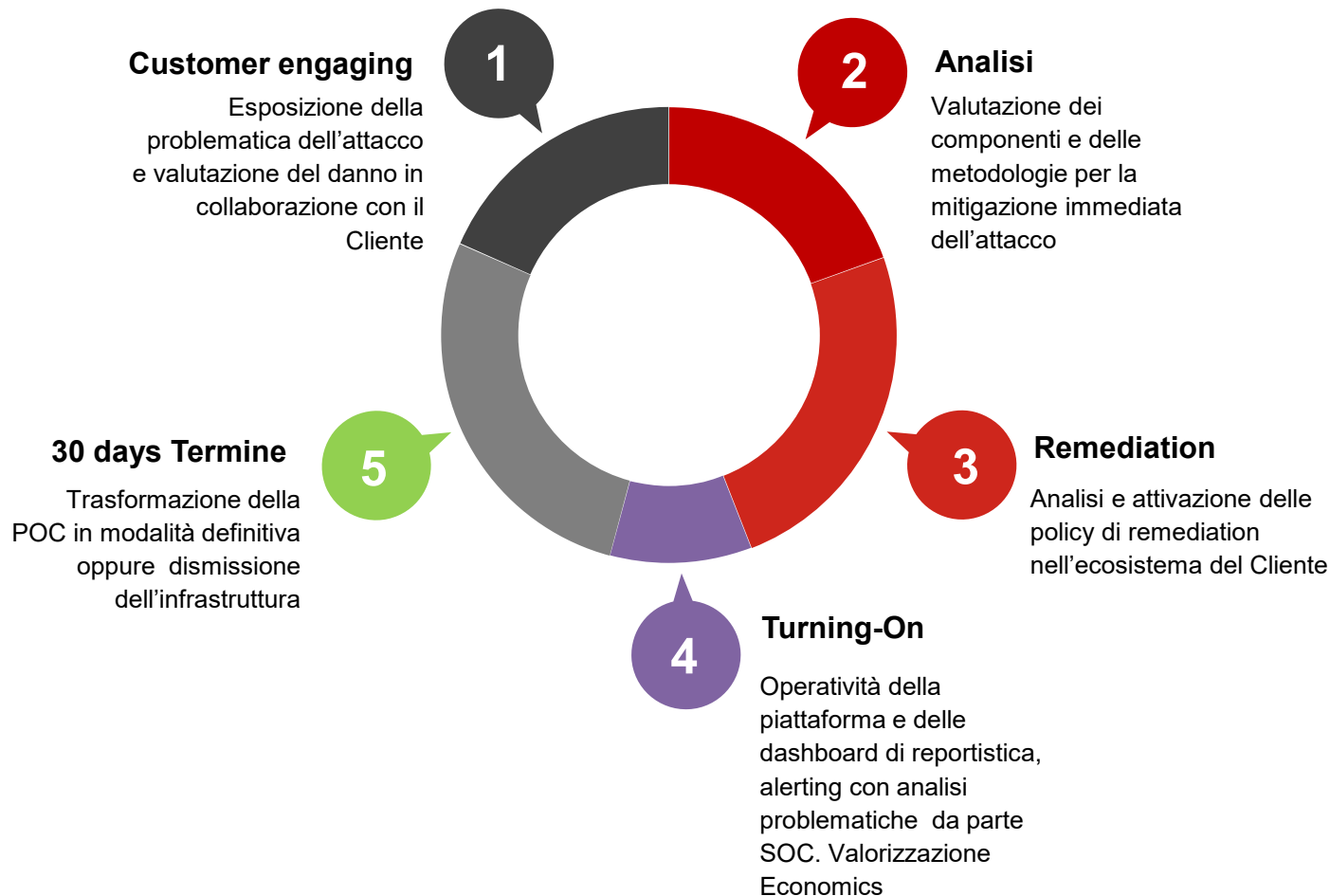




CORTEX 911
Ogni chiamata conta.
Ogni secondo conta.







Come funziona la campagna 911 ?

