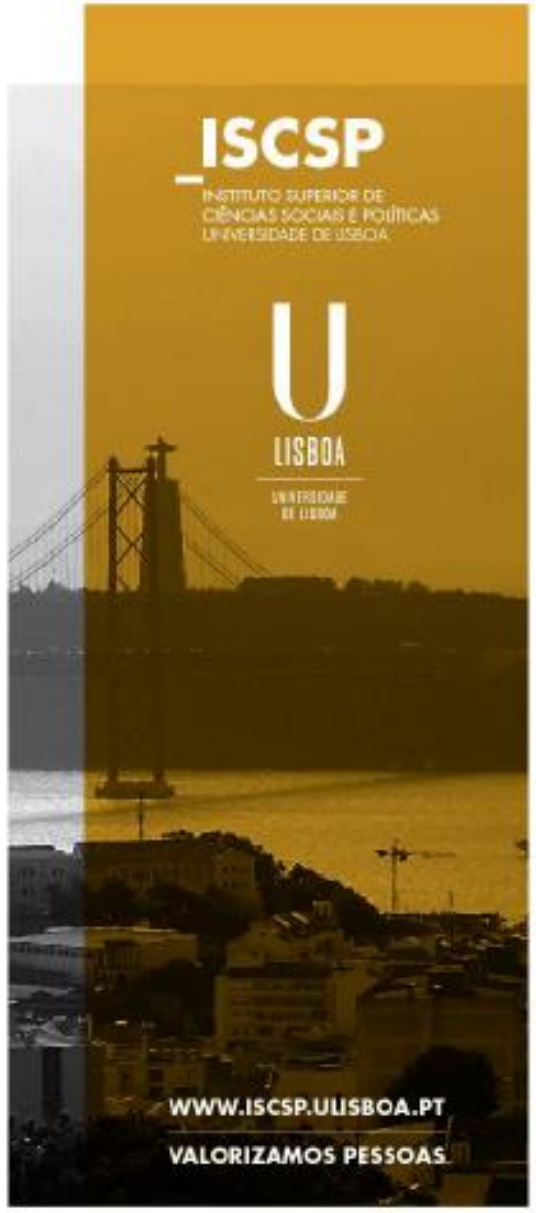
Contratação e Compras Públicas
2024-2025

Desafios e Evolução da Cibersegurança

João Rolo

jrolo@iscsp.ulisboa.pt



MANTER AS PALAVRAS-PASSE SECRETAS E SEGURAS

1. Mantenha as suas palavras-passe apenas sob o seu conhecimento;
2. Crie palavras-passe longas (frases-chave): pelo menos 12 caracteres, e não use termos próximos, como nome, cidade onde nasceu, ou termos conhecidos, como 1234;
3. Use palavras-passe diferentes para cada serviço, guarde-as num gestor de palavras-passe;
4. Altere-as imediatamente caso suspeite de comprometimento;
5. Evite guardar as palavras-passe nos *browsers;*
6. Se possível, ative a autenticação de múltiplo fator;
7. Altere a palavra-passe de origem na compra de um dispositivo - por exemplo, a que é associada à instalação do Wi-Fi doméstico;

Administração Pública é uma peça fundamental na cibersegurança do país

Não só porque deve dar o exemplo às outras organizações, como porque presta serviços muito importantes para o funcionamento da sociedade, a Administração Pública (e a sua cibersegurança) afeta todos os cidadãos, direta ou indiretamente.

Por essa razão, o CNCS disponibiliza um conjunto de recursos que procuram ajudar os organismos e serviços da Administração Pública a atingirem a maturidade em cibersegurança.

A palavra-passe é um dos mecanismos mais importantes de segurança contra acessos indevidos a plataformas digitais, algumas delas com informação pessoal ou sensível, como o *email* ou o banco *online.*

Quando a nossa palavra-passe é comprometida, ficamos vulneráveis ao roubo de identidade através das redes sociais, ao uso indevido da nossa conta bancária ou à exfiltração de dados pessoais.

