CyberOps Associate (CA) v1.0
Scope and Sequence

Última atualização Novembro 17, 2020

Introdução

As empresas de hoje são desafiadas pela detecção rápida das violações de segurança cibernética e pela resposta eficaz aos incidentes de segurança. As equipes nos centros de operações de segurança (SOCs) estão atentas aos sistemas de segurança, protegendo as empresas ao detectar e responder a ameaças e exploits de segurança cibernética. O CyberOps Associate prepara os candidatos para iniciar uma carreira como analistas de segurança cibernética de nível de associado nos centros de operações de segurança.

Público-alvo

O curso CyberOps Associate foi criado para os alunos da Cisco Networking Academy® que estão em busca das habilidades de analista de segurança de nível básico, orientadas para a carreira. Os alunos-alvo incluem os inscritos em programas de graduação em tecnologia nas instituições de ensino superior e profissionais de TI que desejam seguir carreira no centro de operações de segurança (SOC). Os alunos deste curso estão expostos a todo o conhecimento fundamental necessário para detectar, analisar e escalonar ameaças básicas à segurança cibernética usando ferramentas comuns de código aberto.

Pré-requisitos

Os alunos do CyberOps Associate devem ter as seguintes habilidades e conhecimentos:

- Habilidades de navegação no PC e na Internet
- Conceitos básicos do sistema Windows e Linux
- Noções básicas das redes de computador (nível CCNA ITN)
- Compreensão binária e hexadecimal
- Familiaridade com o Cisco Packet Tracer

Certificações pretendidas

Este curso está alinhado à certificação Cisco Certified CyberOps Associate (CBROPS). Os candidatos precisam passar no exame 200-201 CBROPS para obter a certificação Cisco Certified CyberOps Associate. O exame CBROPS avalia o conhecimento e as habilidades de um candidato no que diz respeito a conceitos de segurança, monitoramento de segurança, análise baseada em host, análise de invasão de rede e políticas e procedimentos de segurança.

Descrição do curso

O curso dispõe de muitos recursos que ajudam os alunos a entender esses conceitos:

- O curso consiste em vinte e oito (28) módulos. Cada módulo é composto de tópicos.
- Os módulos enfatizam o pensamento crítico, a solução de problemas, a colaboração e a aplicação prática de habilidades.

- Cada módulo contém uma forma de praticar e avaliar a compreensão, como uma atividade de laboratório ou do Packet Tracer. Essas atividades em módulos fornecem feedback e indicam o domínio do aluno em relação às habilidades necessárias para o curso. Os alunos podem garantir o nível de compreensão bem antes de fazer um teste ou exame graduado.
- Alguns tópicos podem conter um questionário interativo Verifique seu conhecimento ou alguma outra maneira de avaliar a compreensão, como um laboratório ou um Packet Tracer. Essas avaliações em tópicos informam os alunos se eles têm uma boa compreensão do conteúdo ou se precisam fazer uma revisão antes de continuar. Os alunos podem garantir o nível de compreensão bem antes de fazer um teste ou exame graduado. Verifique se os questionários de Verifique seu conhecimento não afetam a nota geral do aluno.
- Conteúdo multimídia avançado, como atividades interativas, vídeos e testes, para atender a estilos de aprendizagem variados, ajudar a estimular o aprendizado e aumentar a retenção do conhecimento.
- Os ambientes virtuais simulam cenários de ameaças à segurança cibernética do mundo real e criam oportunidades para monitoramento, análise e resolução de segurança.
- Os laboratórios práticos ajudam os alunos a desenvolver atividades de pensamento crítico e de solução de problemas complexos.
- Análises inovadoras oferecem feedback imediato para dar respaldo às avaliações de conhecimento e habilidades adquiridas.
- Os conceitos técnicos são explicados com uma linguagem apropriada para alunos de todos os níveis, e as atividades interativas integradas dividem a leitura do conteúdo em partes e reforçam o entendimento.
- O currículo incentiva os alunos a considerar uma formação mais aprofundada na área de TI e também enfatiza habilidades aplicadas e experiência prática.
- As atividades do Cisco Packet Tracer foram elaboradas para o Packet Tracer 7.3.0 ou versão mais recente.

