itetica

Without frills

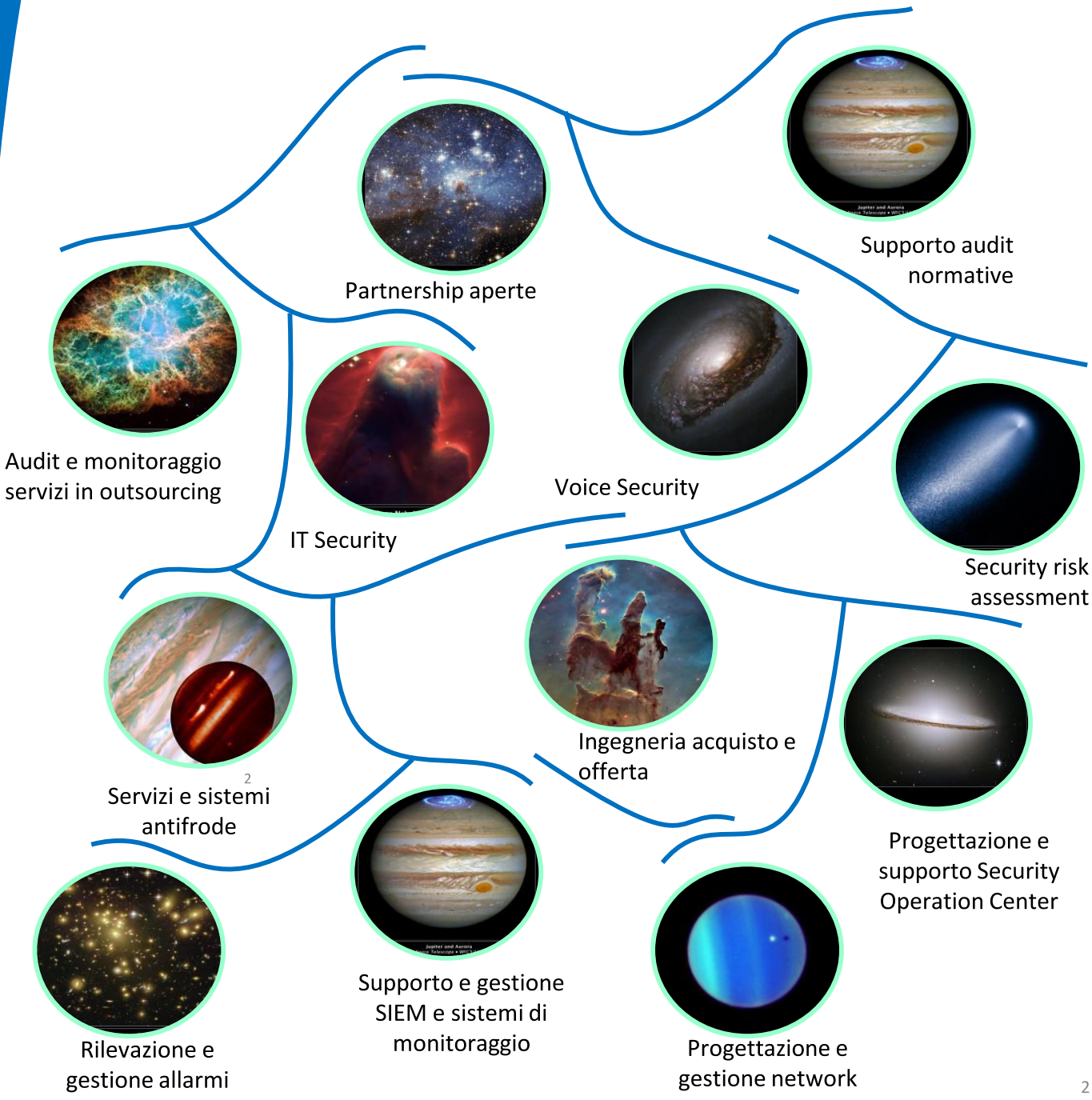
itetica S.r.l.
Piazza Giorgio La Pira 27/A
43123 Parma
email: contact@itetica.it
Telefono: +39-0521-1856293
Fax: +39-0521-1854789
www.itetica.it

itetica nasce dall'esperienza di professionisti IT che si sono riuniti per condividere non solo le proprie esperienze e competenze, ma anche quelle di altre realtà di eccellenza, al fine di garantire ai propri partner il successo nei propri obbiettivi in termini di utilità, efficienza e sostenibilità.

Il raggiungimento degli obbiettivi è primario, ma per noi è fondamentale come portarlo a termine.

