BRIGHT ARTMS

Automatic Real Time Monitoring System

GUIA DO USUÁRIO

V 1.2

BRIGHT SECURITY SERVICES®

ARTMS[1] by XSITE

[1] BRIGHT ARTMS é um produto da XSITE Consultoria e Tecnologia,
CNPJ 40.584.096/0001-05.

SUMÁRIO

Sumário

Índice de Figuras

1 APRESENTAÇÃO

ARTMS é o sistema de monitoramento automático de soluções Cloud e On-Premises do *BRIGHT Security Services*® da XSITE. O ARTMS permite ao SOC (Security Operations Center) da XSITE monitorar as soluções de segurança do cliente de forma automática sem necessidade de intervenção humana.

O ARTMS monitora automaticamente as soluções de segurança através de API's (Application Programming Interfaces) conectadas às consoles e/ou servidores de gerenciamento central, estejam elas em nuvem ou on-premises.

O ARTMS permite a customização de consultas às soluções monitoradas para s. As consultas substituem a ação humana de monitoramento de telas no SOC muito propensa à fadiga e a falhas de interpretação. A definição das condições para enquadramento nos níveis de alerta são customizáveis para cada cliente.

Para cada nível de alerta são executadas ações de ativação do SOC, através de aplicativo de celular e e-mail, podendo ser aplicadas também para ativação da equipe de SOC e/ou de suporte do cliente, conforme a necessidade.

Todos os quatro níveis de alerta ativam o SOC/Cliente através de e-mail e, adicionalmente, os alertas do tipo Emergency, High e Normal, ativam o SOC/Cliente através de aplicativo de celular com alarmes sonoros com diferentes graus de intensidade e de persistência.

Os níveis de alerta Emergency e High, além de ativarem o SOC/Cliente através de aplicativo de celular, disparam ainda a abertura de um processo de investigação de evento crítico, onde cada uma das etapas possui um SLA (Service Level Agreement) pré-definido e que pode ser customizado para cada cliente.

Os processos de monitoramento e de investigação são controlados por plataforma de automação de processos (BPM – Business Process Modeling), que controla de forma automática o cumprimento dos SLA's. O SLA de todos os processos de investigação pode ser acompanhado em tempo real pelo cliente através de Dashboards disponibilizados pelo ARTMS, tanto com informações históricas como de processos em andamento, em tempo real.

Na plataforma de BPM e nos Dashboards, cada cliente possui uma instância (*tenant*) isolada das demais, mantendo assim a independência das informações e processos.

A solução pode ainda ser customizada para atendimento a clientes em regimes 8x5 (oito horas por dia, cinco dias por semana) e 24x7 (vinte e quatro horas por dia, sete dias por semana).

2 FLUXO DE EXECUÇÃO

2.1 Monitoramento

O monitoramento das soluções de segurança é realizado de forma automática pelo ARTMS de acordo com o intervalo de tempo definido pelo cliente.

Para cada solução, são permitidas a definição de até 4 níveis de consulta à solução monitorada. Cada consulta estará associada a um nível de criticidade. Qualquer consulta aos dados e eventos de uma solução de segurança são permitidos, desde que suportados pela sua API.

As informações do cliente, técnicos/analistas de suporte, contatos do SOC, assim como os dados de acesso à aplicação, as consultas, o intervalo de monitoramento e o regime de execução (8x5 ou 24x7) são cadastrados na base de dados do ARTMS através da interface do sistema, conforme ilustrado na Figura 1.

Figura 1 - BRIGHT ARTMS

Uma vez cadastradas as informações no sistema, o ARTMS inicia o monitoramento da(s) solução(ões) de forma automática, conforme os parâmetros informados.

Atualmente o ARTMS suporta o monitoramento das soluções da Crowdstrike, Netskope, Seceon, Trellix, Tenable, Trendmicro, Fortinet, Forescout, dentre outras. Outras soluções podem ser adicionadas ao sistema conforme necessidade do cliente e disponibilização dos dados necessários ao cadastramento do mesmo na plataforma.

