BRIGHT
Client View

Guia do Usuário
Versão 1.0 — Março 2026

1. Introdução

O **Bright Client View (BCV)** é o portal de transparência e governança dos serviços de segurança da informação prestados pela XSITE. Ele foi desenvolvido para oferecer ao gestor de TI e ao responsável pela segurança cibernética uma visão consolidada, em tempo real, de todos os indicadores operacionais e estratégicos relacionados ao SOC (Security Operations Center), ao monitoramento ARTMS e às soluções de segurança contratadas.

Principais benefícios

- **Transparência operacional** — Visibilidade contínua sobre o desempenho do SOC/MSSP/MDR, com métricas de SLA, tempos de resposta e volumes de tickets.
- **KPIs estratégicos** — Indicadores-chave consolidados por período, permitindo acompanhamento da evolução da postura de segurança.
- **Governança de fornecedores** — Dashboards dedicados para cada solução contratada (EDR, VM, SIEM, WAF, CASB, BAS, PAM, entre outros), com dados extraídos diretamente das APIs dos fabricantes.
- **Visão unificada** — Um único portal para acompanhar contratos, licenciamento, relatórios e o estado geral da segurança da organização.

Acesso à plataforma

- 1.Acesse a URL fornecida pela XSITE no seu navegador (recomenda-se Google Chrome ou Microsoft Edge).
- 2. Insira suas credenciais (e-mail e senha) na tela de login. Se sua organização utiliza SSO (Single Sign-On), clique em "Entrar com SSO".
- 3. Após a autenticação, você será direcionado automaticamente para a página inicial.

2. Navegação Geral

A barra de navegação superior exibe os menus disponíveis de acordo com o seu perfil e os serviços contratados. Para o perfil de cliente, os menus principais são:

Menu	Ícone	Descrição
ARTMS		Monitoramento e relatoria dos ativos e contratos gerenciados
SOC		Indicadores do Security Operations Center
Soluções (Vendors)		Dashboards das soluções de segurança contratadas

No canto superior direito, são exibidos o nome do usuário e a identificação do tenant (organização). Todos os dados apresentados são filtrados automaticamente para o seu ambiente.

3. Menu ARTMS - Monitoramento e Relatoria

O ARTMS (Autonomous Real Time Monitoring System) é o módulo de monitoramento contínuo. Ao acessá-lo, você encontrará as seguintes abas:

3.1 DASHBOARD

Painel principal com indicadores de saúde do monitoramento:

- **Verificações realizadas —** Quantidade de verificações executadas no período.
- **Incidentes tratados —** Total de incidentes detectados e tratados
- **Participação Diana AI —** Percentual de incidentes em que a inteligência artificial Diana contribuiu na análise.
- **Tratados 100% por Diana —** Percentual de incidentes em que a inteligência artificial Diana resolveu o ticket integralmente sem intervenção humana (zero touch).
- **Soluções monitoradas —** Quantidade de soluções de segurança integradas.
- **Rituais de Prevenção —** Quantidade de Rituais de Prevenção executados pelo time da XSITE no período para garantir estabilidade e eficácia das soluções monitoradas.
- **Detecções por severidade** — Distribuição das detecções por nível de criticidade (Emergency, High, Normal, Low).
- **Resumo diário** — Gráfico de evolução das verificações e detecções ao longo do tempo.

Utilize o seletor de período no topo da página para alternar entre períodos predefinidos (7, 30 ou 90 dias) ou definir um intervalo personalizado com datas absolutas.

3.2 LIVE MONITORING

O Live Monitoring é o painel de operações em tempo real do ARTMS. Ele oferece uma visão ao vivo das atividades de monitoramento por meio de duas perspectivas complementares, alternáveis por um botão de modo:

- ***MODO KPIS***

Exibe os indicadores operacionais em formato de cards, incluindo
total de verificações, detecções por severidade, participação da Diana AI e alertas por vendor de segurança. Os dados são atualizados em tempo real via WebSocket.

- ***MODO JORNADA***

Apresenta a jornada completa do processo de monitoramento, mostrando o fluxo de eventos desde a detecção inicial até a resolução, permitindo visualizar cada etapa do pipeline de operações.