Objetivos do curso

O CyberOps Associate v1.0 abrange as habilidades e os conhecimentos necessários para cumprir com sucesso as tarefas, os deveres e as responsabilidades de um analista de segurança cibernética no nível de associado que trabalha em um centro de operações de segurança (SOC).

Depois da conclusão do curso *CyberOps Associate v1.0* , os alunos serão capazes de realizar as seguintes tarefas:

- Instalar máquinas virtuais para criar um ambiente seguro para implementar e analisar eventos de ameaças à segurança cibernética.
- Explicar a função do analista de operações de segurança cibernética na empresa.
- Explicar os recursos e as características do sistema operacional Windows necessários para oferecer suporte às análises de segurança cibernética.
- Explicar os recursos e as características do sistema operacional Linux.
- Analisar a operação de protocolos e serviços de rede.
- Explicar a operação da infraestrutura de rede.
- Classificar os vários tipos de ataques à rede.
- Usar ferramentas de monitoramento de rede para identificar ataques contra protocolos e serviços de rede.
- Explicar como evitar o acesso mal-intencionado a redes, hosts e dados de computadores.

- Explicar os impactos da criptografia no monitoramento de segurança de rede.
- Explicar como investigar vulnerabilidades e ataques de endpoints.
- Avaliar os alertas de segurança de rede.
- Analisar dados de invasão de rede para identificar hosts comprometidos.
- Aplicar modelos de resposta a incidentes para gerenciar incidentes de segurança de rede.

Requisitos dos equipamentos de laboratório

Este curso não requer equipamentos físicos além do PC de laboratório do aluno. Ele usa várias máquinas virtuais (VMs) para criar a experiência de laboratório.

Pacote de equipamentos de linha de base:

- PCs - requisitos mínimos de sistema
  - CPU: Intel Pentium 4, 2,53 GHz ou equivalente com suporte à virtualização
  - Sistemas operacionais, como Microsoft Windows, Linux e Mac OS
  - Processador de 64 bits
  - RAM: 8 GB
  - Armazenamento: 40 GB de espaço livre em disco
  - Resolução de exibição: 1024 x 768
  - Fontes de idioma compatíveis com a codificação Unicode (se estiver visualizando em idiomas diferentes do inglês)
  - Drivers de placa de vídeo mais recentes e atualizações do sistema operacional
- Conexão com a Internet para PCs de laboratório e do aluno

Software para PC do aluno:

- Oracle VM VirtualBox Manager (versão 6.1 ou posterior)
- VM do local de trabalho de CyberOps
  - Download disponível no curso
  - Requer 1 GB de RAM, 20 GB de espaço em disco
- VM Security Onion
  - Download disponível no curso
  - Requer 4 GB de RAM (mínimo), 8 GB de RAM (altamente recomendado), 20 GB de espaço em disco

Estrutura do CyberOps Associate

Listados abaixo estão o conjunto atual de módulos e as competências associadas descritas para este curso. Cada módulo é uma unidade integrada de aprendizagem que consiste em conteúdo, atividades e avaliações que visam um conjunto específico de competências. O tamanho do módulo dependerá da profundidade do conhecimento e da habilidade necessária para dominar a competência. Alguns módulos são considerados fundamentais, pois os artefatos apresentados, embora não avaliados, permitem a aprendizagem de conceitos abordados no exame de certificação CBROPS.