2.2 Acionamento

Quando alguma das consultas à API, conforme definidas na seção anterior, retorna um resultado positivo, imediatamente as seguintes ações são executadas:

1. Os detalhes do evento coletado são enriquecidos através do envio destas informações para solução de Inteligência Artificial Generativa (IAG) (Open AI ChatGPT-4), com o objetivo de detalhar a ocorrência e orientar o analista sobre como mitigar e tratar o alerta.
    a. O detalhamento do alerta contém, além das informações sobre a ocorrência em si, a correlação desta com as Técnicas e Táticas do Framework ATT&CK do MITRE, caso as informações estejam presentes no alerta, explicando o que significa cada uma das táticas e técnicas utilizadas e seus objetivos.
    b. Para as ocorrências de maior gravidade (Emergency ou High), todos os hashes encontrados na ocorrência são ainda submetidos à avaliação em tempo real do Virus Total e os resultados são inclusos no e-mail de acionamento do SOC.
2. E-mail enriquecido com as informações da lAG é enviado para a equipe do SOC da XSITE independente da criticidade do evento.
3. E-mail enriquecido com as informações da lAG é enviado para a equipe do cliente em caso de eventos do tipo Emergency ou High.
4. Envio de notificação “push” em aplicativo de celular:
    a. Em caso de eventos do tipo Emergency, High ou Normal, um aviso é enviado para a equipe de plantão do SOC da XSITE, com

diferentes níveis de intensidades e persistência, a depender da criticidade do evento.

b. Em caso de eventos do tipo Emergency ou High, um aviso é enviado para a equipe de plantão do cliente, caso este tenha optado por esta funcionalidade, com diferentes níveis de intensidades e persistência, a depender da criticidade do evento.

c. Para os clientes com atendimento 24x7, estas notificações são enviadas de forma imediata.

d. Para os clientes com atendimento 8x5, estas notificações são enviadas de forma imediata, caso ocorram dentro do horário normal de expediente. Notificações fora do horário normal serão enviadas no próximo dia útil às 08:00hs da manhã.

O diagrama abaixo apresenta o processo de Monitoramento e Acionamento em notação BPMn:

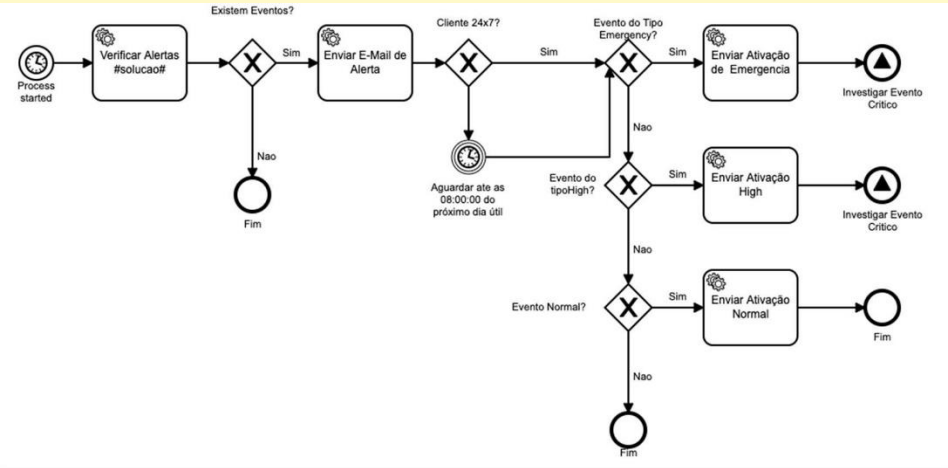

Figura 2 - Processo de Monitoramento e Acionamento ARTMS

2.3 Resposta

1. Abertura de Processo de Investigação de Evento Relevante
    a. Nos casos de ocorrência de eventos do tipo Emergency ou High, será aberto de forma automática na plataforma de Gestão Automatizada de Processos (BPM), um processo para que a ocorrência seja investigada.
        i. Para os clientes com atendimento 24x7, o processo será iniciado de forma imediata.
        ii. Para os clientes com atendimento 8x5, o processo será iniciado de forma imediata, caso a ocorrência esteja

dentro do horário normal de expediente. Caso contrário, serão iniciados no próximo dia útil às 08:00hs da manhã.