Funcionalidades adicionais do Live Monitoring:

- **Feed de eventos em tempo real —** Terminal ao vivo com eventos categorizados por tipo (Sistema, Alerta, Check, Sucesso, Erro, Ticket), cada um com código de cores para identificação rápida.
- **Auto-refresh configurável —** Possibilidade de configurar atualização automática em intervalos de 5, 10, 15 ou 30 minutos.
- **Modo tela cheia (fullscreen) —** O painel pode ser expandido para ocupar toda a tela do monitor, ideal para exibição em telões de NOC/SOC.
- **Filtro por tipo de evento —** Os eventos podem ser filtrados por tipo (Todos, Check, Alerta, Sistema, Sucesso, Erro) para focar no que é mais relevante.
- **Alertas por vendor —** Contagem de alertas de segurança por fabricante integrado (CrowdStrike, FortiSIEM, Cortex XDR, Seceon, TrendMicro, Trellix), com carregamento progressivo.

3.3 LOGS EM TEMPO REAL

Exibe os logs de eventos do monitoramento à medida que são gerados, permitindo acompanhamento em tempo real da atividade operacional.

3.4 Relatoria

Apresenta a tabela de contratos vigentes com detalhes de cada solução contratada: fabricante, solução, quantidade de licenças, datas de início e fim do contrato, período e tipo. Também exibe os relatórios periódicos gerados pela equipe de operações, com KPIs de status (abertos, pendentes, resolvidos).

3.5 Custom

Área reservada para dashboards personalizados, configurados conforme necessidades específicas do cliente.

4. Menu SOC — Security Operations Center

O módulo SOC oferece visibilidade completa sobre a operação do centro de operações de segurança. Ele possui um filtro por tipo de ticket (Todos, Requisições ou Incidentes) que se aplica a todas as abas.

4.1 Dashboard

Painel consolidado com os principais KPIs operacionais:

- **Tickets abertos** — Volume de chamados registrados no período.
- **Tickets resolvidos** — Volume de chamados finalizados no período.

- **MTTO (Mean Time to Own)** — Tempo médio para atribuição de um ticket a um

analista.

- **% SLA TTO** — Percentual de tickets atribuídos dentro do SLA.
- **MTTR (Mean Time to Resolve)** — Tempo médio de resolução de tickets.
- **% SLA TTR** — Percentual de tickets resolvidos dentro do SLA.
- **SLA a vencer / SLA vencido** — Tickets próximos do vencimento ou com SLA já ultrapassado.
- **Tickets por categoria** — Distribuição dos chamados por tipo/tag.
- **Evolução semanal** — Gráfico de evolução de tickets ao longo do tempo.
- **Tickets fora do horário** — Chamados registrados fora do expediente.
- **Taxa de falsos positivos** — Percentual de alertas confirmados como falsos positivos.

4.2 Demanda

Dashboard de análise de demanda que permite identificar padrões e tendências de volume de tickets ao longo do tempo.

4.3 Monitoramento de SLA

Acompanhamento detalhado do cumprimento dos níveis de serviço contratados, com termômetros visuais de SLA que facilitam a identificação rápida de desvios.

4.4 Tickets

Listagem completa dos tickets em processamento e pendentes, com informações de status, analista responsável, data de abertura e links diretos para detalhamento.

4.5 MTTO (Mean Time to Own)

Análise aprofundada do tempo médio de atribuição, com gráficos de evolução e detalhamento por período e categoria.

4.6 MTTR (Mean Time to Resolve)

Análise aprofundada do tempo médio de resolução, com séries temporais e segmentação por tipo de chamado.

4.7 War Room

Visão consolidada para situações críticas, reunindo informações relevantes para resposta a incidentes em andamento.

4.8 Documentos

Repositório de documentos operacionais, incluindo Cartas de Risco e outros documentos relevantes para a governança de segurança.

4.9 Custom

Dashboards personalizados com indicadores específicos definidos em conjunto com a equipe XSITE, adaptados às necessidades do contrato.

