DiGi ONE
the leading
digital company

Chi siamo in sintesi

- Siamo una PMI INNOVATIVA del settore ICT
- Abbiamo 2 sedi operative: Roma e Terni
- INVESTIAMO in Ricerca&Sviluppo
- SVILUPPIAMO sistemi e soluzioni IT per aziende operanti nei principali settori di mercato: Pubblica Amministrazione, Industria, Enti Statali, Sanità, Istruzione, Terziario
- INTEGRIAMO le tecnologie più innovative, rendendole aderenti alle esigenze dei clienti, e di anticipare le future tendenze del business dell'era digitale
- COLLABORIAMO con i grandi Player tecnologici internazionali

Le nostre Partnership

20 anni di collaborazione, più di 30 Certificazioni, oltre 300 progetti, testimoniano la capacità di **DiGi ONE** di affiancare un Vendor di livello mondiale sul mercato

Microsoft è uno dei partner che completa la proposta **DiGi ONE** di Servizi per il Cloud e il Messaging & Collaboration in ambito Enterprise

DiGi ONE è partner Red Hat, quale leader di mercato per le soluzioni open source di tipo enterprise, in particolare per il cloud ibrido basato sulla piattaforma OpenShift.

HCL Software è parte del portfolio prodotti **DiGi ONE** per Messaging, Collaboration, Application Development, Digital Experience e Security.

Cisco è partner strategico nel range di offerta **DiGi ONE** che si riferisce alla Sicurezza in ambito IT/IoT/OT, Collaboration, Data Center Automation e Cloud.

Fortinet rappresenta un partner strategico di **DiGi ONE** per quel che concerne le loro soluzioni e prodotti inerenti gli aspetti di Sicurezza Industriale.

Centreon è il partner **DiGi ONE** per i servizi di monitoraggio dell'infrastruttura IT attraverso una supervisione globale, semplice e intuitiva.

DiGi ONE integra e supporta KOFAX, la piattaforma software di automazione per tecnologie e processi quali RPA, acquisizione cognitiva, mobilità e analisi.

Clienti e Referenze

INFORMATION TECHNOLOGY

- Computer Gross
- Engineering D. Hub
- FAURECIA Emissions Control Technologies Italy
- IBM Italia
- Italware
- Octotelematics
- Sistematica
- Terni Reti
- Thales Alenia Spazio
- TI Trust Technologies

SERVIZI

- IdeaRE - Idea Real Estate
- ItaliaCamp
- Media Point 95

PUBBLICA AMMINISTRAZIONE

- Agecontrol
- ASL RM3
- Autorità di Sistema Portuale del Mar Tirreno Settentrionale
- Autorità Garante del Commercio e del Mercato
- Azienda Ospedaliera di Terni
- Azienda Ospedaliera Universitaria Città della Salute e della Scienza di Torino
- Azienda Policlinico Umberto I - Roma
- Azienda Regionale per Innovazione e gli Acquisti (ARIA)
- Azienda Strade Lazio - Astral
- Azienda Unita' Sanitaria Locale Umbria 1
- Comune di Terni
- ENPAF - Ente Nazionale di Previdenza ed Assistenza Farmacisti
- ESA - European Space Agency
- ESTAR - Ente di Supporto Tecnico Amministrativo Regionale
- INMI Lazzaro Spallanzani
- Ministero Difesa
- Ministero Interno-Dipartimento Pubblica Sicurezza
- Ospedale Santa Maria della Misericordia di Perugia
- Regione Toscana - Giunta Regionale-Sistemi Informativi
- Senato della Repubblica
- Umbria Digitale scarl
- USL Toscana Centro
- USL Toscana Sud-Est

DiGi ONE the leading digital company

PRODUZIONE INDUSTRIALE

- Alcantara
- Cementerie Aldo Barbetti
- Co.Ri.Metal
- Elettronica
- GE AVIO
- Stannah
- Vitrociset
- COBLIGHT
- Consorzio S3Log
- IMA
- MBDA ITALIA