b. O SOC da XSITE deverá iniciar a investigação do evento dentro do SLA contratado com o cliente. O SLA será atribuído a esta tarefa dentro do ARTMS durante a configuração inicial do *tenant* do cliente.
c. A análise do(s) evento(s) encontrados deve ser realizado também dentro do SLA contratado com o cliente O SLA será atribuído a esta tarefa dentro do ARTMS durante a configuração inicial do *tenant* do cliente.
d. Durante a análise dos eventos, a equipe do SOC irá proceder de acordo com os playbooks existentes para determinação da gravidade da ocorrência e das ações a serem executadas.
e. Uma vez determinada a gravidade do(s) evento(s):
    i. Em caso de eventos de baixo impacto:
        1. O SOC da XSITE irá enviar e-mail para os contatos registados pelo cliente com os resultados da investigação e as recomendações de melhoria do ambiente para que o(s) evento(s) não volte(m) a ocorrer.
    ii. Em caso de eventos de alto impacto:
        1. O SOC irá elaborar um Plano de Ação de Emergência e:
            - Caso as ações de contenção necessárias estejam previamente autorizadas pelo cliente no escopo da ocorrência, estas serão executadas imediatamente pela equipe do SOC.
            - Caso as ações de contenção necessárias não estejam previamente autorizadas pelo cliente no escopo da ocorrência, a equipe do SOC irá contactar o cliente para atuação em conjunto e com as devidas aprovações.

O diagrama abaixo apresenta o processo de Resposta em notação BPMn:

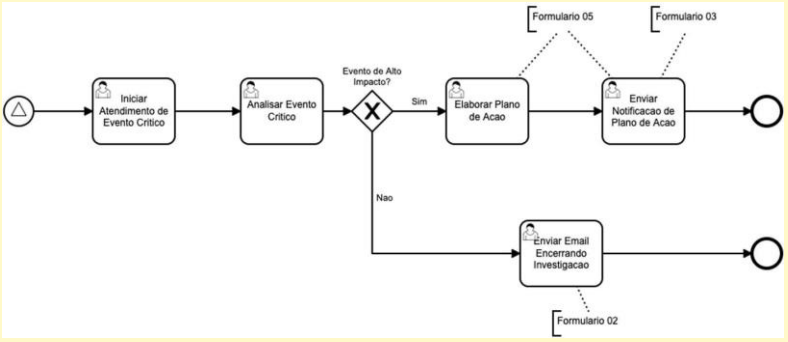

Figura 3 - Processo de Resposta do SOC

3 DASHBOARDS

O cliente terá acesso às informações mais relevantes geradas pelo ARTMS através dos Dashboards disponibilizados pela solução.

Os dashboards apresentam informações gráficas e textuais, em forma de tabelas, para que o cliente possa acompanhar toda a operação do SOC em tempo real e o cumprimento/descumprimento dos SLA's contratados. Todas as informações são geradas automaticamente pelo sistema de Gestão Automatizada de Processos, de acordo com a execução das atividades.

Nesta seção utilizaremos o termo ATIVIDADE ou TAREFA para designar cada uma das ações de um PROCESSO. Um PROCESSO é formado por um conjunto de ATIVIDADES/TAREFAS correlacionadas e sequenciadas. Como exemplo temos a ATIVIDADE de "Analisar Evento Crítico" dentro do PROCESSO de Resposta do SOC (Figura 3).

Atualmente o ARTMS possui 2 dashboards principais. O primeiro deles é o de **Monitoramento de Tarefas do SOC**. Este dashboard é composto por tabelas que permitem ao cliente acompanhar em detalhes informações sobre a execução de tarefas em andamento, tarefas em atraso e tempos médios de execução/atraso de tarefas.

O segundo dashboard é o de **Monitoramento de Processos do SOC**. Neste dashboard é possível monitorar o tempo total de execução do Processo de Resposta do SOC, bem como incidentes em aberto etempo total gasto até o momento para tratamento do mesmo, acompanhamento gráfico dos SLA's das tarefas de Iniciar Atendimento de Evento Crítico e de Analisar Evento Crítico, bem como a quantidade e tempo de tarefas em atraso por processo de investigação.