Vogliamo lavorare secondo principi di trasparenza, sostenibilità, empatia ed essenzialità, sviluppo del territorio, e promuoviamo progetti in cui successo sia misurabile e garantito da risultati oggettivi.

I NOSTRI AMBITI DI ATTIVITA'



SUPPORTO AUDIT NORMATIVE

Tutte le aziende devono o dovranno soddisfare requisiti di normative riguardo a trattamenti di dati (Garante Privacy, ISO 27001, SOX, PCI, Dossier Sanitario Elettronico, normative di settore, conformità a compliance clienti).

- Come sodisfare i requisiti?
- Come mantenere l'azienda compliant senza costosi interventi pre-audit?
- Sono già presenti anche se non utilizzati strumenti e/o procedure necessarie?
- Come mantenere aggiornati processi e tecnologie rispetto ad evoluzioni tecnologiche o normative?
- Come integrare i processi con altri presenti o necessari senza inutili aggravi di costi?
- Sono possibili economie di scala per essere rispondenti a più normative?

PARTNERSHIP APERTE

Grandi e piccoli system integrator e società di consulenza distribuiscono tecnologie, competenze e servizi di terzi.
Questo vale anche per i grandi vendor, per ragioni di flessibilità o per completare la propria offerta.
Non sempre la selezione dei fornitori avviene sulla base delle reali esigenze progettuali, spesso è dettata da valutazioni di tipo economico, da vincoli contrattuali, da semplice comodità o consuetudine.

- Quanto viene proposto è stato valutato come ottimale tra altre soluzioni?
- La diffusione di un brand e quadranti magici richiedono costi. Gli aggravi economici indiretti sono indispensabili per il conseguimento degli obiettivi?
- Altri fornitori consigliati possono soddisfare in modo migliore le esigenze progettuali?

AUDIT E MONITORAGGIO SERVIZI IN OUTSOURCING

La percentuale delle aziende che ricorre a servizi in outsourcing è assimilabile a quella delle aziende che utilizzano servizi in cloud. Nonostante si tratti sempre di esternalizzazione di processi o tecnologie, l'attenzione ad aspetti di sicurezza, compliance, e performance viene quasi esclusivamente dedicata al mondo cloud.
Riguardo a servizi in outsourcing:

- L'erogazione è adeguatamente monitorata?
- Le prestazioni e i processi sono migliorabili?
- Gli impegni contrattuali sono rispettati e rivisti periodicamente rispetto alle performance?
- Nell'ambito dell'erogazione dei servizi sono rispettati vincoli e normative vigenti?
- Si dispongono delle informazioni necessarie per poter rinegoziare efficacemente i contratti o per valutare fornitori alternativi?

VOICE SECURITY

Gran parte delle informazioni è trasmessa per via telefonica, quindi molteplici frodi possono essere effettuate utilizzando i sistemi voce (furto di informazioni, autenticazioni, acquisti…). Mentre i canali di comunicazione dati sono in generale oggetto di verifica di comportamenti e pattern anomali, i canali di comunicazione voce spesso non sono presidiati in tal senso.

- Sono presenti modem non autorizzati che bypassano le misure di sicurezza interne e perimetrali?
- Si verificano chiamate non autorizzate da parte di personale interno e/o esterno?
- Vengono rilevati comportamenti anomali nei pattern di voce?
- Vengono monitorati attacchi voce indirizzati al furto di informazioni?

IT SECURITY E PROGETTAZIONE E GESTIONE NETWORK

La remunerativitá dei progetti di networking e security negli ultimi anni è diminuita fortemente, e con questa gli investimenti in ricerca e formazione.
Il numero di attori attivi in progetti di network e security si è invece moltiplicato, sia per la sempre maggiore sensibilizzazione su problematiche di sicurezza sia per la larga diffusione di tecnologie, in periodico rinnovamento.

- L'approccio progettuale è corretto nella valutazione degli obiettivi?
- Le attività sono correttamente progettate e adeguatamente documentate?
- Le competenze del fornitore sono esclusivamente tecnologiche?
- Viene garantito un adeguato supporto post vendita?

SECURITY RISK ASSESSMENT

Una verifica dello stato di sicurezza può essere necessario per motivi normativi, procedurali o contingenti e può interessare applicazioni web o mobile, perimetri network, ambienti wireless…
In ogni caso oltre all'aspetto esecutivo è fondamentale la capacità di analizzare processi e architetture anche applicative in modo che eventuali correzioni da apportare siano necessarie ed efficaci.