Existem programas que permitem descobrir automaticamente as palavras-passe caso elas sejam fracas.

No mercado negro da Internet, vendem-se listas de palavras-passe roubadas, por isso é importante alterá-las quando desconfiamos do seu comprometimento.

Também é fundamental evitar que, na descoberta de uma palavra-passe por um agente malicioso, ele tenha acesso a mais do que uma plataforma

Garantir a Cibersegurança do Teletrabalho ou Trabalho à Distância

Cuide dos dispositivos:

- Utilize de preferência dispositivos autorizados pela sua organização e, se os perder, informe o responsável de cibersegurança;
- Seja o único a utilizá-los – evite que terceiros os utilizem;
- Use apenas pens USBs confiáveis;
- Ative o bloqueio automático dos dispositivos e use PIN ou password;
- Utilize filtro no ecrã do portátil.

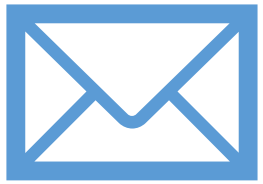
Cuide dos sistemas e dos dados:

Garanta junto da sua organização que os dispositivos estão atualizados e têm o antivírus e a firewall ativados;

Faça backups regulares para um dispositivo externo.

- **Cuide da navegação:**

  Evite usar o Wi-Fi de espaços públicos e utilize sempre a VPN da sua organização;
- Navegue sempre em websitesHTTPS;
- Altere a password do Wi-Fi doméstico depois da instalação;
- Garanta que o seu Wi-Fi doméstico tem uma password forte, secreta e altere-a regularmente;
- Altere o nome do seu Wi-Fi doméstico de modo a não ser facilmente identificado como seu;
- Escolha o modo de cifrar mais forte da sua rede Wi-Fi;
- Garanta que a rede da sua organização é segmentada de modo a proteger a rede interna.



Cuide da comunicação:

Não abra emails ou SMS, nem clique em links ou anexos, desconhecidos;

Cifre as comunicações sensíveis;

Não partilhe informação profissional nas redes sociais.

Os trabalhadores, voluntaria ou involuntariamente, são por vezes os principais responsáveis por ciberataques que afetam as suas organizações (insider).

Na verdade, frequentemente, essa responsabilidade resulta mais da falta de cuidado do que de intenções maliciosas.

É por essa razão que em cibersegurança se dá tanta importância ao fator humano.

Por mais que as organizações estejam apetrechadas das melhores infraestruturas técnicas de proteção, basta um erro humano para colocar a cibersegurança em causa, nomeadamente através de ações como clicar num link com software malicioso, partilhar informação sensível com agentes mal intencionados ou em websites inseguros, perder dispositivos não bloqueados, utilizar pens comprometidas, aceder a Wi-Fi públicos ou não ter o Wi-Fi doméstico com uma password segura.

- Os trabalhadores de algumas organizações, quer públicas, quer privadas, podem ser alvos apetecíveis para atividades de ciberespionagem.
- Quando a organização é privada e com fins lucrativos, normalmente o motivo é económico e prende-se com a espionagem industrial, visando obter informação privilegiada para a competitividade.
- Contudo, noutros casos, em geral ligados a organizações públicas, os motivos podem colocar em causa a segurança nacional.

A informação, profissional ou privada, que os trabalhadores expõem na Internet pode ser utilizada contra eles, em atos de engenharia social, como phishing, smishing, vishing ou deep fake de modo a levar estes trabalhadores, isolados em teletrabalho, a agir beneficiando o infrator, como seja fornecendo credenciais, fazendo transferências bancárias ou transmitindo outras informações sensíveis.

Em muitas situações esta engenharia social atua simulando a identidade do CEO ou de outra chefia (CEO fraud) de modo a tornar-se mais credível e com autoridade.

