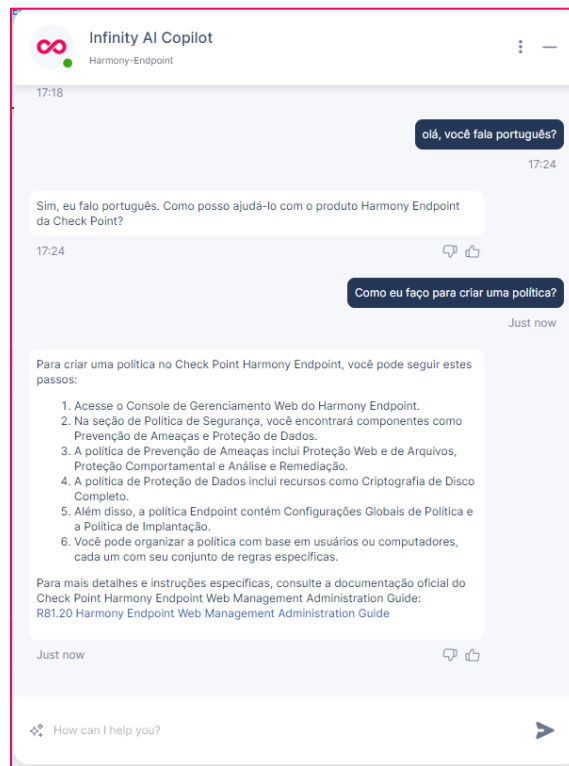


Automatizando tarefas e acelerando a investigação de eventos com o Copilot no Harmony Endpoint

A inteligência artificial aplicada à ciberataques vem sendo pauta já há algum tempo, mas em 2024 o tema ficou ainda mais em voga no mercado de cibersegurança. Os grandes players do mercado estão cada vez mais utilizando IA para tratamento e consumo de informações que são transacionadas nas ferramentas e como extrair valor disso para melhorar a experiência do usuário e facilitar as tarefas diárias dos administradores. O Infinity AI Copilot aprimora a administração da ferramenta Harmony Endpoint e entrega uma excelente experiência de investigação e tratamento das informações até para usuários mais inexperientes da ferramenta.

Podemos agilizar tarefas mais corriqueiras, como pedir a relação de máquinas e usuários mais atacados, até investigações de incidentes de forma mais aprofundada. Vamos começar com uma pergunta simples (lembrando que o AI Copilot suporta diversos idiomas, incluindo português):



Agora vamos pedir algumas informações que demorariam alguns cliques para serem consultadas. Podemos fazer isso de forma simples e rápida usando o Copilot:

Quais foram os endpoints que receberam a maior quantidade de tráfego nos últimos 7 dias?

Just now

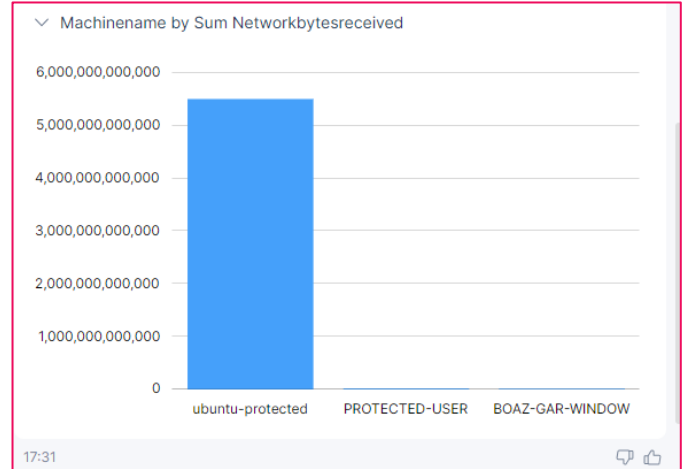
Com base nos registros dos últimos 7 dias, os endpoints que receberam a maior quantidade de tráfego foram:

1. **ubuntu-protected:** 5.498.593.344.984 bytes
2. **PROTECTED-USER:** 8.468.803.569 bytes
3. **BOAZ-GAR-WINDOW:** 4.258.673.321 bytes

Essas são as máquinas que tiveram o maior volume de tráfego de rede nos últimos 7 dias. Se precisar de mais informações ou detalhes específicos, estou à disposição para ajudar.