TELECOMUNICAZIONI&FINANZA

- Gepafin
- IBL Banca
- TIM
- SARA Assicurazioni
- Scai Solution Group

EDUCATION

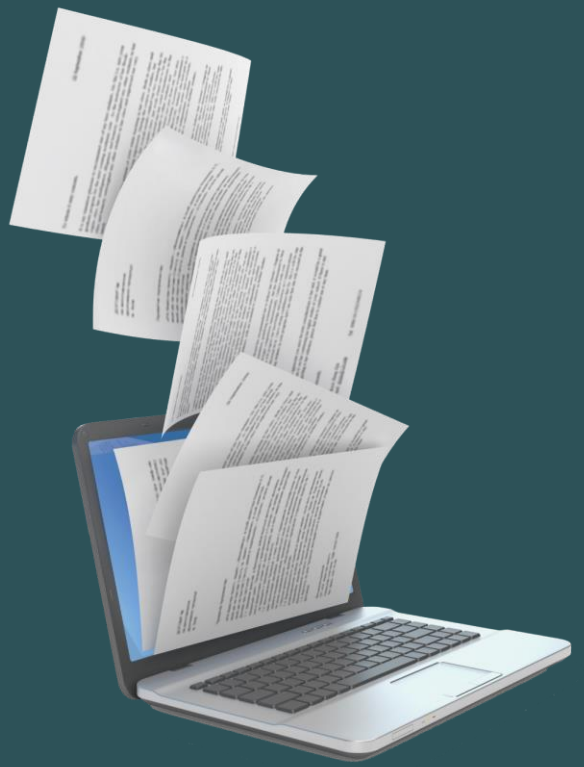
- Facoltà di Economia - Università La Sapienza
- ISFOL

Business Support Systems & Document Management

Case history di successo con oltre 100 Pubbliche Amministrazioni consentono a **DiGi ONE** di proporsi come partner nell'implementazione di infrastrutture complesse di gestione della documentazione, automazione dei procedimenti, integrazione con sistemi di CRM/ERP.

DiGi ONE offre da più di 20 anni le proprie soluzioni in ambito documentale a più di 100 Enti in Italia e più di 10.000 utenti utilizzatori. Tali soluzioni sono sempre state altamente innovative e dotate di un'ergonomia e facilità d'uso assoluta, includendo funzionalità avanzate con tutti gli strumenti necessari per la gestione dei protocolli e dei documenti secondo le ultime disposizioni normative.

In particolare, la suite **iShareDoc** è la piattaforma documentale di **DiGi ONE**, e rappresenta una soluzione di riferimento per tematiche di automazione documentale complesse.



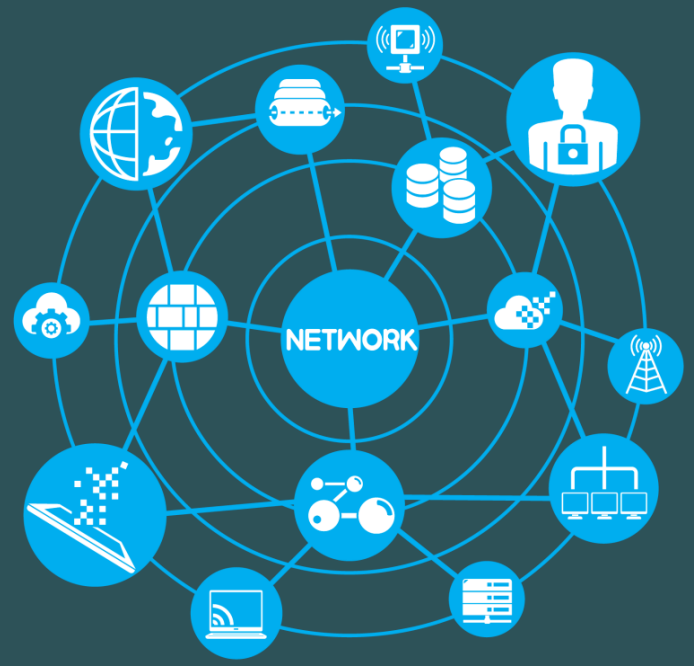
Big Data, Cloud, Cognitive Computing

In un mondo in rapida evoluzione, la grande mole di dati trova la sua naturale implementazione in infrastrutture informatiche distribuite e nell'impiego dell'intelligenza artificiale.