Tabela 1. CyberOps Associate v1.0 - Estrutura do curso

Módulo/Tópicos	Metas/Objetivos
Módulo 1. O perigo	**Explicar por que as redes e os dados são atacados.**
1.0 Introdução	Uma breve introdução ao curso e ao primeiro módulo.
1.1 Histórias de guerra	Destacar os recursos dos incidentes da segurança cibernética.
1.2 Agentes de ameaças	Explicar as motivações dos agentes de ameaças por trás de incidentes de segurança específicos.
1.3 Impacto das ameaças	Explicar o possível impacto dos ataques de segurança de rede.
1.4 O resumo dos perigos	Um breve resumo e o teste do módulo.
Módulo 2. Soldados na guerra contra o crime digital	**Explicar como se preparar para uma carreira nas operações da segurança cibernética.**
2.0 Introdução	Uma introdução ao módulo.
2.1 O moderno centro de operações de segurança	Explicar a missão do centro de operações de segurança.
2.2 Como tornar-se um defensor	Descrever os recursos disponíveis para se preparar para uma carreira nas operações da segurança cibernética.
2.3 Resumo de soldados na guerra contra o crime digital	Um breve resumo e o teste do módulo.
Módulo 3. O sistema operacional Windows	**Explicar os recursos de segurança do sistema operacional Windows.**
3.0 Introdução	Uma introdução ao módulo.
3.1 A história do Windows	Descrever a história do sistema operacional Windows.
3.2 Arquitetura e operações do Windows	Explicar a arquitetura do Windows e sua operação.
3.3 Configuração e monitoramento do Windows	Explicar a configuração e o monitoramento do Windows.
3.4 Segurança do Windows	Explicar como o Windows pode permanecer seguro.
3.5 O resumo do sistema operacional Windows	Um breve resumo e o teste do módulo.
Módulo 4. Visão geral do Linux	**Implementar a segurança básica do Linux.**
4.0 Introdução	Uma introdução ao módulo.
4.1 Noções básicas do Linux	Explicar por que as habilidades do Linux são essenciais para o monitoramento e a investigação de segurança de rede.
4.2 Como trabalhar no Linux Shell	Usar o Linux Shell para manipular arquivos de texto.
4.3 Servidores e clientes do Linux	Explicar como funcionam as redes client-server.
4.4 Administração básica do servidor	Explicar como um administrador do Linux localiza e manipula arquivos de log de segurança.
4.5 O sistema de arquivos Linux	Gerenciar o sistema de arquivos e as permissões do Linux.

Módulo/Tópicos	Metas/Objetivos
4.6 Como trabalhar com a GUI do Linux	Explicar os componentes básicos da GUI do Linux.
4.7 Como trabalhar em um host do Linux	Usar ferramentas para detectar malware em um host do Linux.
4.8 Resumo dos conceitos básicos do Linux	Um breve resumo e o teste do módulo.
Módulo 5. Protocolos de rede	**Explicar como os protocolos viabilizam as operações de rede.**
5.0 Introdução	Uma introdução ao módulo.
5.1 Processo de comunicação de rede	Explicar as operações básicas das comunicações de rede de dados.
5.2 Protocolos de comunicação	Explicar como os protocolos viabilizam as operações de rede.
5.3 Encapsulamento de dados	Explicar como o encapsulamento permite que os dados sejam transportados pela rede.
5.4 Resumo dos protocolos de rede	Um breve resumo e o teste do módulo.
Módulo 6. Ethernet e IP	**Explicar como os protocolos Ethernet e IP oferecem suporte às comunicações de rede.**
6.0 Introdução	Uma introdução ao módulo.
6.1 Ethernet	Explicar como a Ethernet oferece suporte à comunicação de rede.
6.2 IPv4	Explicar como o protocolo IPv4 oferece suporte às comunicações de rede.
6.3 Noções básicas sobre endereçamento IP	Explicar como os endereços IP viabilizam a comunicação de rede.
6.4 Tipos de endereços IPv4	Explicar os tipos de endereços IPv4 que viabilizam a comunicação de rede.
6.5 O gateway padrão	Explicar como o gateway padrão viabiliza a comunicação de rede.
6.6 Comprimento do prefixo IPv6	Explicar como o protocolo IPv6 oferece suporte às comunicações de rede.
6.7 Resumo dos protocolos Ethernet e IP	Um breve resumo e o teste do módulo.
Módulo 7. Princípios da segurança de rede	**Verificação de conectividade**
7.0 Introdução	Uma introdução ao módulo.
7.1 ICMP	Explicar como o protocolo ICMP é usado para testar a conectividade da rede.
7.2 Utilitários Ping e Traceroute	Usar ferramentas do Windows, ping e traceroute para verificar a conectividade de rede.
7.3 Resumo da verificação de conectividade	Um breve resumo e o teste do módulo.
Módulo 8. protocolo ARP	**Analisar as PDUs do protocolo ARP em uma rede.**
8.0 Introdução	Uma introdução ao módulo.

