CLAROTY

COMPANIA Aquaserv Târgu-Mureș

Studiu de caz – soluție integrată de protecție cibernetică și acces securizat de la distanță

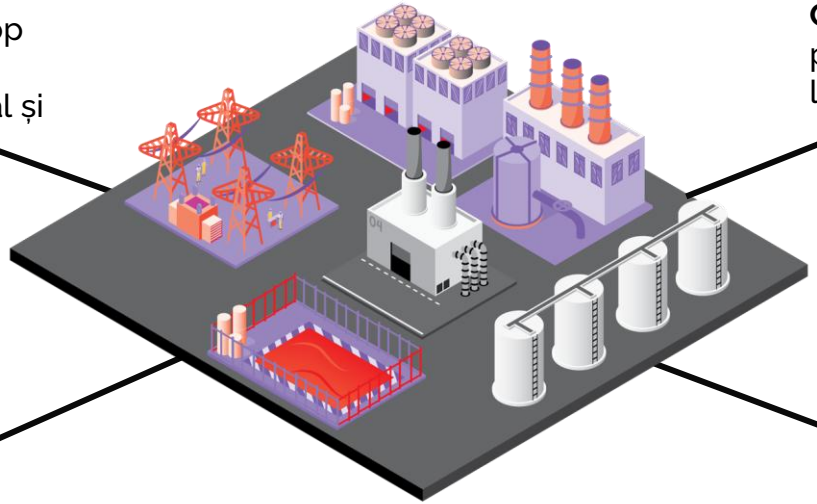
Partenerii

Claroty

Producător mondial de top de soluții de securitate pentru domeniul industrial și al sănătății

COMPANIA Aquaserv Târgu-Mureș

Client - operator în domeniul apei potabile şi al apelor uzate pe o arie lărgită de operare



Accurate Business

Reprezentant exclusiv al Claroty în România

Cancom

Partener – a realizat implementarea cu succes a proiectului la sediul central și 4 locații la distanță

Soluțiile implementate

Continuous Threat Detection (CTD)

Soluție de tip “on-premise” destinată protecției cibernetice a sistemelor de control industrial, care monitorizează și expune în mod nativ un inventar complet al dispozitivelor clientului, generează harta riscului pentru fiecare locație industrială și alertează în timp real asupra amenințărilor

xDome Secure Access

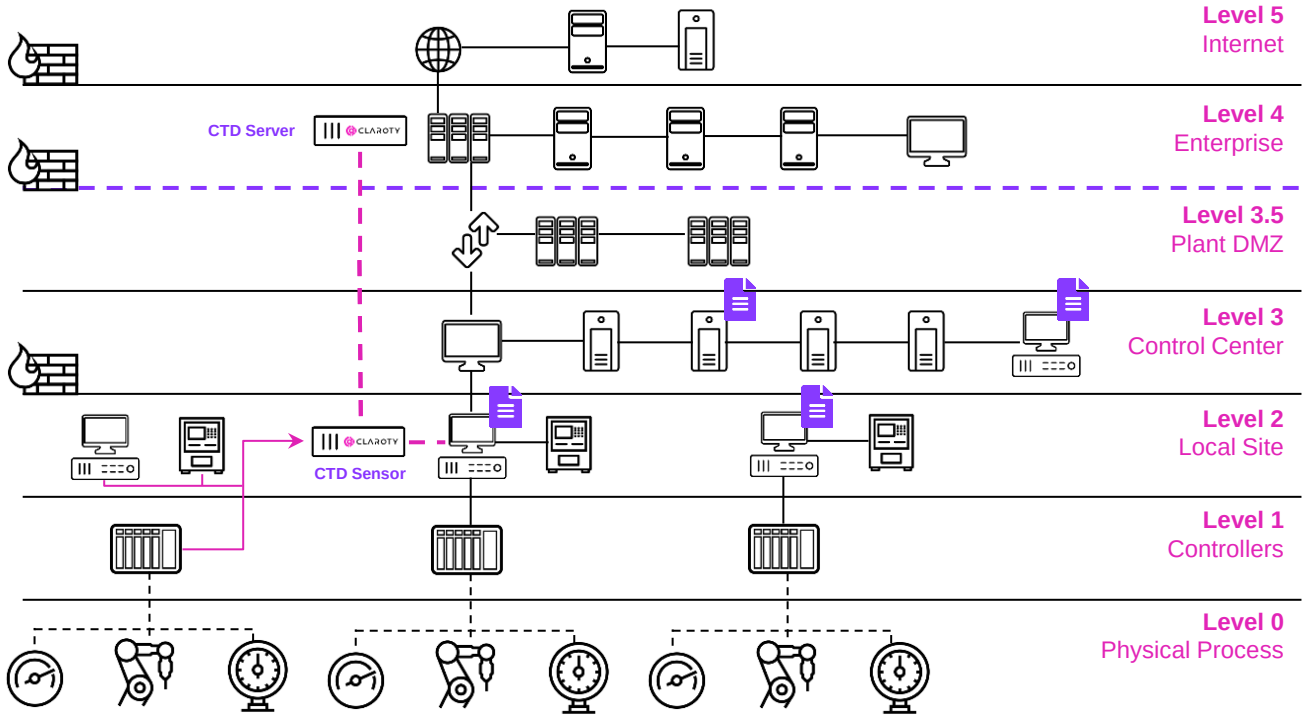
Soluție de acces securizat de la distanță, destinată în mod specific rețelelor de control industrial și optimizată pentru a reduce complexitatea conectării, nivelul de risc și a permite un mod de control și audit foarte granular. Integrată nativ cu CTD

Arhitectura Claroty CTD

Componentele platformei CTD:

- **CTD Server:** Localizat de obicei în rețeaua IT a organizației, în general în DMZ, elementul central al soluției

- **CTD Sensors:** Dispuși în diferite locații, la nivele inferioare Purdue, pentru a colecta copia traficului relevant din rețelele industriale monitorizate – procesează parțial și transmit către CTD Server informațiile ce se expun în interfața grafică a acestuia

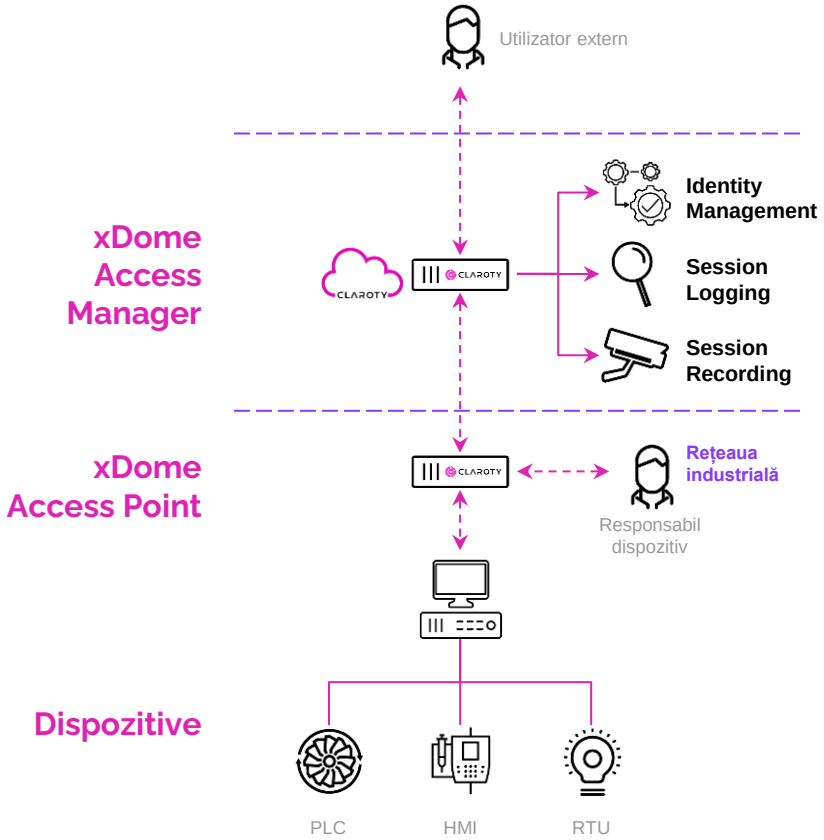


CLAROTY

Integrarea cu soluția de acces securizat – SRA (xDome Secure Access)

xDome Secure Access funcționează prin segmentarea accesului utilizatorilor în mai multe stadii, aplicând principiile de tip ZeroTrust la politicile de acces

- **xDome Access Manager – fostul SRA SAC:** localizat de asemenea în DMZ, Access Manager furnizează o interfață unică de configurare și de "portal" de conectare a utilizatorilor externi
- **xDome Local Access Point – fostul SRA Site:** dispuse în rețeaua operațională, sunt elementele prin care se realizează efectiv conexiunea către dispozitivele interne



CLAROTY

Componentele soluției - detalii

	CTD	SRA (xDome Secure Access)
	Implementare integrală în mediu virtual (VMware) – toate componentele	Implementare integrală în mediu virtual (VMware) – toate componentele
	1 buc. **CTD Server** la sediul central – Târgu-Mureș	1 buc. **SRA SAC** (xDome Access Manager) la sediul central – Târgu-Mureș
	4 buc. **CTD Senzori**: • Sediul central – HQ SCADA • Stație tratare apă potabilă Tg-M • Stație de epurare Cristești -Tg-M • Stație tratare apă potabilă și stație de epurare Reghin	5 buc. **SRA Site** (xDome Access Points): • Sediul central – clădire principală • Sediul central –HQ SCADA • Stație tratare apă potabilă Tg-M • Stație de epurare Cristești -Tg-M • Stație tratare apă potabilă și stație de epurare Reghin
		
	Integrare operațională cu SIEM/SOC24 și soluția de acces la distanță	Integrare nativă cu soluția CTD
	Scalabilitate pentru zeci de locații adiționale, cu suport pentru mii de dispozitive	Scalabilitate acces până la 30 de locații la distanță

CLAROTY

Exemple beneficii concrete

CTD

Sistemul CTD împreună cu SIEM a detectat pornirea unei aplicații tip RDP pe un server SCADA.

A fost alertat prin SOC24 echipa CSIRT/OT AQUASERV fiind o activitate nepermisă
Serverul este izolat de restul rețelei.

La fața locului s-a constatat următoarele:

- Contul de Guest nu a fost dezactivat și nici parolat
- Un soft tip RDP (cu multiple vulnerabilități) care era folosit de dezvoltatorul sistemului SCADA nu a fost dezinstalat și s-a activat automat cu pornirea utilizatorului Guest
- S-au luat măsurile necesare pentru securizarea accesului la servere.

SRA (xDome Secure Access)

Unul dintre Antreprenori are suspiciunea că subantreprenorul raportează/facturează mult mai multe ore lucrate cât este de fapt în realitate.

Cu soluția Claroty SRA s-a constatat că subantreprenorul era logat pe sistemele SCADA ore întregi conform raportării/ facturii

Verificând înregistrările video a sesiunii (captura ecran) s-a constatat că lucrul efectiv era max. 20 min./sesiune (2-3 ore).

CLAROTY

Mulțumim

CLAROTY