Tali sistemi possono essere resi disponibili su Cloud pubblici, privati o su infrastrutture ibride integrate e orchestrate da strumenti leader di mercato.

DiGi ONE vanta competenze peculiari nelle infrastrutture Cloud, ed è in grado di svolgere quanto segue:

- ✓ disegno ed implementazione di soluzioni IaaS basate su data center distribuiti geograficamente;
- ✓ disegno e realizzazione sistemi di Cloud Automation;
- ✓ disegno e realizzazione di soluzioni PaaS;
- ✓ disegno e realizzazione di soluzioni SaaS per posta elettronica e Social Collaboration;
- ✓ disegno ed implementazione di soluzioni basate su Cloud Ibridi.



Messaging & Collaboration

Le tecnologie di Comunicazioni Unificate & Collaborazione incentivano le aziende a sistemi di lavoro più flessibili e aperti a contesti produttivi diversi. **DiGi ONE** vanta un'esperienza pluriennale in questo settore per grandi realtà pubbliche e private ed è il partner ideale per affiancare le aziende nella progettazione di nuovi modelli di organizzazione del lavoro.

Video conferenza

Didattica ibrida

Condivisione cartelle

Mail, Webmail, chat aziendali

Condivisione contatti, mailbox, gruppi

Un "case history" particolarmente significativo riguarda la gestione di servizi IT e progetti a valore inerenti le piattaforme di Messaging & Collaboration del cliente **ESA – European Space Agency**: in tale contesto, abbiamo gestito:

- ❖ oltre 5000 utenti in Europa;
- ❖ oltre 2500 device mobili;
- ❖ 1 milione di email al mese;
- ❖ 300 ticket al mese.

Cyber Security

In un mondo sempre più integrato e connesso, in cui persone, cose e apparati produttivi interagiscono in maniera "intelligente", cresce in maniera esponenziale la necessità di sicurezza.

DiGi ONE propone un'offerta tecnologica basata sulle competenze e su vare soluzioni orientate sia in ambito di sicurezza IT, sia in ambito ibrido (IoT).

DiGi ONE è in grado di offrire competenze, soluzioni, servizi e prodotti per proteggere le aziende costantemente esposte al rischio di crimini informatici che possono avere impatti gravissimi: perdita di informazioni sensibili, interruzione dei processi di business, danni all'immagine pubblica dell'azienda, eccetera.

