Secure Journey: un viaggio per raggiungere una buona Cyber Posture

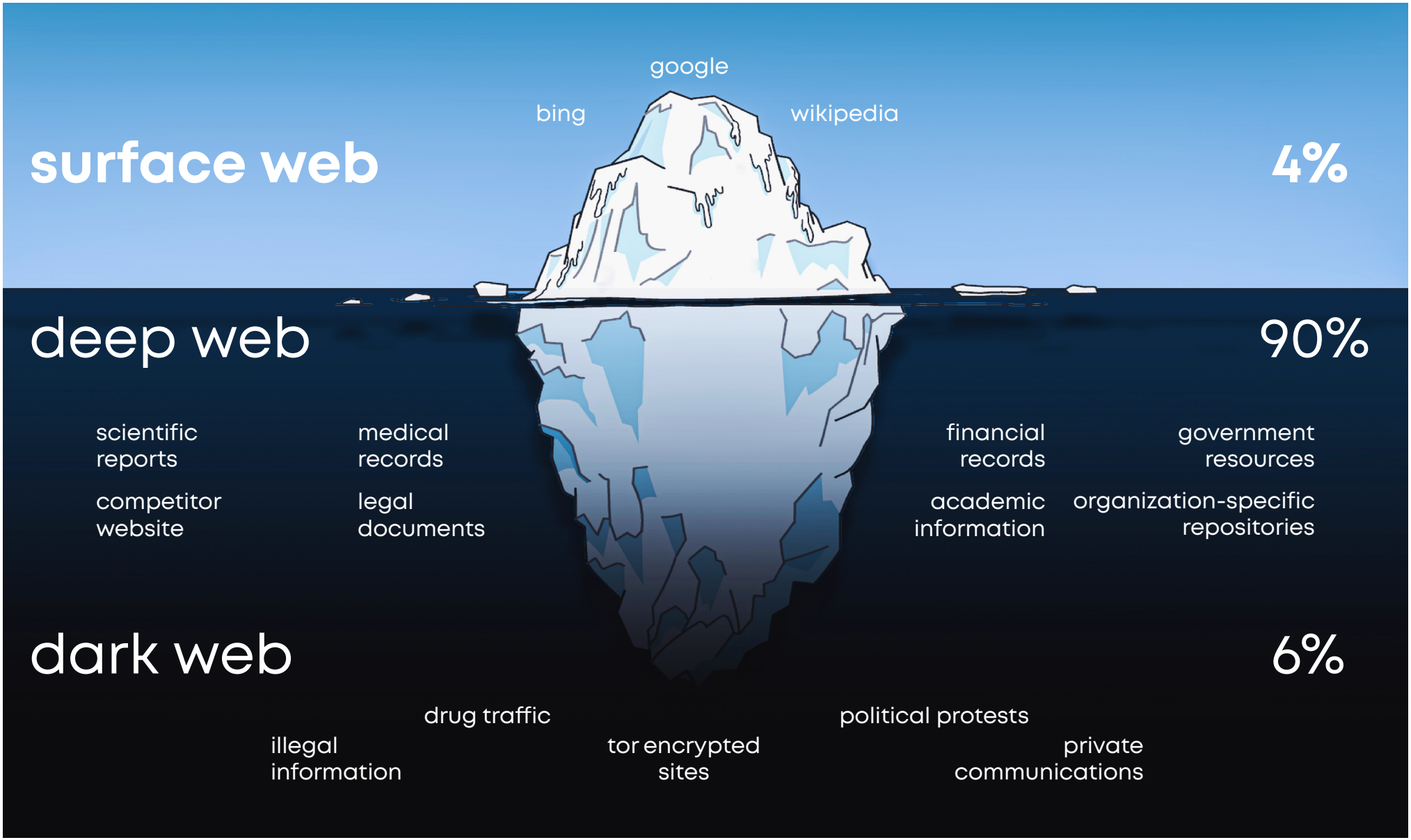
Il cyberspazio è un nuovo fronte culturale e economico: è il quinto dominio del warfare e sta diventando sempre più complesso e frequentato dalla (cyber) criminalità.

BlueIT®

Al cyberspazio si sono aggiunti i dispositivi Internet-of-Things (IoT) e, con il paradigma Industry 4.0, anche i sistemi OT di fabbrica esponendoli a maggiori rischi di attacchi informatici.

Veicoli e mezzi di trasporto sono sempre più automatizzati e connessi a Internet. La robotica e la telemedicina sono entrate nelle sale operatorie e alcuni dispositivi salva-vita sono controllabili attraverso reti wireless.