> Machinename by Sum Networkbytesreceived

Just now



Note que ao final da resposta o prompt ainda entrega um gráfico com as máquinas listadas e a quantidade de bytes recebidos por cada um deles. E se a organização estiver preocupada, por exemplo, com campanhas de phishing que tiveram seus endpoints como alvo? Podemos fazer a investigação de incidentes de forma simples e organizar essas informações em tabelas e gráficos.

Liste as tentativas de phishing detectadas e prevenidas pela ferramenta no ano de 2024 e coloque-as em uma tabela

Just now

Aqui está uma tabela com as tentativas de phishing detectadas e prevenidas pela ferramenta Harmony Endpoint no ano de 2024:

ID do Incidente	Status do Ataque	Modo de Aplicação	Motor de Detecção	Descrição da Detecção
0f133584-2a39-42d6-a8b8-6cd20fda0eeb	Bloqueado	Prevenido	Harmony Agent for Browsers	Para excluir o arquivo: Adicione esta exclusão de sha1 no Gerenciamento do Harmony Endpoint: d2726507-4c9eac2e-2122ed69-294dbc4d-7cce9141
bd881c63-5d71-40d6-8cff-7e65435c5f72	Bloqueado	Prevenido	Harmony Agent for Browsers	Para excluir o arquivo: Adicione esta exclusão de sha1 no Gerenciamento do Harmony Endpoint: e2758b33-2defa4e1-bb9af936-6c73e714-974e7dbc
b95d3405-9843-473e-b00d-7765506e1262	Bloqueado	Prevenido	Harmony Agent for Browsers	Para excluir o arquivo: Adicione esta exclusão de sha1 no Gerenciamento do Harmony Endpoint: f1dacb65-048287d4-3977730e-f87da831-9f41fd00
6dce5aac-d3d3-4e14-9d8a-dcdf2f81f910	Bloqueado	Prevenido	Harmony Agent for Browsers	Para excluir o arquivo: Adicione esta exclusão de sha1 no Gerenciamento do Harmony Endpoint: f1dacb65-048287d4-3977730e-f87da831-9f41fd00

Atividades corriqueiras que poderiam custar muito mais tempo ao administrador, são executadas de forma simples e rápida, basta apenas saber fazer as perguntas certas.

Mostre-me os top 10 endereços IP que se comunicaram com a máquina DESKTOP-SEP574A desde o início do Ano?

17:53

Aqui estão os 10 principais endereços IP que se comunicaram com a máquina DESKTOP-SEP574A desde o início do ano:

1. **192.168.1.175**: 645.977 comunicações
2. **Endereço IP em branco**: 160.657 comunicações
3. **fe80::225c:e8c9:8b3d:a2cb**: 124.387 comunicações
4. **192.168.142.133**: 29.854 comunicações
5. **192.168.140.136**: 27.563 comunicações
6. **192.168.143.63**: 17.954 comunicações
7. **10.8.189.61**: 17.584 comunicações
8. **192.168.142.96**: 17.310 comunicações
9. **192.168.143.193**: 17.048 comunicações
10. **192.168.141.194**: 15.418 comunicações

Esses são os endereços IP que mais se comunicaram com a máquina DESKTOP-SEP574A desde o início do ano. Se precisar de mais informações ou detalhes adicionais, estou à disposição para ajudar.

> Networkscip by Count

Para cada endereço IP, mostre-me o tempo mínimo, tempo máximo e a contagem. Formate tudo em uma tabela.

Just now

Aqui está a tabela com os detalhes de tempo mínimo, tempo máximo e contagem para os 10 principais endereços IP que se comunicaram com a máquina DESKTOP-SEP574A desde o início do ano:

Endereço IP	Contagem	Tempo Mínimo	Tempo Máximo
192.168.1.175	645.977	02/01/2024 09:59:34	07/06/2024 00:23:42
Endereço IP em branco	160.657	02/01/2024 09:59:44	07/06/2024 00:20:19
fe80::225c:e8c9:8b3d:a2cb	124.387	02/01/2024 09:59:32	07/06/2024 00:23:08
192.168.142.133	29.854	12/02/2024 07:07:27	14/02/2024 11:01:08
192.168.140.136	27.563	18/01/2024 07:29:19	20/01/2024 05:18:05
192.168.143.63	17.954	12/01/2024 06:57:37	13:35:18
10.8.189.61	17.584	18/05/2024 06:21:53	17/05/2024 04:26:10
192.168.142.96	17.310	22/02/2024 06:33:41	23/02/2024 05:29:39
192.168.143.193	17.048	01/02/2024 07:05:04	01/02/2024 17:23:03
192.168.141.194	15.418	29/02/2024 06:29:55	01/03/2024 05:28:33

Esses são os detalhes de comunicação para os 10 principais endereços IP que se comunicaram com a máquina DESKTOP-SEP574A desde o início do ano. Se precisar de mais informações ou assistência adicional, estou à disposição para ajudar.