3.1 Dashboard de Monitoramento de Tarefas do SOC

O dashboard de monitoramento de tarefas do SOC traz informações detalhadas sobre o histórico, métricas de atendimento e a situação de tarefas em andamento em tempo real.

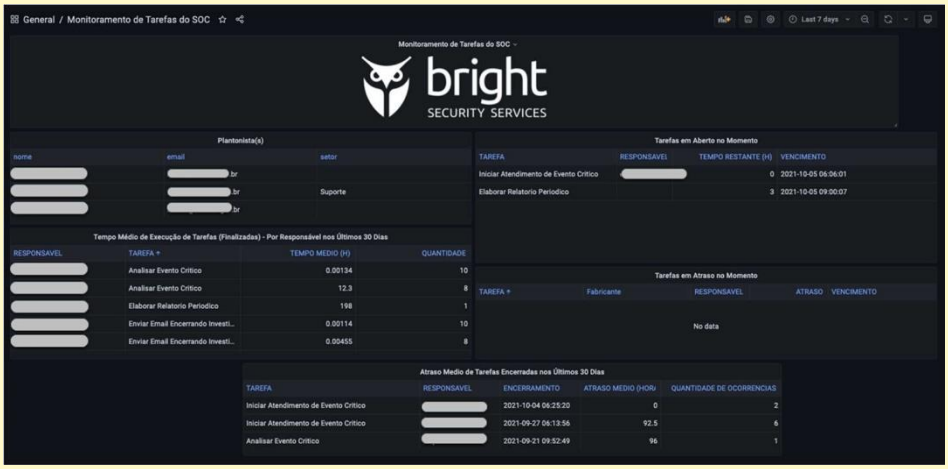

Figura 4 - Dashboard de Monitoramento de Tarefas do SOC

3.1.1 Plantonistas

Este widget apresenta em tempo real os analistas de segurança da XSITE que estão designados para o atendimento, bem como as pessoas da equipe do cliente que serão notificadas pelo ARTMS em caso de ocorrências, conforme descrito no processo de Monitoramento e Ativação.

Figura 5 - Widget Plantonistas

3.1.2 Tarefas em Aberto no Momento

Este widget apresenta as tarefas que estão sendo executadas no momento, dentro do SLA, indicando o nome da tarefa, o fabricante/solução, o responsável pela sua execução, o tempo que falta para atingir o SLA e a previsão de data/hora de encerramento do SLA.

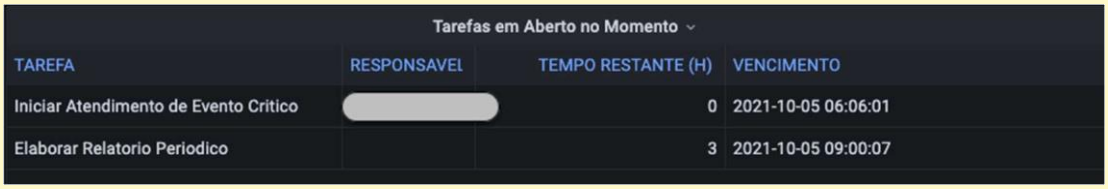

Figura 6 - Widget Tarefas em Aberto no Momento

3.1.3 Tarefas em Atraso no Momento

Este widget apresenta as tarefas que estão sendo executadas no momento, fora do SLA, indicando o nome da tarefa, o fabricante/solução, o responsável pela sua execução, o tempo de atraso em relação ao SLA e a previsão original de data/hora de encerramento baseado no SLA.

