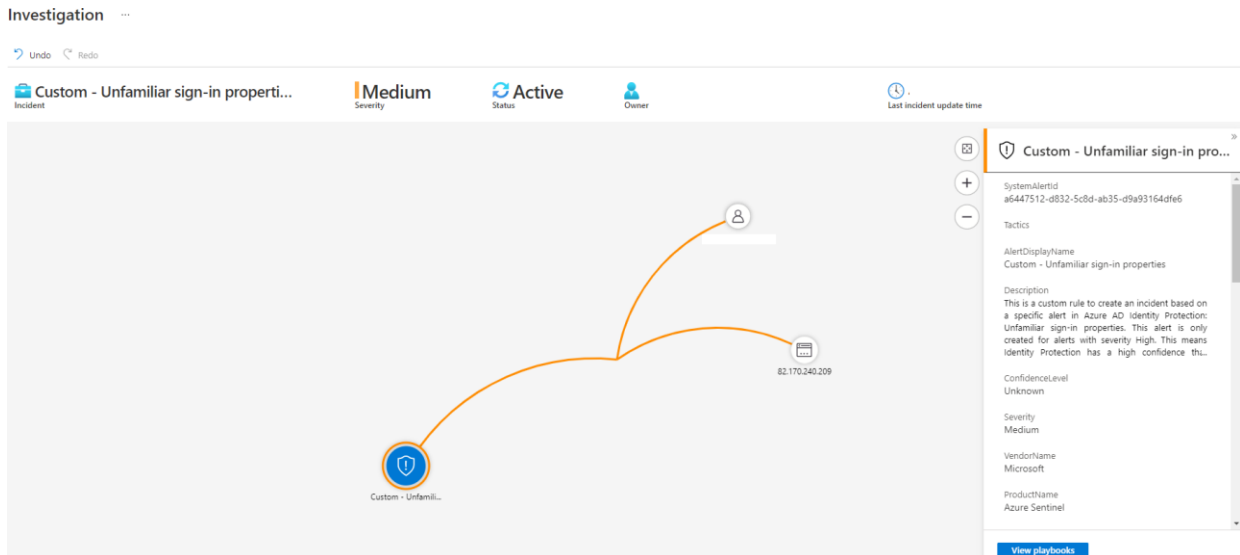
Usando informações do ATP do Office 365, o Microsoft Defender ATP EDR imediatamente gerou um alerta ao encontrar o arquivo em outras organizações, enquanto as proteções baseadas em nuvem bloqueavam o arquivo nessas organizações.

Neste caso se tratava de um macro existente em um falso arquivo Excel enviada via Phishing. O próprio sistema detectou, bloqueou, excluiu e gerou um alerta a equipe responsável.

Unfamiliar Sign-in Properties – Propriedades de Login Desconhecidas

Na Figura 17 vemos um exemplo de Propriedades de Login desconhecidos.

Figura 17 - Propriedades de Login Desconhecidas



Fonte: Próprio Autor

Esse tipo de detecção de risco considera o histórico de entrada anterior (IP, latitude/longitude e ASN) para procurar por entradas anormais. O sistema armazena informações sobre os locais anteriores usados por um usuário e considera esses locais "familiares".

A detecção de risco é disparada quando a entrada ocorre de um local que ainda não está na lista de locais familiares. Os usuários recém-criados estarão no "modo de aprendizado" por um período em que as propriedades de entrada desconhecidas as detecções de risco serão desativadas enquanto nossos algoritmos aprendem o comportamento do usuário.

A duração do modo de aprendizado é dinâmica e depende de quanto tempo leva o algoritmo para reunir informações suficientes sobre os padrões de entrada do usuário. A duração mínima é de cinco dias.

