



CERTIFICADO

A Unirede Inteligência em TI certifica



EDILMAR RODRIGUES FONSECA JUNIOR

pela participação no Treinamento **Wazuh SIEM e XDR** com carga horária de **30 horas**.

Gabriel Pedroso

CEO - Unirede Inteligência em TI

- **FUNDAMENTOS SIEM E XDR:**

1. COMPREENSÃO DOS CONCEITOS DE SIEM E XDR.
2. IMPORTÂNCIA DO MONITORAMENTO CONTÍNUO E RESPOSTA A INCIDENTES.
3. NOÇÕES SOBRE CONFORMIDADE COM REGULAMENTAÇÕES E LEGISLAÇÕES.

- **INSTALAÇÃO E CONFIGURAÇÃO DO WAZUH:**

4. INSTALAÇÃO DO WAZUH INDEXER, MANAGER E DASHBOARD.
5. CONFIGURAÇÃO DO WAZUH AGENT EM DIFERENTES AMBIENTES (LINUX E WINDOWS).
6. HABILITAÇÃO E EXPLORAÇÃO DE CONFIGURAÇÕES DOS AGENTES.

- **COLETA E ANALISE DE LOGS:**

7. CONFIGURAÇÃO DE AGENTES PARA A COLETA DE LOGS EM SISTEMAS OPERACIONAIS LINUX E WINDOWS.
8. COLETA DE LOGS SEM AGENTES VIA SYSLOG E CONFIGURAÇÃO DE SYSLOG RELAY PARA LOCALIDADES REMOTAS.

- **CRIAÇÃO DE DECODERS E REGRAS PERSONALIZADAS:**

9. ENTENDIMENTO DA ESTRUTURA DE DECODERS E REGRAS NO WAZUH.
10. CRIAÇÃO DE DECODERS E REGRAS PERSONALIZADAS PARA ANÁLISE DE LOGS E DETECÇÃO DE AMEAÇAS ESPECÍFICAS.

- **DETECÇÃO DE AMEAÇAS E MONITORAMENTO DE SEGURANÇA:**

11. CONFIGURAÇÃO DE REGRAS DE IDS/IPS PARA DETECÇÃO DE AMEAÇAS.
12. IMPLEMENTAÇÃO DE MONITORAMENTO DE INTEGRIDADE DE ARQUIVOS (FIM) NO WAZUH.
13. INTEGRAÇÃO DO WAZUH COM FERRAMENTAS COMO SURICATA E YARA PARA DETECÇÃO DE PADRÕES DE MALWARE.

- **CONFIGURAÇÃO DE ALERTAS E NOTIFICAÇÕES:**

14. CRIAÇÃO DE ALERTAS CUSTOMIZADOS.
15. CONFIGURAÇÃO DE NOTIFICAÇÕES VIA SLACK E E-MAIL (SMTP).
16. AUTOMATIZAÇÃO DE ALERTAS CRÍTICOS PARA RESPOSTA A INCIDENTES.

- **AUTOMAÇÃO DE RESPOSTA A INCIDENTES:**

17. AUTOMAÇÃO DE RESPOSTAS USANDO FIREWALLD E IPTABLES.
18. CRIAÇÃO DE SCRIPTS DE RESPOSTA AUTOMÁTICA PARA BLOQUEIO DE IPS MALICIOSOS.
19. SIMULAÇÃO DE ATAQUES E TESTE DE RESPOSTA AUTOMÁTICA CONFIGURADA.

- **CRIAÇÃO DE DASHBOARDS E VISUALIZAÇÃO DE DADOS NO OPENSEARCH:**

20. CRIAÇÃO DE DASHBOARDS CUSTOMIZADOS NO OPENSEARCH.
21. CONFIGURAÇÃO DE RELATÓRIOS E ALERTAS AUTOMATIZADOS.
22. UTILIZAÇÃO DE PLUGINS PARA VISUALIZAÇÕES E ANÁLISES AVANÇADAS NO OPENSEARCH.

Início: 20/07/2026 Término 29/07/2026