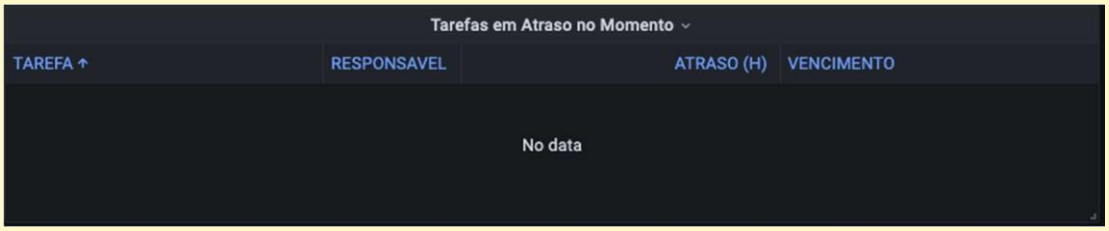

Figura 7 - Widget Tarefas em Atraso no Momento

3.1.4 Tempo Médio de Execução de Tarefas por Responsável nos Últimos 30 Dias

Este widget apresenta o tempo médio de execução de cada atividade que foi encerrada nos últimos 30 dias. Neste caso são consideradas todas as execuções encerradas nos últimos 30 dias, independente de terem cumprido ou não o SLA contratado.

Figura 8 - Widget Tempo Médio de Execução de Tarefas nos Últimos 30 Dias

3.1.5 Atraso Médio de Execução de Tarefas por Responsável nos Últimos 30 Dias

Este widget apresenta o tempo médio de atraso de cada atividade que foi encerrada nos últimos 30 dias. Neste caso são consideradas apenas as execuções encerradas nos últimos 30 dias, que não cumpriram o SLA contratado.

Figura 9 - Widget Atraso Médio de Tarefas nos Últimos 30 Dias

3.2 Dashboard de Monitoramento de Processos do SOC e SLA

O dashboard de Monitoramento de Processos do SOC e SLA apresenta informações agregadas e de forma gráfica da execução de processos e atividades de resposta aos alertas gerados, de acordo com o período selecionado, inclusive com indicação visual, em cores, do atendimento aos SLA's contratados.

Figura 10 - Dashboard de Monitoramento de Processos do SOC e SLA

3.2.1 Tempo de Tratamento de Incidentes Abertos pelo ARTMS

Este widget apresenta o tempo total (em horas) de execução dos processos de Resposta do SOC, deste a sua abertura pelo ARTMS até o seu encerramento, seja com o envio do e-mail de encerramento da investigação, seja com o envio do Plano de Ação (Figura 3). A data apresentada na base de cada uma das barras é a data de início do processo.

A coloração das barras indica, visualmente, o quanto o tempo total de execução do processo se aproximou ou ultrapassou o SLA contratado. Os SLA's podem ser definidos para cada cliente de forma independente, conforme o contrato existente entre as partes.

Figura 11 - – Widget Tempo de Tratamento de Incidentes Abertos Pelo ARTMS

3.2.2 Quantidade de Incidentes Tratados (por Tempo de Resolução)

Este widget apresenta o número de incidentes tratados no período selecionado, distribuídos pelo tempo de resolução.

Figura 12 - Widget Quantidade de Incidentes Tratados por Tempo de Resolução

3.2.3 Incidentes Abertos pelo ARTMS em Andamento

Este widget apresenta os processos de Resposta do SOC que estão abertos (em andamento). A barra representa o número de processos em andamento.

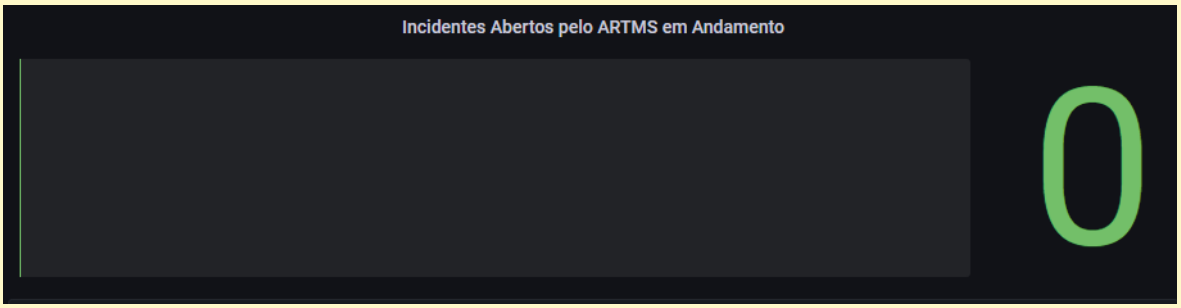

Figura 13 - Widget Incientes Abertos pelo ARTMS em Andamento

3.2.4 SLA de Início de Atendimento

Este widget apresenta o tempo, em minutos, para início da investigação após a geração do alerta pelo ARTMS. A data apresentada na base de cada uma das barras é a data de início da tarefa.