Phishing:

O **phishing** consiste no envio de mensagens fraudulentas a partir de uma suposta fonte segura e credível tentando convencer-nos a atuar sobre algo que de outra forma não faríamos. É usualmente feito **via email** e tem como objetivo o **roubo de informação pessoal e sensível** como dados de cartões de crédito e palavras-passe ou conseguir instalar malware, um software malicioso, no computador da vítima.

O termo malware refere-se a um software nocivo que interrompe ou manipula a operação normal de um dispositivo eletrónico. Pode infetar computadores pessoais, smartphones, tablets, servidores e até mesmo equipamentos domésticos — basicamente qualquer dispositivo com recursos de computação e que esteja ligado à internet.

Malware

- O malware pode entrar no seu dispositivo enquanto navega em sites pirateados, clica em demonstrações de jogos, transfere ficheiros de música infetados, instala novas barras de ferramentas, configura software de uma fonte suspeita, abre um anexo de um e-mail malicioso ou quando faz download de conteúdo da Internet para um dispositivo que não esteja protegido.
- Pode esconder-se em aplicações aparentemente legítimas, especialmente quando descarregadas de sites ou através de SMS, em vez de uma loja segura. Consoante os diferentes tipos de malware, o código malicioso executa ações que podem incluir:
- Auto-replicação em diferentes partes do sistema de ficheiros
- Reduzir a velocidade do sistema operativo
- Bloquear o acesso a documentos, programas ou até ao sistema, obrigando o utilizador a fazer um pagamento para recuperar o acesso
- Bombardear o computador com pop-ups
- Tornar o dispositivo inoperável

Malware

- Ao espalhar malware, os cibercriminosos podem ter vários objetivos. Sendo os principais:
- **Roubo de identidade**. Podem utilizar os seus dados pessoais para se fazerem passar por si - ou vendê-los na dark web - e cometer crimes.
- **Aceder à sua conta bancária**. Utilizando técnicas de spyware, os hackers podem roubar as suas passwords e, assim, conseguirem entrar na sua conta bancária para desviarem dinheiro.
- **Espionagem empresarial**. As empresas podem roubar informações da concorrência para depois utilizá-las a seu favor.
- **Sabotagem**. Às vezes, a intenção é apenas causar o caos. Os hackers podem apagar apagar ficheiros, registos ou impedir que acedam ao sistema para causar danos.
- **Extorsão**. A técnica de ransomware criptografa os arquivos ou dispositivos da vítima e exige pagamento para autorizar o acesso de novo. O objetivo é fazer com que a vítima – uma pessoa, instituição ou governo – pague o resgate.
- **Mineração de criptomoedas**. Forçando o computador da vítima a gerar ou minerar criptomoedas para o invasor.

- Quando se trata de malware, é melhor prevenir do que remediar. Incorpore as seguintes dicas na sua vida digital para minimizar o risco e proteger-se contra um possível ataque:
- **Não confie em estranhos online**. E-mails desconhecidos, alertas abruptos e perfis falsos são os métodos mais comuns para espalhar malware. A regra é: em caso de dúvida, não clique.
- **Investigue antes de fazer downloads**. É importante verificar se o site de onde está a fazer o download é confiável.
- **Instale um bloqueador de anúncios**. Alguns anúncios infetados (mais conhecido como malvertising) podem instalar malware no seu dispositivo assim que aparecem, sem que tenha de clicar.
- **Mantenha o seu software atualizado**. Caso contrário pode deixar o seu dispositivo vulnerável.
- **Evite clicar em pop-ups**. Sempre que conseguir, feche a janela no “X” que costuma estar no canto superior direito.
- **Atenção aos e-mails**. Se receber uma mensagem do seu banco a pedir para clicar num link, para fornecer dados pessoais ou para alterar os códigos de acesso ao homebanking, não o faça e denuncie a situação.
- **Execute análises regularmente**. Utilizando o software de segurança que instalou no dispositivo.