Módulo/Tópicos	Metas/Objetivos
8.1 MAC e IP	Comparar as funções do endereço MAC e do endereço IP.
8.2 ARP	Analisar o ARP examinando os quadros Ethernet.
8.3 Problemas do ARP	Explicar como as requisições ARP afetam o desempenho da rede e do host.
8.4 Resumo do protocolo ARP	Um breve resumo e o teste do módulo.
Módulo 9. A camada de transporte	**Explicar como os protocolos da camada de transporte oferecem suporte à funcionalidade de rede.**
9.0 Introdução	Uma introdução ao módulo.
9.1 Características da camada de transporte	Explicar como os protocolos da camada de transporte oferecem suporte à comunicação de rede.
9.2 Estabelecimento das sessões da camada de transporte	Explicar como a camada de transporte estabelece sessões de comunicação.
9.3 Confiabilidade da camada de transporte	Explicar como a camada de transporte estabelece comunicações confiáveis.
9.4 O resumo da camada de transporte	Um breve resumo e o teste do módulo.
Módulo 10. Serviços de rede	**Explicar como os serviços de rede viabilizam a funcionalidade de rede.**
10.0 Introdução	Uma introdução ao módulo.
10.1 DHCP	Explicar como os serviços de DHCP viabilizam a funcionalidade de rede.
10.2 DNS	Explicar como os serviços de DNS viabilizam a funcionalidade de rede.
10.3 NAT	Explicar como os serviços de NAT viabilizam a funcionalidade de rede.
10.4 Serviços de transferência e compartilhamento de arquivos	Explicar como os serviços de transferência de arquivos viabilizam a funcionalidade de rede.
10.5 E-mail	Explicar como os serviços de e-mail viabilizam a funcionalidade de rede.
10.6 HTTP	Explicar como os serviços de HTTP viabilizam a funcionalidade de rede.
10.7 Resumo dos serviços de rede	Um breve resumo e o teste do módulo.
Módulo 11. Dispositivos de comunicação de rede	**Explicar como os dispositivos de rede viabilizam a comunicação de rede com e sem fio.**
11.0 Introdução	Uma introdução ao módulo.
11.1 Dispositivos de rede	Explicar como os dispositivos de rede viabilizam a comunicação de rede.

Módulo/Tópicos	Metas/Objetivos
11.2 Comunicações sem fio	Explicar como os dispositivos sem fio viabilizam a comunicação de rede.
11.3 Resumo dos dispositivos de comunicação de rede	Um breve resumo e o teste do módulo.
Módulo 12. Infraestrutura de segurança de rede	**Explicar como os dispositivos e serviços de rede são usados para melhorar a segurança da rede.**
12.0 Introdução	Uma introdução ao módulo.
12.1 Topologias de rede	Explicar como os projetos de rede influenciam o fluxo de tráfego pela rede.
12.2 Dispositivos de segurança	Explicar como os dispositivos especializados são usados para aprimorar a segurança da rede.
12.3 Serviços de segurança	Explicar como os serviços de rede melhoram a segurança da rede.
12.4 Resumo da infraestrutura de segurança de rede	Um breve resumo deste módulo.
Módulo 13. Invasores e suas ferramentas	**Explicar como as redes são atacadas.**
13.0 Introdução	Uma introdução ao módulo.
13.1 Quem está atacando nossa rede?	Explicar como as ameaças à rede evoluíram.
13.2 Ferramentas dos agentes de ameaças	Descrever os vários tipos de ferramentas de ataque usadas pelos agentes de ameaças.
13.3 Resumo dos invasores e suas ferramentas	Um breve resumo e o teste do módulo.
Módulo 14. Ameaças e ataques comuns	**Explicar os vários tipos de ameaças e ataques.**
14.0 Introdução	Uma introdução ao módulo.
14.1 Malware	Descrever os tipos de malware.
14.2 Ataques de rede comuns - reconhecimento, acesso e engenharia social	Explicar os ataques de reconhecimento, acesso e engenharia social.
14.3 Ataques de rede – negação de serviço, saturação de buffer e evasão	Explicar a negação de serviço, a saturação de buffer e os ataques de evasão.
14.4 Resumo de ameaças e ataques comuns	Um breve resumo e o teste do módulo.
Módulo 15. Observação da operação de rede	**Explicar o monitoramento do tráfego de rede.**
15.0 Introdução	Uma introdução ao módulo.
15.1 Introdução ao monitoramento de rede	Explicar a importância do monitoramento de rede
15.2 Introdução às ferramentas de monitoramento de rede	Explicar como o monitoramento de rede é realizado.
15.3 Resumo do monitoramento e das ferramentas de rede	Um breve resumo e o teste do módulo.
Módulo 16. Ataque à base	**Explicar como as vulnerabilidades de TCP/IP possibilitam**