5. Menu Soluções (Vendors)

Os menus de Soluções são exibidos dinamicamente conforme os contratos ativos da sua organização. Cada fabricante possui um conjunto de abas especializadas. Abaixo, os principais vendors suportados:

5.1 CrowdStrike (EDR/XDR)

KPIs	Indicadores de proteção de endpoints: cobertura de sensores, detecções, alertas por severidade
Compliance	Verificação de conformidade dos agentes instalados
Triagem	Lista de alertas para triagem e acompanhamento de detecções, com análise assistida por IA (Diana)
Relatórios	Relatórios mensais da operação CrowdStrike, com opção de impressão em PDF

5.2 Tenable (Gestão de Vulnerabilidades)

Aba	Descrição
KPIs	Indicadores gerais: Cyber Exposure Score (CES), vulnerabilidades críticas, total de ativos
Lumin	Visão do Tenable Lumin com benchmarks e priorização de riscos
Compliance	Estado de conformidade dos agentes e scans realizados
VM	Vulnerability Management: vulnerabilidades por criticidade e ações recomendadas
WAS	Web Application Scanning: vulnerabilidades em aplicações web
Cloud	Segurança de ambientes cloud
Identity	Indicadores de exposição de identidades e credenciais
Licenciamento	Uso atual vs. licenças adquiridas
Relatórios	Relatórios detalhados com drill-down por vulnerabilidade

5.3 Fortinet (SIEM / EMS / WAF)

Aba	Descrição
EMS Dashboard	Status dos endpoints gerenciados pelo FortiClient EMS
FortiWEB (vdom)	Dashboard por domínio virtual do WAF: ataques bloqueados, top ameaças, tráfego. Uma aba por vdom.
FortiSIEM Performance	Métricas de performance do SIEM: EPS, armazenamento, saúde de coletores
FortiSIEM Incidentes	Lista de incidentes de segurança detectados pelo SIEM
FortiSIEM MITRE	Mapeamento de incidentes no framework MITRE ATT&CK
FortiSIEM CMDB	Inventário de dispositivos monitorados pelo SIEM
FortiSIEM Triagem	Fila de triagem de alertas para análise

5.4 Palo Alto Cortex (XDR/XSIAM)

Aba	Descrição
Dashboard Cortex	Visão geral de alertas, incidentes e endpoints gerenciados pelo Cortex XDR
Compliance	Conformidade de agentes e políticas de proteção

5.5 Picus Security (BAS — Breach and Attack Simulation)

Aba	Descrição
Dashboard	Resultados consolidados das simulações de ataque: score de segurança, ameaças testadas
Riscos	KPIs de risco, lista de ameaças não bloqueadas e análise de gaps de segurança
MITRE ATT&CK	Cobertura das técnicas MITRE com heatmap visual e tabela detalhada de técnicas
Evolução	Histórico de evolução dos scores de segurança ao longo das simulações realizadas
Mitigações	Sugestões de mitigação por dispositivo de segurança com assinaturas recomendadas

5.6 Netskope (CASB/SSE)

Aba	Descrição
Dashboard	Visão geral de uso de cloud, aplicações de risco, alertas DLP e ameaças detectadas
Compliance	Conformidade de políticas de segurança em nuvem

5.7 BeyondTrust (Acesso Privilegiado — PAM)

A solução BeyondTrust é voltada para o gerenciamento de acesso privilegiado (PAM). O BCV oferece dois módulos com dashboards completos:

Aba	Descrição
PRA (Privileged Remote Access)	Sessões de acesso remoto privilegiado: KPIs de sessões, top servidores acessados, sessões por jump group, sessões por analista, auditoria de sessões, injeção de credenciais, duração média por analista, evolução de qualidade e comparativo mensal
PWS (Password Safe)	Gerenciamento de senhas privilegiadas: contas inativas e classificação, histórico de inatividade, top 10 senhas por idade, status de gerenciamento, classificação de idade de senhas, relação idade×conta, atividade de contas e informações de sistemas

5.8 Seceon (aiSIEM / aiXDR)

O Seceon é uma plataforma de SIEM/XDR baseada em inteligência artificial. O BCV integra os seguintes painéis:

Aba	Descrição
KPI	Indicadores consolidados: total de alertas, distribuição por severidade (Critical, Major, Minor), alertas por tipo, por status, por confiança, volume de tráfego de rede, gráficos de distribuição e tendências
Performance	Métricas de desempenho da plataforma: tempo de detecção, volume de eventos processados (EPS), alertas por severidade ao longo do tempo, tabela detalhada de alertas com data, tipo e status
Alertas	Lista detalhada de alertas com severidade, tipo, status, entidade afetada, IPs de origem/destino e análise assistida por IA (Diana) para cada alerta
Threat Indicators	Indicadores de ameaça: IPs maliciosos, geolocalização de origens, categorias de eventos, tendências de ameaças por período
Triagem	Análise de alertas MINOR para otimização de regras e redução de ruído, com estatísticas de confiança média, top tipos de alerta e análise consolidada por Diana AI

5.9 Trend Micro (XDR)

O painel Trend Micro exibe indicadores da solução XDR (Extended Detection and Response):

Aba	Descrição
Alertas Geral	Evolução diária de alertas por severidade (Critical, High, Medium, Low), alertas por entidade, top tipos de alertas e top entidades por tipo de alerta
Alertas High	Detalhamento dos alertas de severidade High: evolução temporal, distribuição por categoria e análise de origens
Alertas Medium	Detalhamento dos alertas de severidade Medium com os mesmos indicadores e gráficos da aba Alertas High
Detecções High	Detecções de alto risco: evolução diária, distribuição por categoria, top origens, top tipos, top destinos e cruzamento origem×tipo e destino×tipo. Inclui filtro por regra de detecção (rule_name) para análise dirigida

5.10 Aba Custom (todos os Vendors)

Presente em cada vendor, exibe um resumo contratual com: produtos contratados, quantidade de licenças adquiridas, data de expiração do contrato e dias restantes. Um código de cores visual indica a proximidade do vencimento:

Cor	Significado
Vermelho	Contrato expirado
Roxo	Expira em menos de 30 dias
Laranja	Expira em menos de 90 dias
Âmbar	Expira em menos de 180 dias
Normal	Mais de 180 dias para expiração

6. Filtros e Controles Comuns

Diversos filtros são reutilizados em toda a plataforma:

- **Filtro de período** — Disponível em dashboards do ARTMS e SOC. Permite selecionar períodos predefinidos (7, 30 ou 90 dias) ou informar datas absolutas (início e fim).
- **Filtro de tipo de ticket** — No SOC, permite visualizar todos os tickets, somente requisições ou somente incidentes.

7. Boas Práticas de Uso

Para extrair o máximo valor do Bright Client View, recomendamos:

- **Acesse regularmente** — Consulte o BCV ao menos semanalmente para acompanhar a evolução dos indicadores e identificar tendências e para checar as novidades, que são constantes.
- **Monitore os SLAs** — As abas de Monitoramento de SLA e o Dashboard do SOC são sua principal ferramenta para garantir que os níveis de serviço estão sendo cumpridos.
- **Acompanhe a postura de segurança** — Utilize os dashboards dos vendors para acompanhar a evolução da superfície de ataque e a eficácia das defesas.
- **Utilize filtros de período** — Compare períodos distintos para identificar melhorias ou degradações nos indicadores.
- **Verifique o licenciamento** — A aba Custom de cada vendor e a seção de Licenciamento ajudam a garantir que sua organização está com licenças ativas e adequadas.
- **Relatórios para reuniões de governança** — Os relatórios de CrowdStrike e Tenable podem ser impressos/exportados em PDF para apresentações em comitês de segurança.
- **Aproveite o Live Monitoring** — O Live Monitoring pode ser exibido em tela cheia com auto-refresh, ideal para telões de NOC/SOC, proporcionando acompanhamento contínuo das operações.

8. Suporte

Para dúvidas sobre a plataforma, dados apresentados ou funcionalidades adicionais, entre em contato com a equipe XSITE pelo canal de atendimento habitual.

Todos os dados exibidos são atualizados em tempo real ou próximo a tempo real, conforme a integração com cada solução.