Smishing

- **Smishing** é quando alguém tenta convencê-lo a fornecer informações privadas através de mensagens SMS ou de texto
- O smishing é todo tipo de phishing que envolve uma mensagem de texto. Na maioria das vezes, essa forma de phishing envolve uma mensagem de texto via SMS ou número de telefone. O smishing é perigoso porque as pessoas parecem confiar mais em uma mensagem de texto do que em um email. Muitas pessoas estão cientes dos riscos de segurança associados a clicar em links contidos em emails. Isso não é tão claro em relação a mensagens de texto.
- O smishing utiliza elementos de **engenharia social** para convencê-lo a compartilhar suas informações pessoais. Essa tática aproveita da sua confiança para obter suas informações. Smishers estão em busca de diferentes informações, como senhas online, números de CPF ou de cartões de crédito. Depois que obtêm essas informações, eles com frequência passam a solicitar novos cartões de crédito em seu nome, e aqui começam os seus problemas.
- Outra tática usada pelos smishers é ameaçá-lo de começar a cobrar uma tarifa diária pelo uso de um serviço, caso você não clique em um link e insira as informações pessoais solicitadas. Se você não se inscreveu no serviço, ignore a mensagem. Caso detecte alguma cobrança não autorizada em seu cartão de crédito ou débito, entre em contato com o banco. Eles atuarão para defendê-lo.

- Em geral, não responda a mensagens de texto de pessoas desconhecidas. Essa é a melhor forma de se manter protegido. Isso é ainda mais relevante quando o SMS for enviado de um número de telefone incomum, que você não reconhece. Esse é um sinal de que a mensagem de texto é na verdade um email enviado a um telefone. Tome precauções básicas ao usar o telefone, como:
- Não clique em links que receber no telefone, a não ser que conheça a pessoa que o enviou. Mesmo se receber uma mensagem de texto de um amigo que contenha um link, verifique se o remetente enviou mesmo o link antes de clicar nele.
- Nunca instale aplicativos a partir de mensagens de texto. Todos os aplicativos que deseja instalar em seu dispositivo deverão ser obtidos diretamente da App Store oficial. Esses programas passam por procedimentos de testes rigorosos antes de serem colocados no mercado. É sempre melhor prevenir do que remediar. Se estiver em dúvida em relação à segurança de uma mensagem de texto, não a abra.

CHAMADAS DE VISHING

O vishing (combinação das palavras voice e phishing) é um ataque por telefone no qual o atacante tenta enganar a vítima para que esta forneça dados pessoais, financeiros ou de segurança ou transfira dinheiro para ele.

O QUE PODE FAZER?

- **Tenha cuidado** com chamadas não solicitadas.
- **Anote o número de quem liga** e indique-lhe que vai ligar de volta.
- Para verificar a identidade de quem liga, **procure o número de telefone da entidade** e ligue diretamente para lá.
- **Não valide quem lhe liga usando o número de telefone que essa pessoa lhe deu** (pode ser falso ou mascarado).
- Os atacantes podem encontrar os seus dados básicos online (redes sociais, p.ex.). **Não assuma que a chamada é genuína** porque têm esses dados.
- **Não partilhe** o PIN do cartão de crédito ou débito nem a password do seu homebanking. O seu banco não lhe pede esses dados.
- **Não transfira dinheiro** para outra conta a pedido de quem lhe liga. O seu banco nunca lho pedirá.
- Se acha que a chamada é falsa, **reporte-o ao seu banco.**

- O CERT.PT é um serviço integrante do CNCS que coordena a resposta a incidentes envolvendo entidades da Administração Pública, operadores de infraestruturas críticas, operadores de serviços essenciais e prestadores de serviços digitais além de todo o ciberespaço nacional, incluindo qualquer dispositivo pertencente a uma rede ou bloco de endereçamento atribuído a um operador de comunicações eletrónicas, instituição, pessoa coletiva ou singular com sede em território Português, ou que esteja fisicamente localizado em território Português.
- O CERT.PT reconhece, suporta e respeita os parâmetros de classificação e utilização da informação estabelecidos no Protocolo Traffic Light Protocol (TLP),
- O CERT.PT é membro da Rede Nacional de CSIRT e representante nacional na Rede Europeia de CSIRT, estabelecida pela Diretiva (EU) 2016/1148 (Diretiva SRI).
- O CERT.PT é membro acreditado do Trusted Introducer e Full Member do Forum of Incident Response and Security Teams (FIRST).