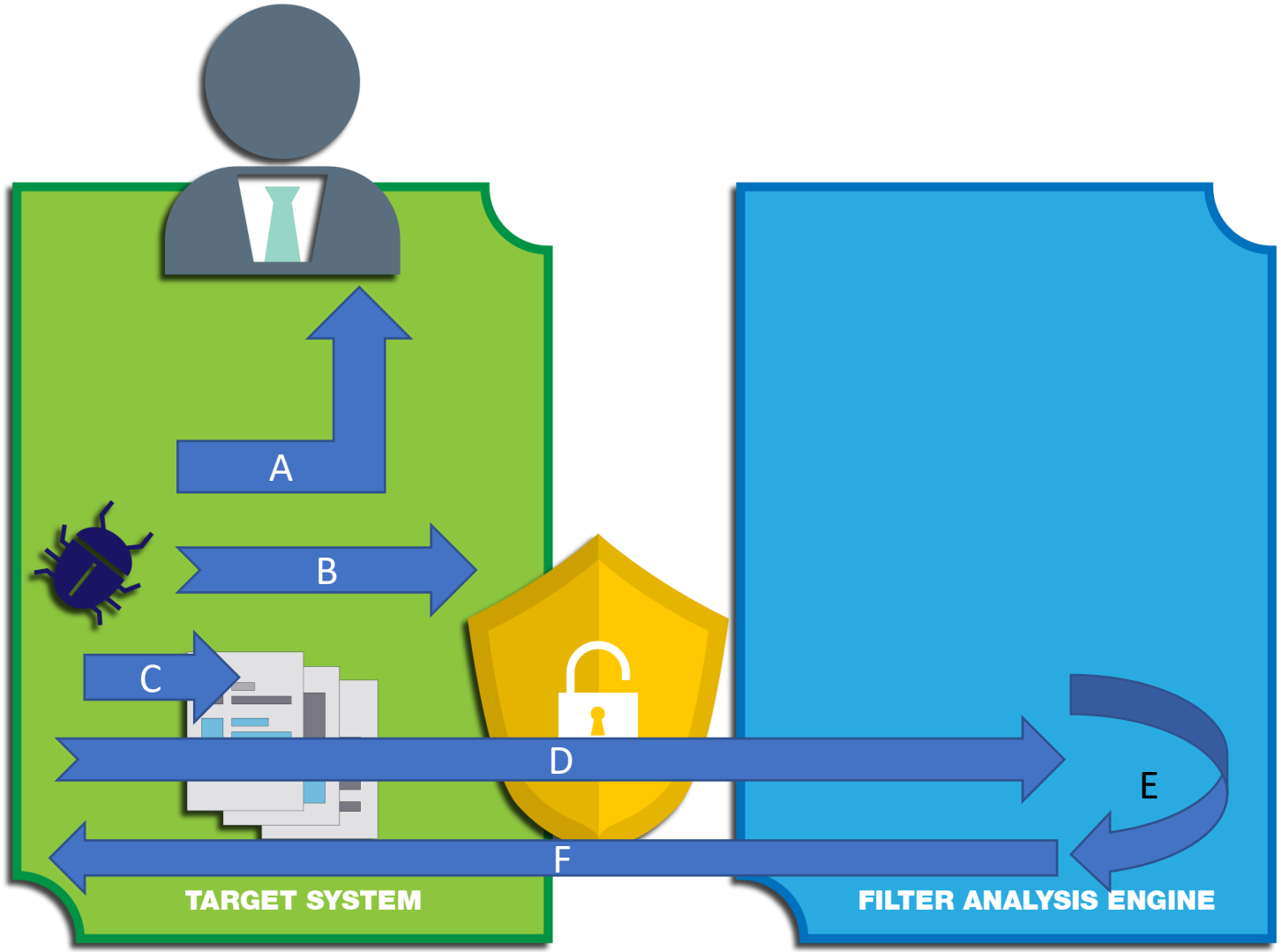
Filter AI

FILTER AI nasce allo scopo di esfiltrare informazioni potenzialmente utili da un sistema obiettivo in modo silenzioso.

La sua efficacia deriva dall'uso di tecniche di apprendimento che permettono di:

- modellare e **imitare il comportamento degli utenti** del sistema;
- **valutare ed eludere dinamicamente le contromisure di sicurezza;**
- **escludere informazioni** che siano state disseminate allo scopo di **depistare;**
- **individuare** eventuali meccanismi di intercettazione basati su **honeypot;**
- **riconfigurare dinamicamente i parametri di ricerca** in modo da dare precedenza ai documenti pertinenti.

Filter AI



- **PHASE A** – User's behaviour mapping
- **PHASE B** – Security perimeter mapping
- **PHASE C** – Data gathering
- **PHASE D** – Exfiltration
- **PHASE E** – Data analysis
- **PHASE F** – Dynamic configuration

Filter AI

PHASE A – User's behaviour mapping

Inizialmente, l'agente software presente sul sistema target effettua una acquisizione dati sul comportamento dell'utente.

Crea una mappa con le fasce orarie di utilizzo, le attività che l'utente effettua e il tipo di traffico di rete che genera.

In questo modo viene definito un modello che sarà utilizzato per dissimulare l'attività dell'agente, emulando il comportamento dell'utente.

Anche la temporizzazione delle attività cicliche è gestita in modo da introdurre ritardi casuali per non avere sequenze troppo serrate che potrebbero far scattare allarmi da parte dei sistemi di sicurezza.

PHASE B – Security perimeter mapping

Prima di iniziare il ciclo principale, l'agente software presente sul sistema target effettua una acquisizione dati sul software di sicurezza presente.

Grazie a questo riesce a individuare, tra le attività previste, quelle «rischiose» per escluderle dall'operatività.

Inoltre può individuare i canali di comunicazione bloccati, tra quelli previsti, e riconfigurarsi per usare quelli disponibili.

PHASE C – Data gathering

L'agente software effettua una scansione del sistema target per individuare i dati di interesse.