Módulo/Tópicos	Metas/Objetivos
	ataques de rede.
16.0 Introdução	Uma introdução ao módulo.
16.1 Detalhes da PDU IP	Explicar a estrutura de cabeçalho IPv4 e IPv6.
16.2 Vulnerabilidades de IP	Explicar como as vulnerabilidades de IP possibilitam ataques de rede.
16.3 Vulnerabilidades de TCP e UDP	Explicar como as vulnerabilidades de TCP e UDP possibilitam ataques de rede.
16.4 Resumo do ataque à base	Um breve resumo e o teste do módulo.
Módulo 17. Ataque ao trabalho	**Explicar como os aplicativos e serviços de rede comuns estão vulneráveis ao ataque.**
17.0 Introdução	Uma introdução ao módulo.
17.1 Serviços IP	Explicar as vulnerabilidades do serviço IP.
17.2 Serviços corporativos	Explicar como as vulnerabilidades dos aplicativos de rede possibilitam ataques de rede.
17.3 Resumo do ataque ao nosso trabalho	Um breve resumo e o teste do módulo.
Módulo 18. Noções básicas sobre defesa	**Explicar as abordagens para a defesa de segurança da rede.**
18.0 Introdução	Uma introdução ao módulo.
18.1 Defense-in-Depth	Explicar como a estratégia de defense-in-depth é usada para proteger as redes.
18.2 Políticas de segurança, regulamentos e padrões	Explicar as políticas, os regulamentos e os padrões de segurança.
18.3 Resumo das noções básicas de defesa	Um breve resumo e o teste do módulo.
Módulo 19. Controle de acesso	**Explicar o controle de acesso como um método de proteção de rede.**
19.0 Introdução	Uma introdução ao módulo.
19.1 Conceitos de controle de acesso	Explicar como o controle de acesso protege os dados da rede.
19.2 Uso e operação de AAA	Explicar como o AAA é usado para controlar o acesso à rede.
19.3 Resumo do controle de acesso	Um breve resumo e o teste do módulo.
Módulo 20. Inteligência de ameaças	**Usar várias fontes de inteligência para localizar as ameaças à segurança atuais.**
20.0 Introdução	Uma introdução ao módulo.
20.1 Fontes de informações	Descrever as fontes de informações usadas para comunicar ameaças emergentes à segurança de rede.
20.2 Serviços de inteligência de ameaças	Descrever vários serviços de inteligência de ameaças.

Módulo/Tópicos	Metas/Objetivos
20.3 Resumo da inteligência de ameaças	Um breve resumo e o teste do módulo.
Módulo 21. Criptografia	**Explicar como a infraestrutura de chave pública oferece suporte à segurança da rede.**
21.0 Introdução	Uma introdução ao módulo.
21.1 Integridade e autenticidade	Explicar o papel da criptografia para garantir a integridade e autenticidade dos dados.
21.2 Confidencialidade	Explicar como as abordagens criptográficas aumentam a confidencialidade dos dados.
21.3 Criptografia de chave pública	Explicar a criptografia de chave pública.
21.4 Autoridades e o sistema de confiança de PKI	Explicar como funciona a infraestrutura de chave pública.
21.5 Aplicações e impactos da criptografia	Explicar como o uso da criptografia afeta as operações de segurança cibernética.
21.6 Resumo da criptografia	Um breve resumo deste módulo.
Módulo 22. Proteção de endpoints	**Explicar como um site de análise de malware gera um relatório de análise de malware.**
22.0 Introdução	Uma introdução ao módulo.
22.1 Proteção antimalware	Explicar os métodos de mitigação de malware.
22.2 Prevenção contra invasões baseada em host	Explicar as entradas de registro de IPS/IDS baseadas em host.
22.3 Segurança de aplicativos	Explicar como a sandbox é usada para analisar malware.
22.4 Resumo da proteção do endpoint	Um breve resumo e o teste do módulo.
Módulo 23. Avaliação das vulnerabilidades de endpoint	**Explicar como as vulnerabilidades de endpoint são avaliadas e gerenciadas.**
23.0 Introdução	Uma introdução ao módulo.
23.1 Perfil de rede e servidor	Explicar o valor do perfil de rede e servidor.
23.2 Common Vulnerability Scoring System (CVSS)	Explicar como os relatórios de CVSS são usados para descrever as vulnerabilidades de segurança.
23.3 Gerenciamento de dispositivo seguro	Explicar como as técnicas de gerenciamento de dispositivo seguro são usadas para proteger dados e ativos.
23.4 Sistemas de gerenciamento de segurança da informação	Explicar como os sistemas de gerenciamento de segurança da informação são usados para proteger os ativos.
23.5 Resumo da avaliação das vulnerabilidades de endpoint	Um breve resumo e o teste do módulo.
Módulo 24. Tecnologias e protocolos	**Explicar como as tecnologias de segurança afetam o monitoramento de segurança.**