- Analizziamo con il Cliente la situazione dell'attacco in corso
- Verifichiamo il to-do insieme al Team Palo Alto
- Pianifichiamo con il Cliente i next-step operativi e requirements
- Installiamo il prodotto Cortex XDR da Remoto sul Site del Cliente
- Abilitiamo la dashboard di monitoring
- Analizziamo con il SOC le problematiche esistenti
- Applichiamo le eventuali policy di remediation & contenimento
- Lasciamo la piattaforma operativa al Cliente per 30 giorni fornendo gli economics per la decisione finale di acquisto o dismissione

Per 30 Giorni avrai la piattaforma pienamente funzionante.

Potrai decidere se acquistare la soluzione ed i servizi oppure disinstallare il prodotto.

CORTEX 911: Perché

INCIDENT

Un evento di sicurezza che compromette l'integrità, la riservatezza o la disponibilità delle informazioni

BREACH

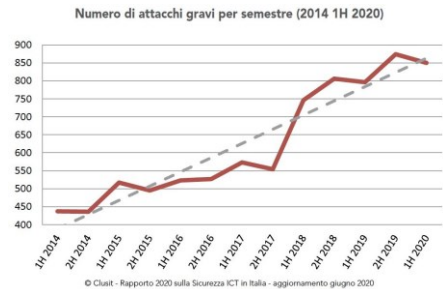
Un incident che conferma la divulgazione, quindi non la potenziale esposizione, di dati ad un soggetto non autorizzato

1 Nel 2020 in Italia circa 2.000 attacchi gravi, vs 1.670 del 2019 e 1.522 del 2018. In media 160 attacchi gravi al mese.

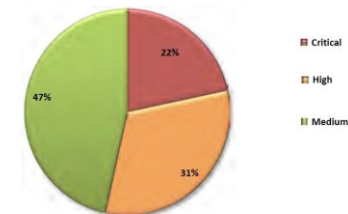
2 Non tutte le aziende sono preparate a rispondere a cyber attacchi complessi

3 Anche i team di Incident Response più efficienti hanno spesso difficoltà nel Contestualizzare le informazioni

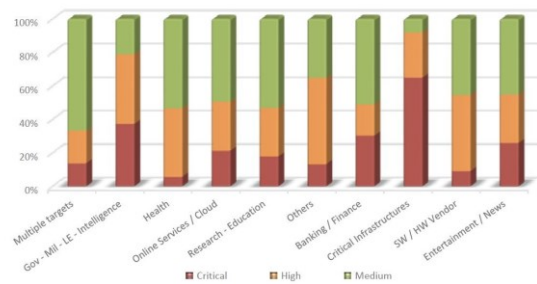
4 Grazie all'integrazione tra CORTEX e le skill dei partner, PANW ha l'obiettivo di rispondere a questi attacchi in pochi minuti.



Tipologia e distribuzione % Severity (1H 2020)



Distribuzione % Severity per 10 target più colpiti (1H 2020)



CORTEX 911: Cos'è



XDR



**Incident
Response
Team**



**Managed
Threat
Hunting**

- **Endpoint Protection +EDR +Threat Intel +Remediation :**
 - Cortex XDR per Endpoints w/Host-Insights
 - Cortex XDR for TB (Analytics PANW e 3rd party)
 - Autofocus
 - XSOAR (inc. TIM) con playbooks pre costruiti per velocizzare Investigation e Remediation
 - Expanse - Expander attack surface viewer
 - Package nel MarketPlace per integrare rapidamente XSOAR e XDR
- **Servizi:**
 - Partner Incident Response Team (CSIRT).
 - Cortex Managed Threat Hunting.
 - 24/7 threat hunting powered by Cortex XDR e dalla Unit 42 (by Palo Alto Networks)
 - Supporto ai team I&R dei Partner per individuare le minacce evasive
 - Cypsis Emergency Response Team - Opzionale
- **Durata:** 30 giorni

CORTEX 911: Inumeri fino ad ora

Cortex 911SERVICES

XDR PRO

NTA +AF +MTH

On top XSOAR

14 Breaches

In Q2

3 Paesi

Attualmente coinvolti nel programma (tra cui l'Italia)