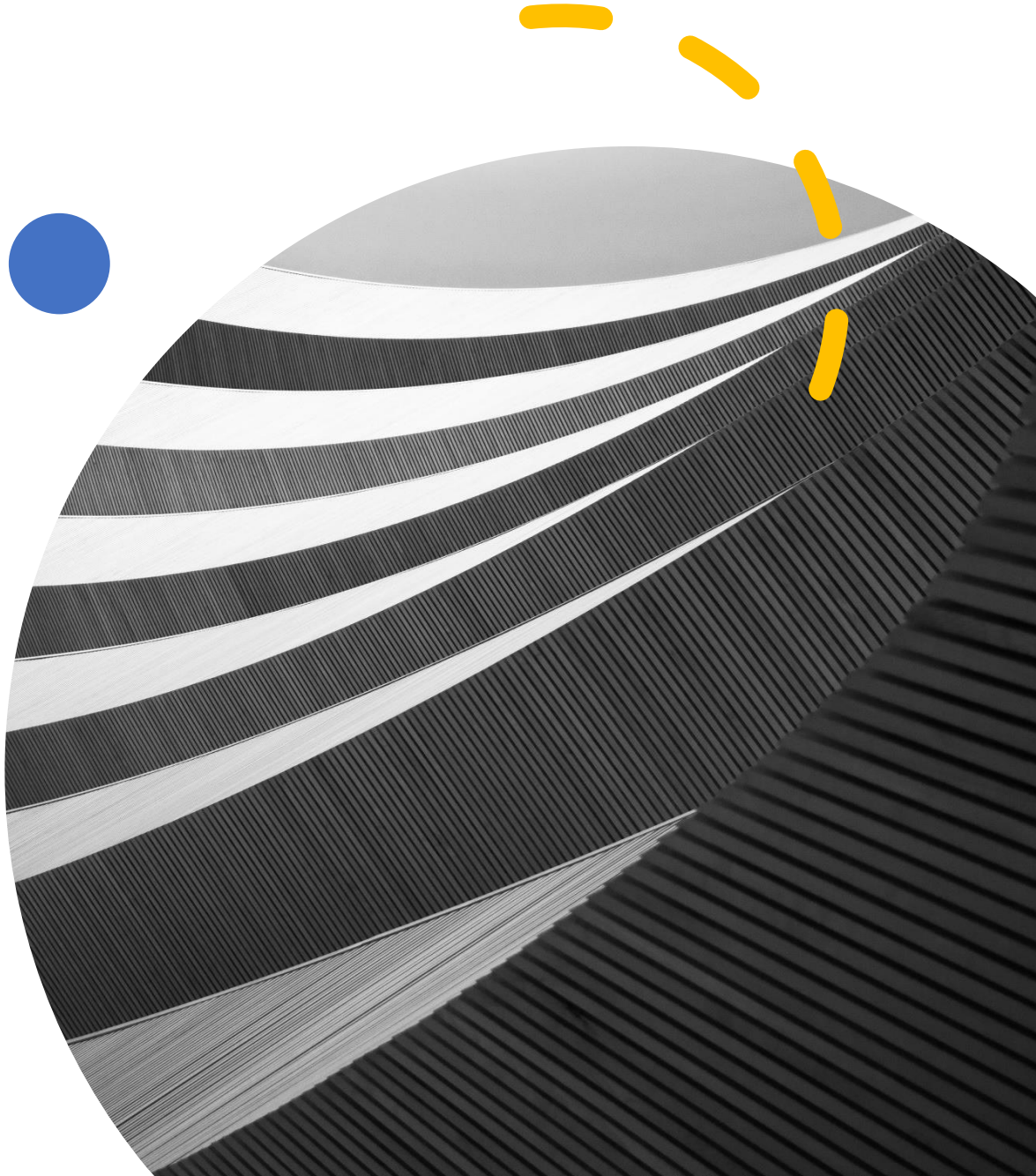
Para contatar o CERT.PT por favor utilize os seguintes contactos:
- Notificação de incidentes de cibersegurança:
cert@cert.pt

