KDFM eXplorer

SEGURANÇA PLATAFORMA
Específica para a nova versão 4 do DCA

- Servidores situados na UE
- Fornecedor independente de software (ISV) não vinculado a nenhum fabricante de hardware
- Ciclo recorrente de avaliações de segurança de aplicações DCA por empresas independentes de consultoria em ciber-segurança
- Plataforma certificada com a norma ISO27001 e em conformidade com o Regulamento Europeu de Proteção de Dados (GDPR).
- Cumprimento do GDPR: um Acordo de Processamento de Dados (DPA) através de um processo automatizado de assinatura eletrónica
- Desenvolvido em colaboração com OWASP Top Ten Web Application Security Risks | OWASP
- A fim de trocar dados e receber informações sobre tarefas a realizar, o software utiliza chamadas de sondagem HTTP2 GRPC (geralmente enviadas uma vez a cada 5 minutos) e ligação MQTT a um Servidor que pode ser alcançado através de diferentes URLs de domínio pertencentes ao domínio raiz https://*.mpsmonitor.com. A ligação MQTT utiliza como padrão MQTT sobre WSS (porta 443). Pode também ser configurada para funcionar como uma ligação MQTT padrão (porta 8883)
- Suporte para SNMPv1/v2 e v3 e descoberta de dispositivos por nomes de anfitrião
- Todos os serviços web são protegidos pela codificação RSA SHA -2 256 Bit TLS. 1.2
- Autenticação avançada do utilizador: Autenticação de dois fatores, Single Sign-On (SSO) para utilizadores do Active Directory (acesso ao portal via autenticação Windows), permissões de utilizador granulares, desativação do utilizador após 5 tentativas sem sucesso ou se não houver ligação dentro de 90/180 dias, ficheiro executável DCA desativado após 5 vezes.
- Certificações: SOC 2 Relatório de Auditoria Tipo 1 fornecido por A-LIGN, Okta, BLI Teste de validação de segurança, ISO 27001 TUV
- SOC 2 Tipo 1 Conformidade da Auditoria de Segurança: as práticas e controlos cumprem os requisitos de Segurança, Disponibilidade, Confidencialidade estabelecidos pelo AICPA (American Institute).

Informação adicional:

1. A Cloud não pode " contactar " o DCA instalado no PC, pelo que nenhuma porta ou serviço é exposto à Internet pelas redes dos clientes.
2. É sempre a DCA que inicia a comunicação através dos protocolos GRPC e MQTT e para um ponto final TCP (porta 443) e a comunicação é encriptada usando o certificado SSL.
3. A porta 22 é necessária para executar o Device Web Access usando o protocolo SSH
4. O DCA utiliza o protocolo SNMP na porta 161 para ler impressoras MIB na rede do cliente e apenas para a gama de endereços IP configurada. O Acesso à Web do dispositivo liga-se às impressoras utilizando HTTP nas portas 80, 433, 8000 ou outras especificamente configuradas. As portas 9100 e 631 também podem ser utilizadas para aceder à impressora.
5. O DCA também pode enviar pacotes ICMP (não há especificação de porta) (isto é usado durante a resolução de problemas)
6. Não há nenhum outro porto ou protocolo.