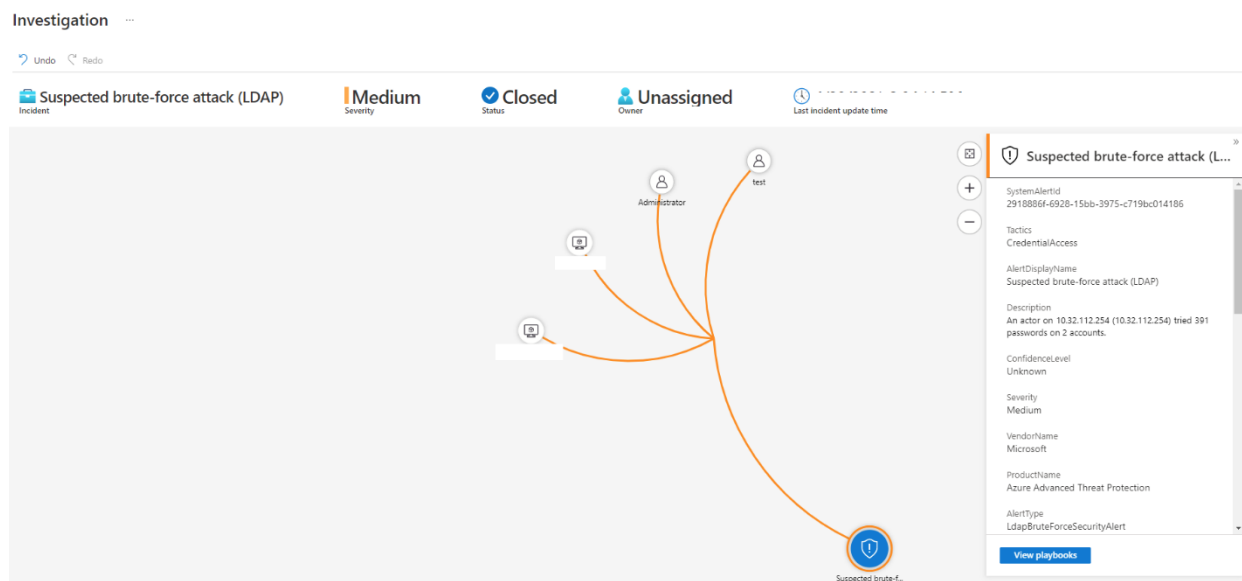
Um usuário pode voltar para o modo de aprendizado após um longo período de inatividade. O sistema também ignora entradas de dispositivos conhecidos e locais que são geograficamente próximos de uma localização familiar.

Também podemos executar essa detecção para a autenticação Básica (ou protocolos herdados). Como esses protocolos não têm propriedades modernas como a ID do cliente, há uma telemetria limitada para reduzir os falsos positivos. Recomendamos que nossos clientes mudem para a autenticação moderna.

Suspected brute-force attack (LDAP) – Suspeita de Ataque de Força Bruta

Na Figura 18 vemos um exemplo de Suspeita de Ataque de Força Bruta:

Figura 18 - Suspeita de Ataque de Força Bruta



Fonte: Próprio Autor

Em um ataque de força bruta, o invasor tenta a autenticação usando várias senhas em diferentes contas até que uma senha correta seja encontrada ou usando uma senha em uma pulverização de senhas de grande escala que funcione para pelo menos uma conta. Uma vez descoberta, o invasor entra usando a conta autenticada.

Nessa detecção, um alerta é disparado quando ocorrem diversas falhas de autenticação usando Kerberos ou NTLM ou ainda quando o uso de uma pulverização de senhas é detectado. Por meio do Kerberos ou NTLM, esse tipo de ataque geralmente é realizado em esquema horizontal, usando um pequeno conjunto de senhas com vários

usuários, ou vertical, com um grande conjunto de senhas com poucos usuários ou uma combinação dos dois.

Em uma pulverização de senhas, depois de enumerar com êxito uma lista de usuários válidos do controlador de domínio, os invasores tentam UMA senha cuidadosamente concebida em TODAS as contas de usuário conhecidas (uma senha para várias contas).

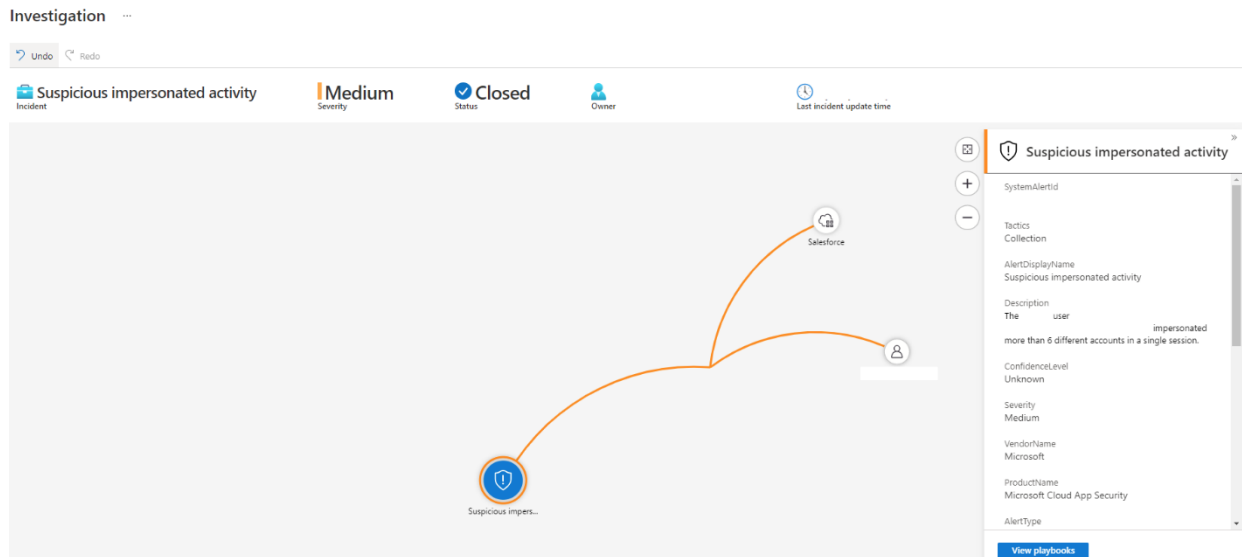
Se a pulverização de senhas inicial falhar, eles tentam novamente utilizando uma senha diferente cuidadosamente concebida, normalmente após aguardar 30 minutos entre as tentativas. Esse tempo de espera permite que os invasores evitem disparar a maioria dos limites de bloqueio de conta que se baseiam no tempo.