Módulo/Tópicos	Metas/Objetivos
24.0 Introdução	Uma introdução ao módulo.
24.1 Protocolos comuns de monitoramento	Explicar o comportamento dos protocolos de rede comuns no contexto do monitoramento de segurança.
24.2 Tecnologias de segurança	Explicar como as tecnologias de segurança afetam a capacidade de monitorar protocolos de rede comuns.
24.3 Resumo de tecnologias e protocolos	Um breve resumo e o teste do módulo.
Módulo 25. Dados de segurança de rede	**Explicar os tipos de dados de segurança de rede usados no monitoramento de segurança.**
25.0 Introdução	Uma introdução ao módulo.
25.1 Tipos de dados de segurança	Descreva os tipos de dados usados no monitoramento de segurança.
25.2 Registros de dispositivo final	Descrever os elementos de um arquivo de log de dispositivo final.
25.3 Registros de rede	Descrever os elementos de um arquivo de log de dispositivo de rede.
25.4 Resumo dos dados de segurança de rede	Um breve resumo e o teste do módulo.
Módulo 26. Avaliação de alertas	**Explicar o processo de avaliação de alertas.**
26.0 Introdução	Uma introdução ao módulo.
26.1 Fonte de alertas	Identificar a estrutura dos alertas.
26.2 Resumo da avaliação de alerta	Explicar como os alertas são classificados.
26.3 Resumo da avaliação de alertas	Um breve resumo e o teste do módulo.
Módulo 27. Como trabalhar com dados de segurança de rede	**Interpretar dados para determinar a origem de um alerta.**
27.0 Introdução	Uma introdução ao módulo.
27.1 Uma plataforma de dados comum	Explicar como os dados são preparados para uso no sistema de monitoramento de segurança de rede (NSM).
27.2 Investigação dos dados de rede	Usar as ferramentas de Security Onion para investigar eventos de segurança de rede.
27.3 Como melhorar o trabalho do analista de segurança cibernética	Descrever as ferramentas de monitoramento de rede que melhoram o gerenciamento do fluxo de trabalho.
27.4 Resumo do trabalho com os dados de segurança de rede	Um breve resumo e o teste do módulo.
Módulo 28. Computação forense digital e análise e resposta a incidentes	**Explicar como o CyberOps Associate responde a incidentes de segurança cibernética.**
28.0 Introdução	Uma introdução ao módulo.
28.1 Manipulação de evidências e atribuição de ataques	Explicar o papel dos processos de computação forense digital.

Módulo/Tópicos	Metas/Objetivos
28.2 A Cyber Kill Chain	Identificar as etapas na Cyber Kill Chain.
28.3 O modelo diamante da análise de invasão	Classificar um evento de invasão usando o Diamond Model.
28.4 Resposta a incidentes	Aplicar os procedimentos de tratamento de incidentes do NIST 800-61r2 a determinado cenário de incidentes.
28.5 Resumo da computação forense digital e análise e resposta a incidentes	Um breve resumo deste módulo.
28.6 Prepare-se para o exame e inicie sua carreira.	Preparação de certificação, vouchers de desconto e outros recursos profissionais.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**