Just now

Vamos agora ver como poderíamos fazer uma investigação mais aprofundada sobre incidentes em um endpoint específico:

Mostre os incidentes envolvendo a máquina DESKTOP-SEP574A nos últimos 180 dias

18:27

Nos últimos 180 dias, a máquina DESKTOP-SEP574A teve os seguintes incidentes registrados no sistema monitorado pelo Check Point Harmony Endpoint:

- Atividades Avançadas: 657.030 incidentes
- Arquivos: 4.067.925 incidentes
- Rede: 1.428.193 incidentes
- Processos: 583.941 incidentes
- Registro: 394.285 incidentes
- Logon Remoto: 3.661 incidentes
- Script: 11.042 incidentes
- Execução Indireta: 256 incidentes
- Eventos de Detecção: 52 incidentes

Esses são os tipos de incidentes registrados envolvendo a máquina DESKTOP-SEP574A nos últimos 180 dias. Se precisar de mais informações ou detalhes adicionais, estou à disposição para ajudar.

> Recordtype by Count

Me mostre mais informações a respeito de eventos de execução indireta

Just now

Aqui estão alguns exemplos de eventos de execução indireta envolvendo a máquina DESKTOP-SEP574A nos últimos 180 dias:

1. **Tipo de Execução:** Criação de Serviço
 - **Nome da Execução:** AarSvc_634d99
 - **Detalhes da Execução:** Tipo de Serviço: 224 | Tipo de Inicialização do Serviço: (3) Inicialização sob Demanda | Conta do Serviço: localsystem
 - **Diretório do Processo Alvo da Execução:** c:\windows\system32
 - **Nome do Processo Alvo da Execução:** svchost.exe
 - **PID do Processo Alvo da Execução:** 0
2. **Tipo de Execução:** Criação de Serviço
 - **Nome da Execução:** BcastDVRUserService_634d99
 - **Detalhes da Execução:** Tipo de Serviço: 224 | Tipo de Inicialização do Serviço: (3) Inicialização sob Demanda | Conta do Serviço: localsystem
 - **Diretório do Processo Alvo da Execução:** c:\windows\system32
 - **Nome do Processo Alvo da Execução:** svchost.exe
 - **PID do Processo Alvo da Execução:** 0

Esses são exemplos de eventos de execução indireta registrados envolvendo a máquina DESKTOP-SEP574A nos últimos 180 dias. Se precisar de mais informações ou detalhes adicionais, estou à disposição para ajudar.

Just now

Nos exemplos acima, conseguimos observar como as atividades de busca, leitura e apresentação de informações nos bancos de dados e políticas configuradas do Harmony Endpoint pode ser facilitada e acelerada com o uso do AI Copilot. Operações de escrita, como mudança de políticas ou colocar um endpoint em quarentena ainda estão em desenvolvimento, mas o prompt entende sua pergunta e te dá o passo a passo para executar a ação quando ele não executar a ação por conta própria.

atualize o agente da máquina WIN-NJ51R8APUP7 para a versão 88.20.0.181

18:52

Para atualizar o agente do Check Point Harmony Endpoint na máquina WIN-NJ51R8APUP7 para a versão 88.20.0.181, você precisará seguir os passos abaixo:

1. Acesse o Console de Gerenciamento do Harmony Endpoint.
2. Navegue até a seção de gerenciamento de endpoints.
3. Localize a máquina WIN-NJ51R8APUP7 na lista de endpoints.
4. Selecione a máquina e procure a opção para atualizar o agente.
5. Escolha a versão 88.20.0.181 do agente para ser instalada.
6. Aplique a atualização e siga as instruções adicionais para concluir o processo.

Certifique-se de que a versão 88.20.0.181 esteja disponível e seja compatível com a máquina em questão. Se você encontrar algum problema ou precisar de assistência adicional, entre em contato com o suporte da Check Point.

18:53