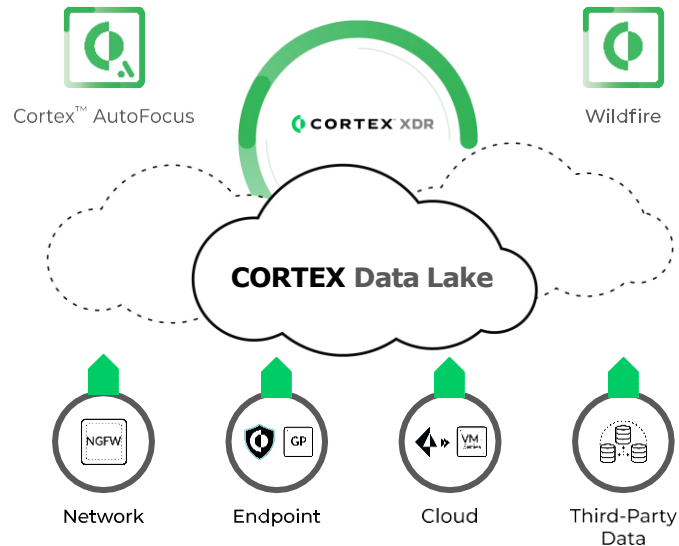
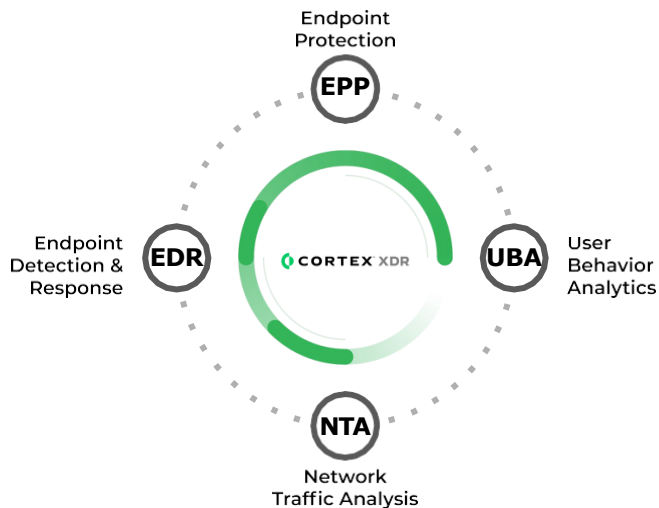
\$2.5 Millions

Di pipeline generata

\$1M+

di bookings a Dic20.
\$500k in pipe per Feb21

CORTEX 911: Quick reminder



La piattaforma **Cortex XDR** permette la gestione **centralizzata** di **prevention, detection, investigation** e **response** con l'obiettivo di **automatizzare** e **semplificare** le **operations**.

Cortex XDR è la piattaforma PANW di **extended detection** e **response** che integra i **dati endpoint, network** e **cloud** – **riducendo il rumore** e **focalizzandosi** sulle **reali minacce**.

CORTEX 911:XSOAR per la collaborazione e l'orchestrazione dell'IR

Un tenant XSOAR (o Co-Managed Tenant) dove:

- Cliente (Vittima), Partner (IR lead) e Distri (Supporto) possono **collaborare, condividere info e intelligence, prendere decisioni** per tutta la durata dell'incidente grazie alla War Room (web interface e mobile App)
- Partner (IR lead) può utilizzare dei playbook per automatizzare dei processi di Response:
 - (Un)isolate endpoints
 - Quarantine / Restore files
 - File Search & Destroy (Hashes, File Paths)
 - Block processes / file hashes
 - Retrieve files with File Paths or Hashes
 - Query XDR data (IP, Domain, File Hash, etc.)
 - Push IOCs from XSOAR into XDR
 - Run script
 - Endpoint Management
- Dashboards & Reports (Breach timer, Nb of XDR Incidents Open / Solved, etc.)

CORTEX 911: **Expense** e la visibilità della **Superficie d'Attacco**



Superficie d'Attacco

CORTEX 911: **Expense** e Use Case utili per gestire un breach



Manage Attack Surface

Organizzazione, aggiornamento e gestione automatica degli Asset Internet



Infrastructure Overwatch

Monitoraggio della security in ambienti segregati



Cloud Security

Gestione del Cloud e enforcement centrale delle policy



Compliance

Identificazione di asset esposti e non in linea con i requisiti di compliance (NIST, PCI)



Third Party Due Diligence

Identificazione dei rischi indotti dalle relazioni con fornitori ed aziende oggetto di M&A

Utilizzo di report per identificare ed indirizzare asset a rischi e flussi malevoli

