Formulário PDTIC 2021-2023

Nome do projeto	*Implantação de XDR na UFABC*
Objetivo estratégico	*Promover a segurança de sistemas de informação*

Categoria do projeto:

Qual é a categoria do projeto?
Aquisição de licença de software
Existe algum equivalente de software livre que pode cumprir o papel mesmo que parcialmente?
Sim
O sistema de gestão da UFABC, SIG, possui módulo similar que atenda a essa necessidade de software?
Não
A licença é temporária?
Sim
Qual é o período previsto para a licença?
até 5 anos
Qual a abrangência do uso do software?
máquinas estratégicas e de VIPs
A disponibilização, utilização e armazenamento serão realizados em nuvem, servidor local, de forma híbrida ou haverá escolha de destino?
Haverá escolha de destino
Escopo do projeto:
XDR (Extended Detection and Response) é uma solução de segurança cibernética que combina várias ferramentas de segurança. XDR é uma arquitetura aberta que integra ferramentas e unifica as operações de segurança em todas as camadas que exigem proteção. XDR inclui ferramentas de: Detecção de endpoint Análise de rede Inteligência de ameaças Resposta a incidentes XDR é uma versão mais avançada de detecção e resposta de endpoint (EDR). Enquanto o EDR se concentra em endpoints, o XDR se concentra mais amplamente em vários pontos de controle de segurança para detectar ameaças mais rapidamente. XDR coleta e correlaciona automaticamente os dados em várias camadas de segurança. Isso permite uma detecção mais rápida de ameaças e melhor investigação e tempos de resposta por meio de análises de segurança. O Gartner definiu o termo pela primeira vez em 2020. Desde então, incontáveis especialistas da área estão rotulando a tecnologia como uma nova abordagem holística para a proteção proativa contra os sofisticados ataques cibernéticos de hoje.
Justificativas do projeto:
Algumas justificativas para a aquisição de XDR incluem: Proteção abrangente, incluindo endpoints, rede, nuvem e dados. Visão holística, permitindo que você detecte e responda às ameaças mais rapidamente e com mais precisão. Redução de custos, pois você não precisa comprar e gerenciar várias ferramentas diferentes. Capacidade estendida de detectar ataques. Tempo de resposta a incidentes reduzido. Otimização de recursos de rede e TI. Mais velocidade na contenção a ataques. Resposta mais ágil para eventos de TI. Melhorar a coleta de dados relacionados a ameaças e incidentes.
Previsão de custo :
2021 : R$ 0,00; 2022 : R$ 0,00; 2023 : R$ 0,00
Como foi estimado o valor da contratação?
O valor da contratação por um ano, de R$687.766,79 foi obtido a partir de consulta com a Approach Tecnologia, fornecedora da solução de XDR Cortex Palo Alto.

Formulário PDTIC 2021-2023

Data de início do projeto:
12.12.2023
Data estimada de fim do projeto:
30.09.2024

Papéis e responsabilidades

Responsáveis pelo projeto:

	Nome	E-mail	Área
Gerente	Paulo Victor	paulo.victor@ufabc.edu.br	NTI
Suplente	Carlos Alberto	carlos.alberto@ufabc.edu.br	NTI

Participantes do projeto:

Nome	Área ou Setor	Função no Projeto	E-mail
Paulo Victor	NTI	Gerente	paulo.victor@ufabc.edu.br

Metas e indicadores

Meta	100% das máquinas destino com a solução implantada até final de setembro de 2024
Prazo de cumprimento	Final de setembro de 2024
Valor esperado	100%
Valor de tolerância	50%
Tipo de valor	porcentagem
Indicador	quantidade de máquinas destino
Polaridade do Indicador	quanto maior melhor
Responsável	Paulo Victor
Valor atual do indicador	0%

Marcos e entregas do projeto

Etapas do projeto	Responsável	Data de início	Data de fim
Planejamento e instrução;	Paulo Victor	01/12/2023	29/02/2024

Custos do projeto

Item	Custo estimado	Ano do orçamento
Cortex XDR Pro por endpoint.	R$ 533,77	2024

Formulário PDTIC 2021-2023

Riscos do projeto

Risco		Avaliação do risco	
Se (causa ou ameaça)	for impossível fazer a instalação remota dos agentes	**Impacto**	4
Então (consequência)	vai ter que ser feita a instalação manual dos agentes	**Probabilidade**	3
Categoria do risco	operacional	**Severidade:**	12
Resposta ao risco			
Opção de tratamento do risco	evitar		
Como será realizado?	obrigar, no termo de referência, de que a instalação manual seja feita pela empresa fornecedora		