Deep e dark web indicano due territori digitali differenti, dove si possono acquistare informazioni e molte altre cose, spesso illecite.



L'Internet di superficie, quella a cui accediamo tutti i giorni, è la parte della rete che viene mappata dai motori di ricerca tradizionali, ma rappresenta solo una piccola parte della rete: circa il 4%.

La **cyber security** è focalizzata principalmente sulla protezione dei sistemi informatici e dell'informazione in formato digitale da attacchi interni e esterni; mentre la **sicurezza delle informazioni** comprende invece anche la protezione delle informazioni in formato non digitale, ad esempio cartaceo.

La **sicurezza informativa** è l'insieme delle risorse, dei processi e delle tecnologie tesi alla protezione dei sistemi informativi in termini di disponibilità, confidenzialità e integrità dei beni o asset informativi.

Nella **sicurezza informativa** sono coinvolti elementi tecnici, organizzativi, giuridici e umani.

La superficie di attacco (attack surface) è l'insieme delle vulnerabilità che un malintenzionato può sfruttare per causare un incidente di information/cyber security.

Le vulnerabilità non sono solo tecniche ma sono insite anche nel comportamento delle persone e possono essere organizzative e di processo.

La superficie di attacco è in continua espansione e le tipologie di minaccia e di attacco sono sempre più creative e sofisticate.

I malintenzionati sono diversamente motivati. Si tratta perlopiù di insider, concorrenti, attivisti, terroristi, criminalità organizzata, eserciti.

La superficie di attacco è quindi l'insieme delle opportunità che può sfruttare un malintenzionato.

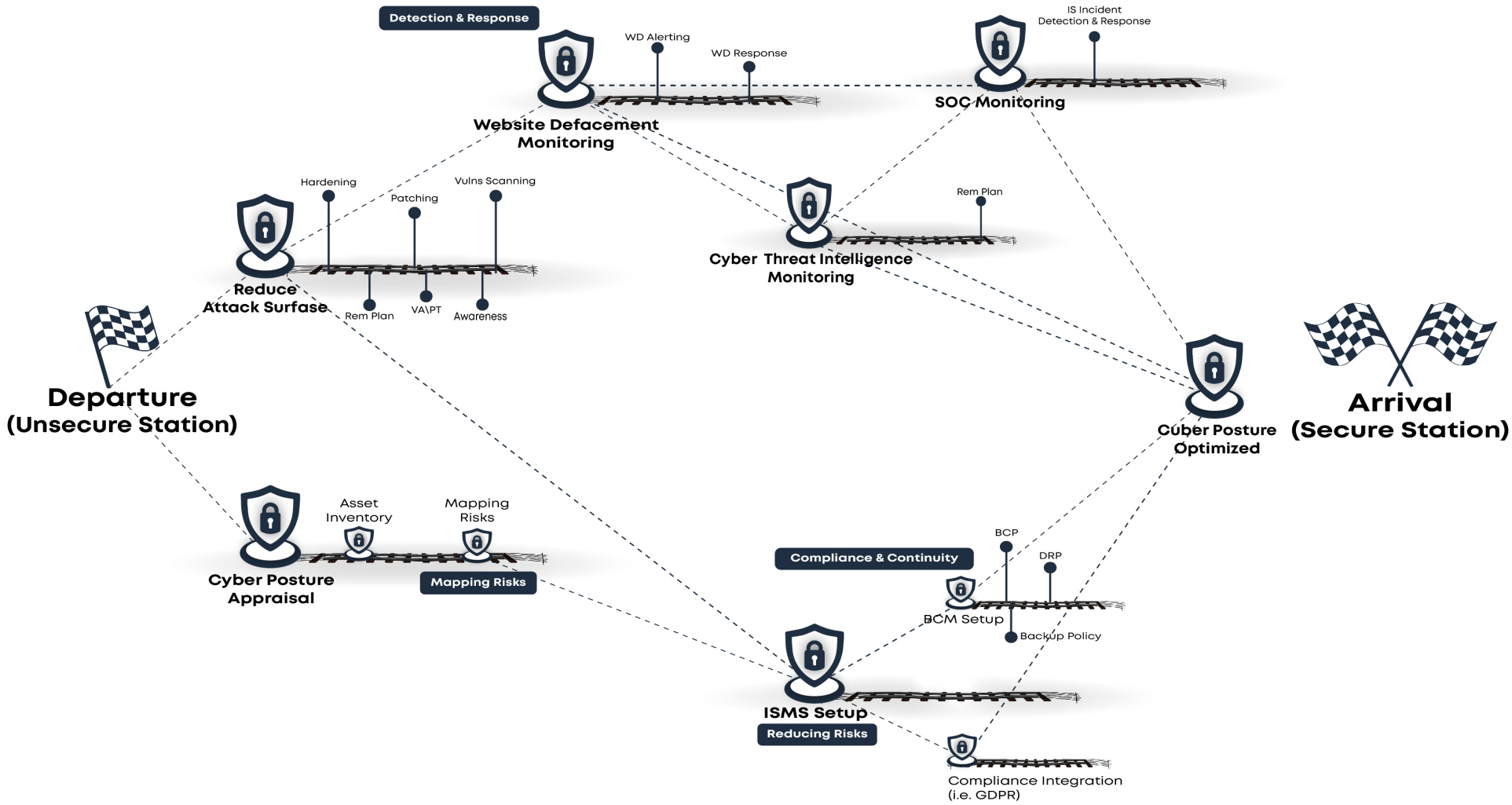
Poi ci sono da tenere in conto anche normative, leggi e regolamenti, generali o di settore, che hanno a che fare con il trattamento di dati e sistemi informativi.