- Quali sono le migliori modalità di valutazione rispetto agli obiettivi dell'assessment (operational risk, compliance risk, information security risk…)?
- Le informazioni ottenute sono utilizzabili efficacemente per migliorare e soddisfano gli obiettivi del test?
- Le modalità di analisi sono ripetibili?
- I risultati sono confrontabili con precedenti o successivi?

INGEGNERIA DI ACQUISTO E OFFERTA

Per le peculiarità dei prodotti e dei servizi offerti nel mondo IT è spesso difficile reperire e confrontare listini e contratti consolidati.
Inoltre motivi organizzativi e procedurali o economici spesso non consentono di comporre nei tempi necessari le competenze tecniche, di mercato, contrattuali indispensabili per costruire corrette richieste di acquisto o di offerta.

- I requisiti di richiesta o di offerta soddisfano le esigenze progettuali?
- Si dispone di adeguati benchmark?
- Si desidera conoscere l'offerta di altri potenziali fornitori qualificati?
- Esistono case history per progetti analoghi o per esigenze simili?
- Gli SLA contrattuali proposti sono coerenti e potenzialmente erogabili?

SERVIZI E SISTEMI ANTIFRODE

Molte tipologie di frodi informatiche sono poco conosciute, sia perché non coinvolgono massivamente importanti volumi di dati o di denaro, sia perché si tratta di azioni non condotte con malware, virus o comunque con strumenti concepiti per effettuare azioni malevole.
Esistono anche attacchi portati con azioni tecnicamente lecite, quindi difficilmente rilevabili con strumenti commerciali, nei quali qualcuno cerca di assumere identità simile a quella di altri.

- Qualcuno cerca di registrare o registra domini con nomi ingannevoli e simili ad esistenti?
- Sui social network esistono profili simili ai nostri?
- Sono in vendita servizi o prodotti con marchio senza autorizzazione?
- Sono scaricabili app ingannevoli?
- Siamo oggetto di campagne di phishing?

PROGETTAZIONE E SUPPORTO SECURITY OPERATION CENTER

La centralizzazione del monitoraggio della sicurezza può essere gestita internamente, essere esternalizzata, avere più o meno profondità, basarsi su infrastrutture proprietarie o open source. Eventuali requisiti obbligatori a parte, non esiste un modello di SOC, ma strutture e processi concepiti per ottimizzare diverse esigenze aziendali.

- Quali sono le priorità di sicurezza rispetto alle singole peculiarità aziendali?
- Le tecnologie e i processi sono ottimizzati rispetto agli obiettivi?
- Possono essere integrati altri servizi di monitoraggio (asset management, compliance normative, monitoraggio sistemistico, sicurezza fisica…)?
- Le performance sono costantemente oggetto di valutazione?

SUPPORTO E GESTIONE SIEM E SISTEMI DI MONITORAGGIO

I sistemi di monitoraggio e di Security Information Event Management sono concepiti per facilitare le attività di monitoraggio di sicurezza e disponibilità, di raccolta e gestione di eventi rilevanti per la sicurezza. Oltre a soluzioni proprietarie ed open source, spesso SW e dispositivi HW prevedono la disponibilità di sistemi di questo tipo o possono essere integrati con essi. Frequentemente si tratta di soluzioni sotto utilizzate e poco aggiornate.

- Come possono essere gestite le variazioni di perimetro?
- Regole di correlazione, database, black list… sono aggiornate e oggetto di periodiche revisioni?
- Sono già presenti sistemi utilizzabili per la raccolta e il monitoraggio degli eventi?

RILEVAZIONE E GESTIONE ALLARMI

Nella generalità dei casi ogni ambiente, IT, SCADA, sicurezza fisica, asset management…) ha sistemi dedicati di rilevazione di allarmi o di eventi significativi.

- Vengono presi in considerazione tutte le informazioni che gli oggetti del perimetro di attenzione possono potenzialmente segnalare?
- Sono oggetto di attenzione situazioni collegate ad eventi correlati e non solo ai singoli?
- Sono possibili utili integrazioni tra segnalazioni provenienti da ambienti eterogenei presenti in azienda?
- Gli allarmi generati sono concepiti in modo efficace rispetto alla realtà e alle esigenze ?
- Sono continuamente o periodicamente riviste le regole di correlazione e allarmistica sulla base delle esigenze organizzative e di business?

itetica S.r.l.
Piazza Giorgio La Pira 27/A
43123 Parma
P.IVA e Cod. Fisc. 02695280343
email: contact@itetica.it
Telefono: +39-0521-1856293
Fax: +39-0521-1854789
www.itetica.it