CYBER INTELLIGENCE REPORT

BlueIT SPA - www.blueit.it

Parliamo di

CYBER THREAT INTELLIGENCE

La Cyber Threat Intelligence (CTI) è l'applicazione di metodologie di intelligence alla cyber security che viene utilizzata a supporto delle attività di Prevention e Detection degli incidenti di sicurezza informativa. Il monitoraggio attivo, basato su analisi e correlazione degli eventi (indicatori), potrebbe non essere sufficiente e alcuni precursori che possono arrivare da fonti di CTI possono, in qualche modo, preannunciare un'azione malevola.

La CTI è la raccolta di informazioni relative a:

- intento: motivazioni e obiettivi degli attaccanti;
- opportunità: possibilità per gli attaccanti di sfruttare vulnerabilità e condizioni favorevoli al raggiungimento dei loro obiettivi;
- capacità: competenze tecniche utilizzate dagli avversari per arrivare ai loro obiettivi sfruttando le opportunità.

Vi sono molte informazioni reperibili sulla rete e che possono essere utilizzate per diverse tipologie di attacco. La Cyber Threat Intelligence (CTI) è l'applicazione di metodologie di intelligence alla cyber security che viene utilizzata a supporto delle attività di Prevention e Detection degli incidenti di sicurezza informativa. Il monitoraggio attivo, basato su analisi e correlazione degli eventi (indicatori), potrebbe non essere sufficiente e alcuni precursori che possono arrivare da fonti di CTI possono, in qualche modo, preannunciare un'azione malevola. Diventano quindi importanti i segnali provenienti dalla rete: sia dalla parte emersa (Surface), sia da quella sommersa (Deep & Dark).

COSA FACCIAMO

L'obiettivo del servizio è analizzare precursori e movimenti su siti e Black Market dove sono esposte o in vendita informazioni relative a Device o Business Email Compromised (BEC) o dichiarati vulnerabili. Questi precursori possono indicare tipologia e direzione di provenienza di possibili attacchi.

BlueIT®

YOUR COGNITIVE PARTNER

Per esempio, una BEC trovata in vendita ieri e non più presente oggi su di un Black Market indica un suo probabile ed imminente utilizzo per accedere ai sistemi aziendali, senza causare indicatori di "Failed Login". Il servizio di Cyber Intelligence Report consente ai nostri clienti di avere una fotografia (una tantum) o un monitoraggio attivo (servizio), con l'obiettivo di avere una visione, dall'esterno, della criticità della propria postura di Cyber Security e di eventuali segnali e movimenti ostili presenti sulla rete, senza analizzare alcun indicatore interno (non invasivo).

Vuoi conoscere tempi e modi per valutare i rischi per la tua azienda?
Contattaci: infoblueit@blueit.it

Il servizio di prova, a investimento, viene proposto per una investigazione CTI su un dominio Internet. Per l'avvio delle attività è richiesto solo un consenso e il nome del dominio o l'Indirizzo IP ad esso associato. Il nostro Cyber Threat Intelligence Team effettua ricerche e investigazioni sul web, producendo un report che viene poi presentato e discusso con il cliente: il Cyber Intelligence Report. Il report espone le minacce rilevate, suddivise nelle categorie: Attack Intention, Data Leakage, Phishing, Brand Security, VIP Users e Exploitable Data.