A resposta a incidentes é o processo de uma empresa para reagir a ameaças de TI, como ataques cibernéticos, violação de segurança e tempo de inatividade do servidor.

Outras equipes de operações de TI e DevOps podem se referir à prática como gerenciamento de incidentes graves ou gerenciamento de incidentes.

As seções a seguir descrevem um processo de resposta a incidentes, o que fazer entre perceber que um serviço está inativo e fazer ele funcionar de novo

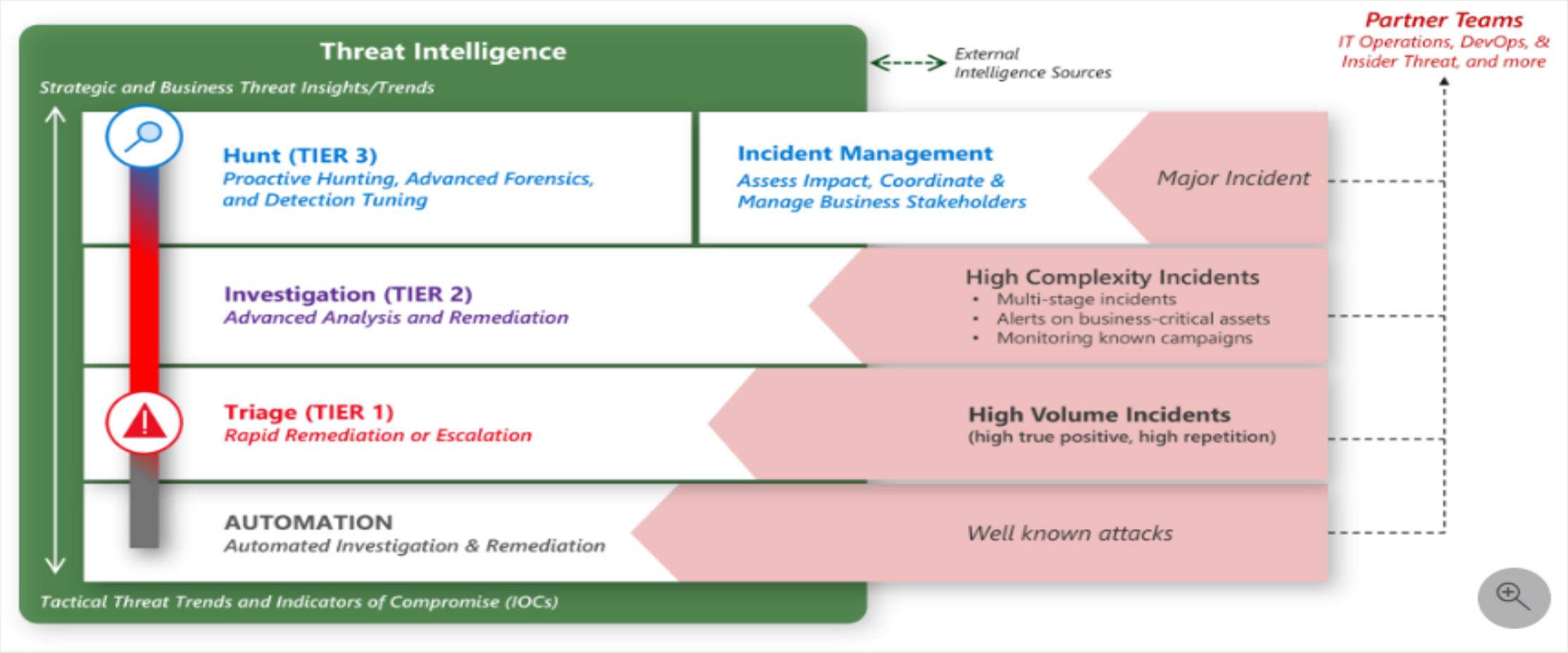

Identificar o incidente
Definir canais de comunicação da equipe
Avaliar o impacto e aplicar um nível de gravidade
Comunique-se com os clientes
Escalonar para os respondentes certos
Delegar funções de resposta a incidentes
Resolver o incidente



- As operações de segurança (SecOps) são por vezes referidas ou estruturadas como um centro de operações de segurança (**SOC**).
- As operações de segurança podem ser altamente técnicas, mas o mais importante, é uma disciplina humana. Pessoas são o bem mais valioso nas operações de segurança. A sua experiência, habilidade, perspicácia, criatividade e engenho são o que torna a disciplina eficaz.
- Os ataques à sua organização também são planeados e conduzidos por pessoas como criminosos, espiões e hacktivistas.
- **Concentre-se em capacitar as pessoas**: o seu objetivo não deve ser substituir pessoas por automação. Capacitar o seu pessoal com ferramentas que simplificam os seus fluxos de trabalho diários. Estas ferramentas permitem-lhes acompanhar ou ficar à frente dos adversários que enfrentam.
- A rápida separação do sinal (deteções reais) do ruído (falsos positivos) requer investimentos tanto em RH como em automação. A automação e a tecnologia podem reduzir o trabalho humano, mas os hackers são o julgamento humano e humano é fundamental para os derrotar.