Nel farlo, determina la priorità con cui effettuare l'esfiltrazione. La priorità è basata sulla presenza di parole chiave.

Questo si rende necessario per gestire prudentemente le risorse (memoria disponibile, banda disponibile, potenza di calcolo residua).

Quindi i dati considerati più utili verranno considerati prioritari, nell'evenienza che il canale a un certo punto non sia più disponibile o che l'agente venga individuato e rimosso.

PHASE D – Exfiltration

L'agente software trasferisce all'esterno i dati raccolti.

Nel farlo utilizza le informazioni sulle priorità stabilite nella fase C (*Data gathering*), attraverso il canali e gli strumenti valutati nella fase B (*Security perimeter mapping*), usando il comportamento modellato nella fase A (*User's behaviour mapping*).

Ad esempio:

- sarà gestito per primo il PDF contenente le parole chiave ritenute prioritarie;
- sarà trasferito tramite HTTP perché il canale SMTP non è disponibile;
- sarà suddiviso in blocchi e spedito a intervalli casuali nelle fasce orarie in cui tipicamente il sistema è usato.

PHASE E – Data analysis

I dati trasmessi alla piattaforma FILTER vengono analizzati da un motore in grado di individuare correlazioni tra documenti diversi e stabilire nuovi schemi.

Il risultato di questa elaborazione permette di:

- segnalare eventuali documenti che presentino anomalie nei metadati che possono far sospettare che si tratti di informazioni predisposte ad arte per depistare gli attaccanti;
- evidenziare nuovi potenziali centri di attenzione e parole chiave.

PHASE F – Dynamic configuration

Il risultato dell'analisi di FILTER (effettuata tramite motori logico-semantici) permette di cambiare la configurazione dell'agente software installato presso il sistema target.

Con un meccanismo di retroazione la nuova configurazione viene usata dall'agente per ricalibrare le priorità.

DiGi ONE
the leading digital company

CONTACT US

info@digi-one.eu | marketing@digi-one.eu

Follow us

www.digi-one.eu

Filter AI

Polymorphism

Lo stealth process crea diversi cloni di sé stesso, introducendo in ciascuno delle differenze morfologiche basate sul concetto per cui ci sono diversi modi di eseguire la stessa azione; questa tecnica impedisce il rilevamento basato sulla ricerca di "firme"; di questa strategia fa parte anche il ricorso ai Domain Generation Algorithm (DGA), che calcola in maniera dinamica le coordinate del server C&C; questa modifica incrementa la difficoltà di bloccare il traffico associato al processo stealth.

Behavior change

Lo stealth process ha due modalità operative, una sicura e l'altra non sicura; la modalità sicura è attiva quando viene rilevato un processo di scansione da parte di software antimalware o antivirus che potrebbe far scattare allarmi in presenza di operazioni sospette; appena il processo di scansione termina, lo stealth process riattiva la modalità non sicura.

Filter AI

Environmental awareness

Analisi del comportamento dell'ambiente in cui lo stealth process si trova a operare (es. si tratta di un host fisico o virtuale); i dati raccolti da questa scansione permettono di adeguare il comportamento e portare attacchi mirati.

Timing-based evasion

Le operazioni aggressive vengono pianificate in finestre temporali prefissate (intervallo di date, oppure orari) o legate ad eventi generati dall'utente (clic su un elemento dell'interfaccia, riavvio).

Obfuscating Internal Data

Lo stealth process utilizza una serie di tecniche per far girare codice che non può essere rilevato: sostituzione dei nomi delle API con valori codificati tramite hash, utilizzo di una tabella di esclusione che impedisce ad alcuni processi di effettuare il parsing, comunicazione con il server C&C attraverso la porta 443 che gestisce il traffico cifrato.

Altre tecniche prevedono di creare file eseguibili che si mascherano tra i file di sistema.

Filter AI

Per raggiungere l'obiettivo, lo stealth process deve usare una combinazione delle tecniche disponibili, in modo da rendere sempre più complessa l'individuazione da parte di tool di sicurezza che stanno crescendo costantemente per fare fronte alle nuove tecniche di mimetizzazione del software aggressivo.