A pulverização de senhas tornou-se rapidamente uma técnica de preferência entre os invasores e testadores de intrusão. Os ataques de pulverização de senhas se mostraram eficazes na conquista de uma entrada na organização e por fazer movimentos laterais posteriores, tentando aumentar os privilégios. O período mínimo antes que um alerta possa ser disparado é de uma semana.

Suspicious impersonated activity - Atividade suspeita de falsificação de identidade

Na Figura 19 vemos um exemplo de Atividade Suspeita de falsificação de identidade:

Figura 19 - Atividade Suspeita de Falsificação de Identidade



Fonte: Próprio Autor

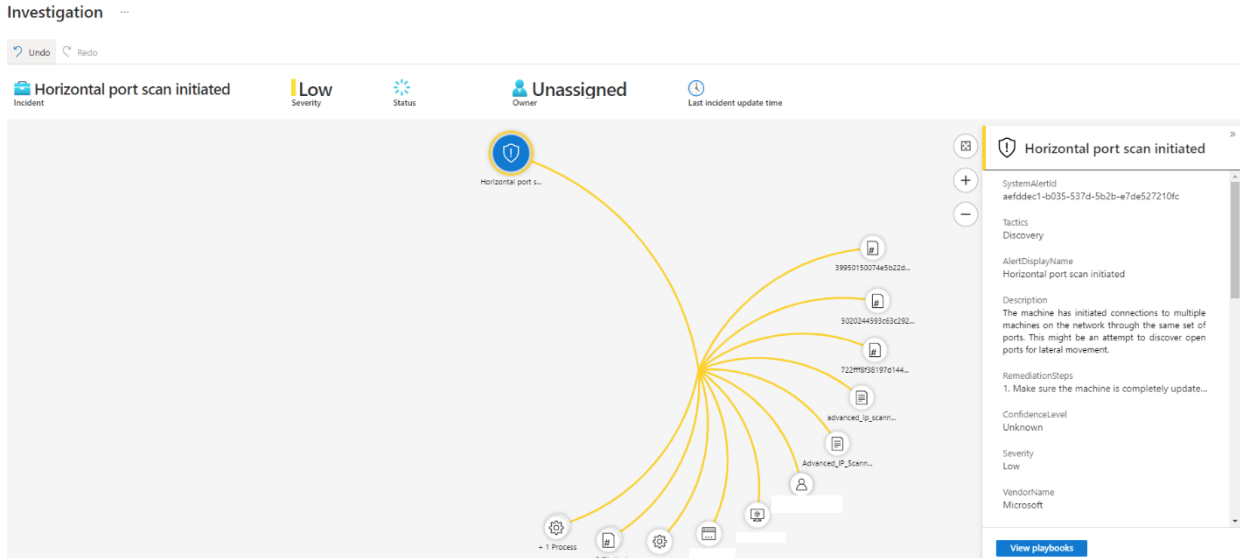
Em alguns softwares, existem opções para permitir que outros usuários se façam passar por outros usuários. Por exemplo, os serviços de e-mail permitem que os usuários autorizem outros usuários a enviar e-mail em seu nome.

Essa atividade é comumente usada por invasores para criar e-mails de Phishing na tentativa de extrair informações sobre sua organização. O Cloud App Security cria uma linha de base com base no comportamento do usuário e cria uma atividade quando uma atividade de personificação incomum é detectada.