Come può difendersi un'azienda da malintenzionati e minacce dal cyberspazio o anche dall'interno?

Un'azienda dovrebbe affrontare un percorso, un viaggio, al termine del quale la propria consapevolezza e la propria postura devono migliorare considerevolmente per affrontare, con minori rischi, la propria interconnessione con il cyberspazio.

BlueIT propone un "Secure Journey", un percorso per mettere le azienda in sicurezza e a minor rischio di attacchi cyber.

Contattaci per fissare un appuntamento con i nostri esperti: infoblueit@blueit.it



Partiamo dalla stazione di partenza: la Unsecure Station, dove la prima cosa da fare è rendersi conto di quale sia la postura attuale.

L’azienda sta gestendo i rischi, con un processo continuo per la loro riduzione?

Questo processo tiene conto delle relazioni tra gli elementi dei sistemi informativi (applicazioni, host e dati) e l’organizzazione aziendale con i suoi macro-processi?

Quanto è ampia la superficie di attacco e quali esposizioni e vulnerabilità sono pubblicate sul web?

Il primo bivio ha due direzioni, una logica e una fisica.

La direzione fisica porta alla stazione Reduce Attack Surface dove si attivano le scansioni delle vulnerabilità, i tentativi di intrusione, hardening, patching, remediation planning e, non meno importante, programmi di awareness indirizzati agli utenti. Tutto ciò allo scopo di ridurre l'esposizione agli attacchi.

La direzione logica porta alla mappatura di: processi, applicazioni, infrastrutture, dati, siti e locazioni; si attiva la gestione dei rischi, sia di business, che ICT.

Una prima fermata importante che si raggiunge da entrambi i percorsi è la ISMS Setup, che permette di ottenere una security organization e una security policy, fondamentali per dare continuità ai processi.

Da ISMS Setup vi è un altro bivio che porta a percorsi di costruzione della compliance e della continuità operativa (Business Continuity Management).

L’altro percorso che si può intraprendere dalla stazione Reduce Attack Surface è quello del monitoraggio attivo, secondo due direttrici: inside the firewall e beyond the firewall.

L’obiettivo è avere un servizio di vedetta sia al di fuori sia all’interno del perimetro (Detection & Response).

Per aziende che vogliono tutelare il proprio sito aziendale o i propri servizi esposti su Internet, è necessario passare per la stazione Website Defacement Monitoring (beyond the firewall).

La stazione Cyber Threat Intelligence Monitoring (beyond the firewall), porta al controllo periodico di ciò che si pubblica e si muove sul web, sia di superficie, sia sommerso, alla ricerca di vulnerabilità pubblicate, credenziali compromesse o rumours che possono far presagire un imminente attacco.

La stazione SOC Monitoring (inside the firewall), rappresenta il servizio di Security Operations Center 24x7, assistito da tecnologie SIEM.

Tutte i percorsi portano alla Secure Station e il costo del biglietto è proporzionale a quanta strada si vuole percorrere.

Raggiungere alcune stazioni intermedie costa di più, rispetto ad altre.

Ovviamente, più fermate intermedie si fanno, più la postura è migliore e i rischi inferiori.

Buon viaggio sicuro da BlueIT.