- **Diversificar o seu portfólio de pensamento**: as operações de segurança podem ser altamente técnicas, mas também é apenas mais uma nova versão da investigação forense que aparece em muitos campos de carreira como a justiça criminal. Não tenha medo de contratar pessoas com uma forte competência na investigação ou razões dedutivas ou indutivas e treiná-las em tecnologia.
- Certifique-se de que a sua equipa está preparada com uma cultura saudável e está a medir os resultados certos. Estas práticas podem aumentar a produtividade da sua equipa.

Modelo de operações de segurança

As operações de segurança lidam com uma combinação de incidentes de grande volume e incidentes de alta complexidade.



As equipas de operações de segurança concentram-se frequentemente em três resultados fundamentais:

- **Gestão de incidentes:** Gerir ataques ativos ao ambiente, incluindo:
  - **Reagindo reactivamente** aos ataques detetados.
  - **Proativamente à procura de** ataques que escaparam através de deteções tradicionais de ameaças.
  - **Coordenação** das implicações legais, comunicações e outros negócios de incidentes de segurança.
- **Preparação do incidente:** Ajude a organização a preparar-se para futuros ataques. A preparação de incidentes é um conjunto estratégico mais alargado de atividades que visam a construção da memória muscular e do contexto a todos os níveis da organização. Esta estratégia prepara as pessoas para lidarem melhor com os grandes ataques e obterem informações sobre as melhorias do processo de segurança.
- **Inteligência de ameaça:** Reunir, processar e divulgar informações de ameaças a operações de segurança, equipas de segurança, liderança de segurança e partes interessadas na liderança do negócio através da liderança de segurança.

PRACTICE EXERCISES / TABLETOPS

Leadership involved in practice exercises to build awareness and muscle memory

BUSINESS PRIORITIES

Inform security teams of critical business assets and priorities

MAJOR INCIDENT STATUS

Inform business stakeholders of incidents and status