Horizontal port scan initiated - Varredura de porta horizontal iniciada

Na Figura 20 vemos um exemplo de Varredura de Porta Horizontal:

Figura 20 - Varredura de Porta Horizontal

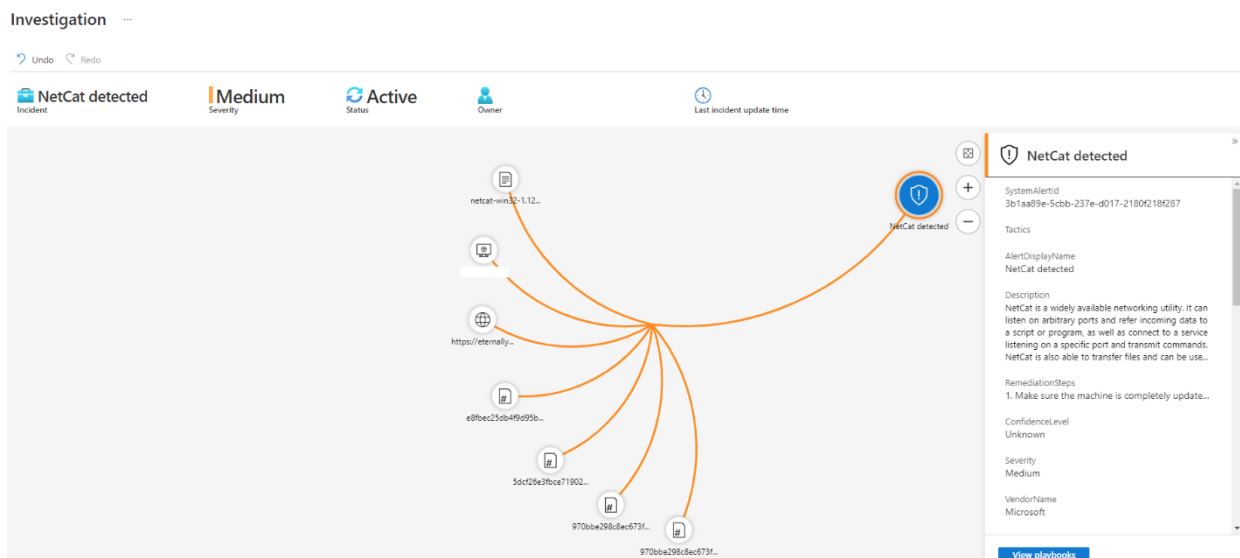


Fonte: Próprio Autor

A máquina iniciou conexões com várias máquinas na rede por meio do mesmo conjunto de portas. Isso pode ser uma tentativa de descobrir portas abertas para movimento lateral.

Net Cat Detectado

Na Figura 21 vemos um exemplo de NetCat detectado: **Figura 21** - NetCat Detectado



Fonte: Próprio Autor

NetCat é um utilitário de rede amplamente disponível. Ele pode escutar em portas arbitrárias e referir os dados de entrada a um script ou programa, bem como conectar-se a um serviço escutando em uma porta específica e transmitir comandos.

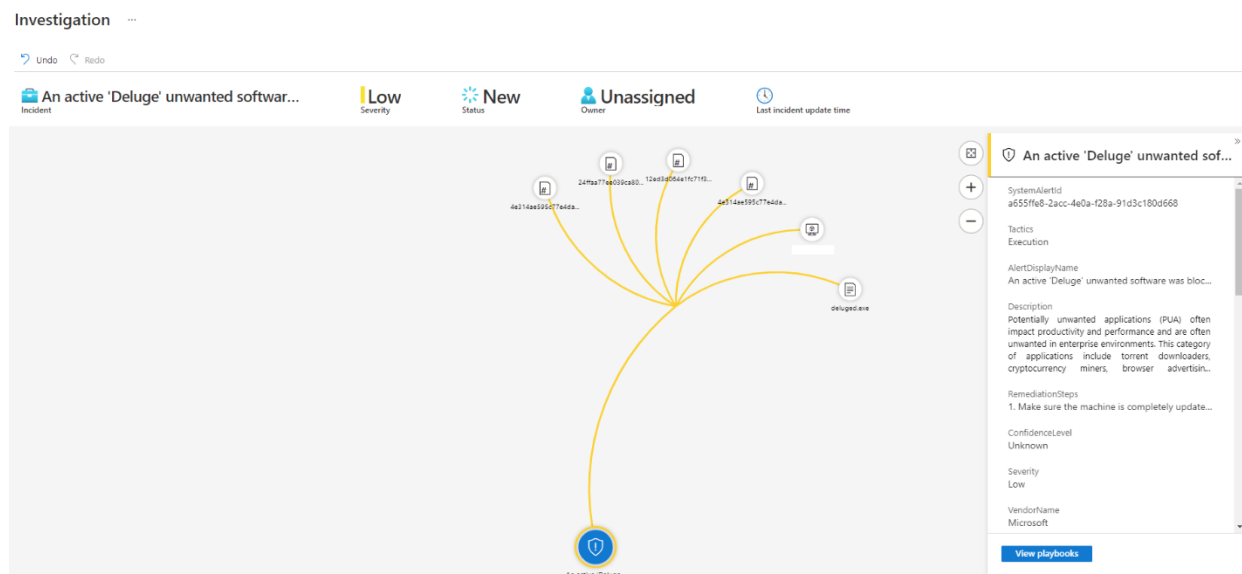
NetCat também é capaz de transferir arquivos e pode ser usado como proxy relay ou backdoor.