Cortex 911- Flusso del Processo di Emergenza (Semplificato)

T0

T0 +5 min

T0 +30 min

T0 +40min

Cliente Attaccato

Chiamata o Mail al Cortex 911

Team di
Risposta alla
Chiamata/Mail

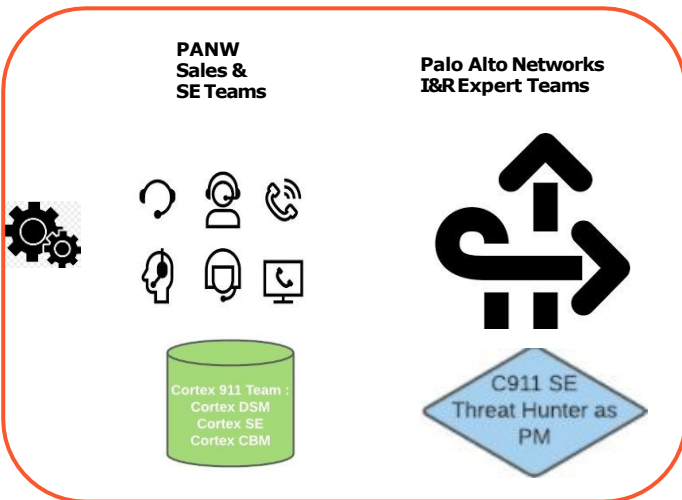
Attivazione del
Team di
Gestione

Attivazione e
Integrazione
Tecnologica

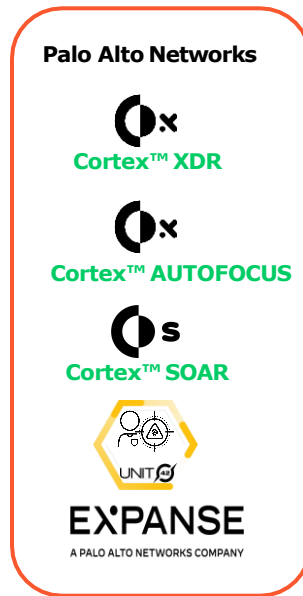
Team di Cyber
Response



Form dedicato
per ogni
Partner C911



Il nostro team Cortex 911 riceve le chiamate/mail di emergenza, crea l'opportunità in SFDC e genera le EVAL per il partner che gestirà la cyberemergenza



Partners/Csirt



Partner 1



Partner 2








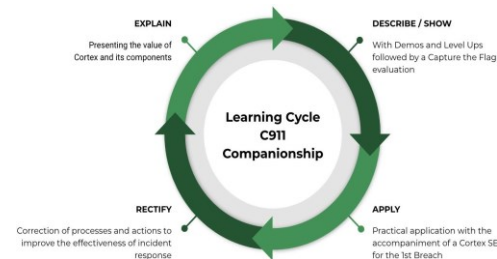
Partner 3



Partner 4

Cortex 911- Partner Onboarding Plan

		Lead by	STANDARD RESOURCE	DEDICATED RESOURCE
			Cortex Local Resources	Cortex 911Team
	Individuazione dei Partner C911	SOC Operator Cert & Csirt Service MDR & XSOAR Partner	● ● ●	
	Knowledge Transfer	Meeting di Qualificazione Cortex Knowledge Transfer Partecipazione al Capture the Flag Creazione Form C911 dedicato al partner	● ● ● ●	
	Guida Costante	Cortex SE assegnato al Partner C911 Follow up del Cortex CBM SEUR Lista Risorse del Partner per i Level UP Consegna del badge CORTEX 911	● ● ● ●	● ● ●
	Fare Esperienza	1° Breach gestito insieme a 4 mani Debrief dopo il 1°Breach Bug Fixing se qualcosa non ha funzionato	● ● ●	● ●
	100% Autonomi	Il Partner 911 si muove in autonomia Assistenza per l'offerta commerciale	●	●



Benefici della Partnership

Guida Costante

- 1 Promozione dello sharing del know-how grazie agli SE CORTEX

Transfer delle best practice

- 2 Creation of a club / Community of 911 partners to share experiences

Riflettori su Cortex

- 3 Possibilità di sfruttare il full pot ential di CORTEX

THANKS