A coloração das barras indica, visualmente, o quanto o tempo total de execução da tarefa se aproximou ou ultrapassou o SLA contratado. Os SLA's podem ser definidos para cada cliente de forma independente, conforme o contrato existente entre as partes.

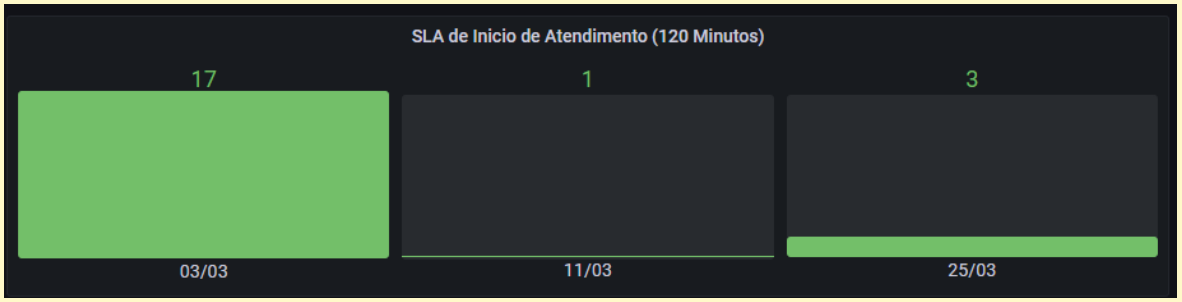

Figura 14 - Widget SLA de Início de Atendimento

3.2.5 SLA de Análise de Evento Crítico

Este widget apresenta o tempo gasto na tarefa de *Análisar de Evento Crítico* (aplicável para eventos do tipo Emergency e High). A data apresentada na base de cada uma das barras é a data de início da tarefa.

A coloração das barras indica, visualmente, o quanto o tempo total de execução da tarefa se aproximou ou ultrapassou o SLA contratado. Os SLA's podem ser definidos para cada cliente de forma independente, conforme o contrato existente entre as partes.

Figura 15 - Widget de SLA de Análise de Evento Crítico

3.2.6 Tarefas de Investigação fora do SLA

Este widget apresenta o somatório dos tempos gastos em tarefas que ultrapassaram o SLA contratado no processo de investigação de eventos. Na base de cada barra é possível verifica a data de início do processo e a quantidade de tarefas que ultrapassaram o SLA contratado.

Figura 16 - Widget Tarefas de Investigação fora do SLA

4 ARTMS FORESCOUT PLUGIN

O ARTMS Forescout Plugin permite o acionamento do plantão do SOC, de forma automática, baseado em políticas definidas na solução da Forescout.

Desta forma, o acionamento do atendimento do SOC pode ser feito sem intervenção humana, de acordo com as condições de saúde e conformidade dos dispositivos do cliente.

O ARTMS Forescout Plugin permite gerar alertas para o SOC nos 4 (quatro) níveis de alerta já definidos: Emergency, High, Normal e Low. O acionamento e as ações do SOC seguem o padrão descrito na seção 2: Fluxo de Execução

A ação de alerta ao SOC fica disponível no grupo de ações ARTMS e pode ser disparada através de políticas, bem como manualmente pelo operador:

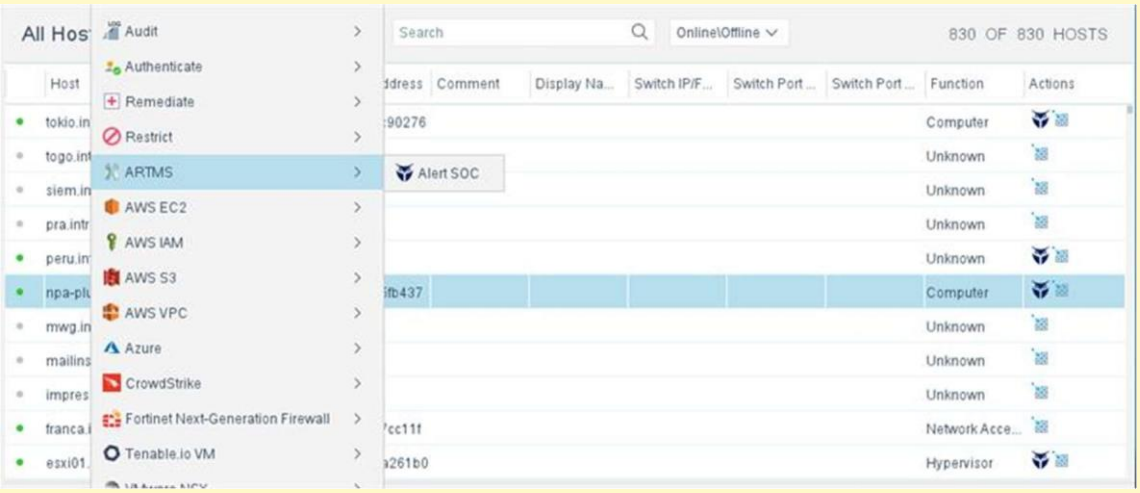

Figura 17 - ARTMS Forescout Plugin - Execução sob Demanda

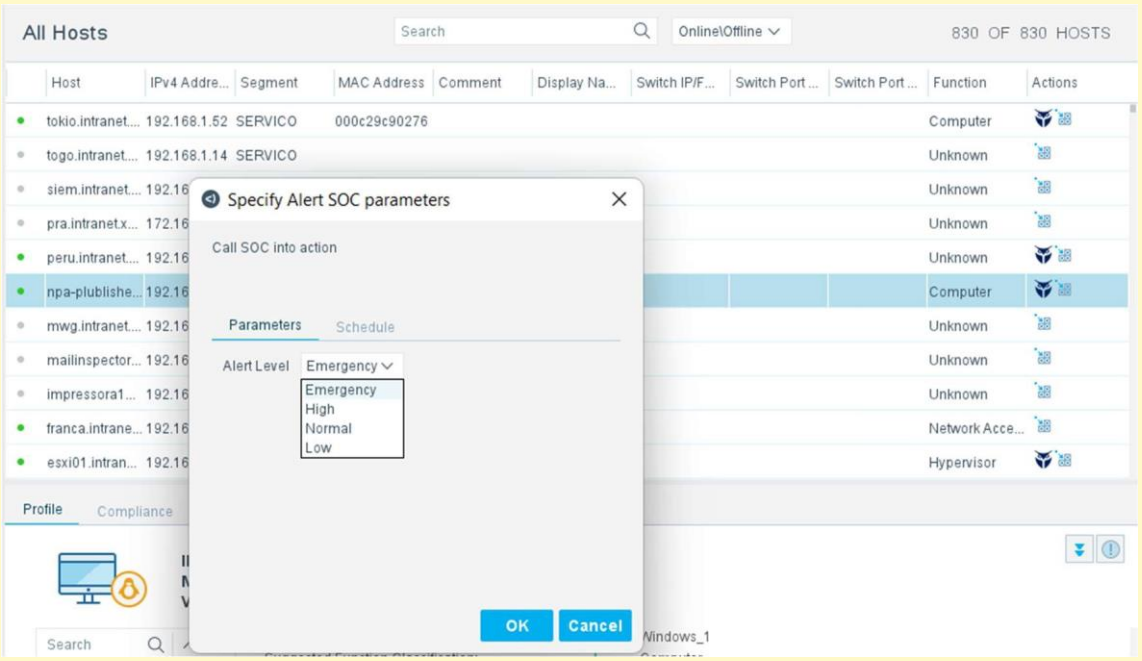

Figura 18 - ARTMS Forescout Plugin - Alert Levels

A instalação e configuração do ARTMS Forescout Plugin é realizado pela equipe do SOC da XSITE e as definições de políticas que irão acionar o SOC, bem como o nível de relevância de cada alarme são definidos em conjunto com o cliente.