Neste incidente foi detectado que um desenvolvedor de software da empresa estava usando o aplicativo para fins de pesquisa, ou seja, falso positivo.

An active 'Deluge' unwanted software was blocked

Na Figura 22 vemos um exemplo de Software suspeito bloqueado:

Figura 22 - Software Indesejado Bloqueado



Fonte: Próprio Autor

Aplicativos potencialmente indesejados geralmente afetam a produtividade e o desempenho de estações de trabalho e são frequentemente indesejados em ambientes corporativos além de trazer problemas de performance. Esta categoria de aplicativos incluem aplicativos como: Gerenciadores de torrent, Mineradores de criptomoedas, Softwares de publicidade em navegadores e Softwares de evasão.

Um aplicativo é considerado ativo se for encontrado em execução na máquina ou se já tiver mecanismos de persistência em vigor. Como este PUA estava ativo, tomei medidas de precaução e verifiquei se há sinais residuais de infecção.

7 – Conclusão

Com a elaboração deste trabalho, apresentei o conceito, técnicas e aplicações dentro do Azure Security Center. No meu ponto de vista o Azure Security Center é uma ótima solução integrada para a segurança da informação em um ambiente corporativo de médio a grande porte.

Creio que a solução não é muito usada no Brasil devido ao alto valor de licenciamento dos produtos envolvidos (Microsoft), a empresa que eu trabalho tem sede da Europa, o que facilita o acesso a solução.

Atualmente no Brasil vemos bastante soluções de segurança baseadas em soluções Linux que são mais acessíveis e com bastante mercado no Brasil e com mais profissionais capacitados a operar a ferramenta, o que difere do Azure Security Center em que localmente tenho apenas um colega que trabalha com a mesma ferramenta, os demais todos residem na Europa.

6 - Fontes Bibliográficas

- Microsoft . (Junho de 2019). *Documentação do Azure*. Fonte: Documentação do Azure: <https://docs.microsoft.com/pt-br/azure/?product=security>
- Microsoft . (Junho de 2019). *Documentação do Azure Sentinel*. Fonte: Documentação do Azure Sentinel: <https://docs.microsoft.com/pt-br/azure/sentinel/>
- Microsoft . (04 de 05 de 2021). *Behavioral blocking and containment: Transforming optics into protection*. Fonte: <https://www.microsoft.com/security/blog/2020/03/09/behavioral-blocking-and-containment-transforming-optics-into-protection/#:~:text=The%20alert%2C%20%E2%80%9CA%20malicious%20file,protected%20by%20Office%20365%20ATP.>
- Microsoft . (29 de Abril de 2021). *O que é proteção de identidade?* Fonte: <https://docs.microsoft.com/pt-br/azure/active-directory/identity-protection/overview-identity-protection>
- Microsoft . (03 de Maio de 2021). *Tutorial: Alertas de reconhecimento*. Fonte: Tutorial: Alertas de reconhecimento: <https://docs.microsoft.com/pt-br/defender-for-identity/reconnaissance-alerts>
- Microsoft. (Junho de 2019). *Azure*. Fonte: Azure: <https://azure.microsoft.com/pt-br/services/security-center/>
- Microsoft. (Junho de 2019). *Azure Documentation*. Fonte: Azure Documentation: <https://docs.microsoft.com/pt-br/azure/?product=featured>
- Microsoft. (2021). *Infraestrutura Global* . Fonte: Infraestrutura Global : <https://azure.microsoft.com/pt-br/global-infrastructure/>
- Microsoft. (17 de Fevereiro de 2021). *Security Center Introduction*. Fonte: <https://docs.microsoft.com/pt-br/azure/security-center/security-center-introduction>