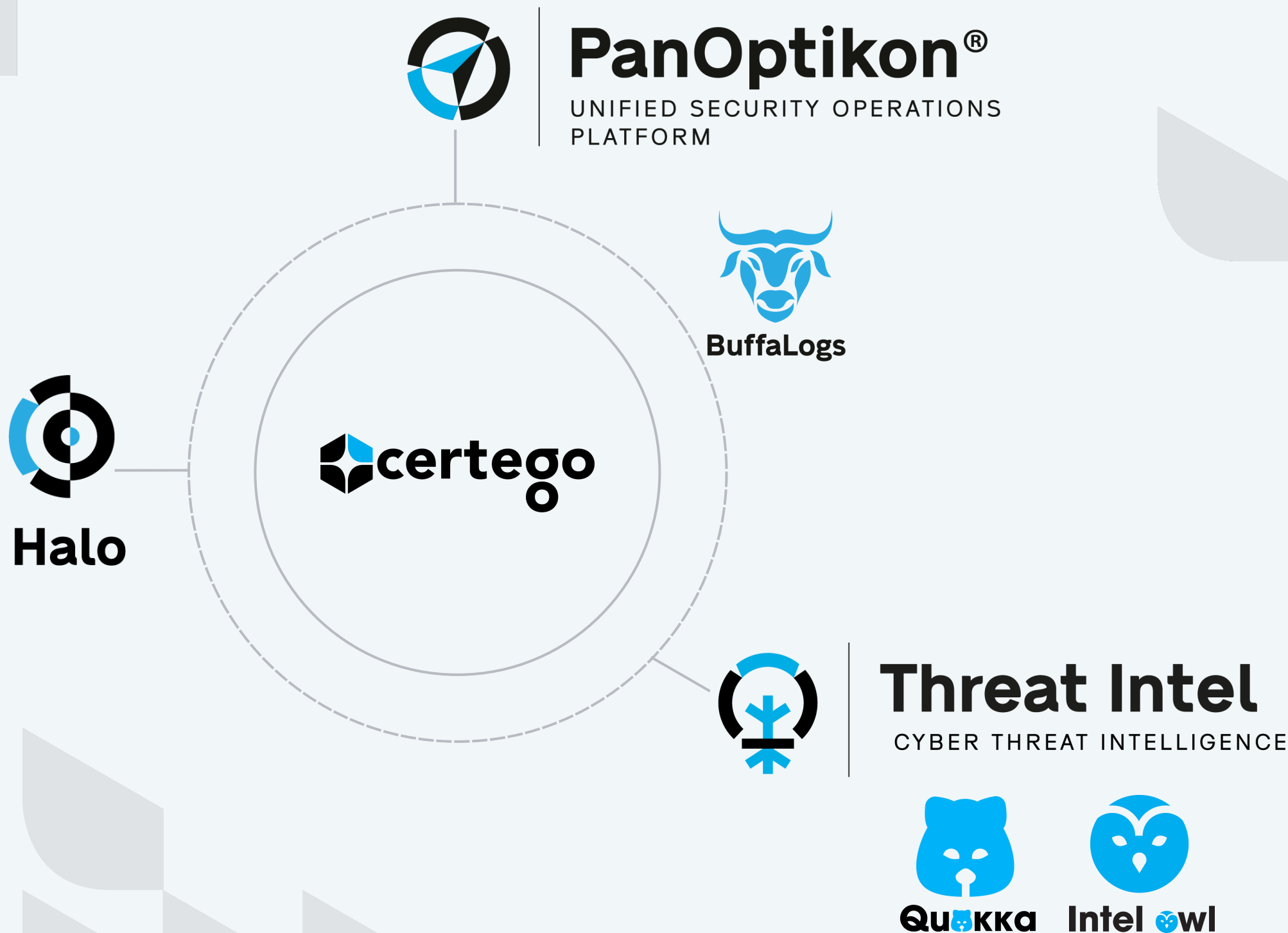


Ecosistema applicativo Certego



1 Soluzioni su misura per Power User

Ogni componente è progettato per le **esigenze** e i **flussi di lavoro avanzati** dei nostri analisti.

2 Nessun vincolo di terze parti

Totale controllo dell'architettura;
Nessuna dipendenza da roadmap di sviluppo esterne.

3 Innovazione più veloce e continua

Aggiornamenti costanti basati sull'**evoluzione delle minacce** e sulle mutevoli esigenze di **analisti esperti**.

4 Protezione dei dati

Conformità completa a **GDPR** e **normative di sicurezza europee**.



PanOptikon®

UNIFIED SECURITY OPERATIONS
PLATFORM

Porta tutte le attività di SecOps in un'unica piattaforma

- ✓ **Visibilità unificata** degli ambienti IT
- ✓ **Comunicazione e collaborazione** centralizzata
- ✓ **Gestione end-to-end** dell'incidente
- ✓ Procedure operative basate sul **framework NIST**
- ✓ Reportistica avanzata **conforme alle normative**



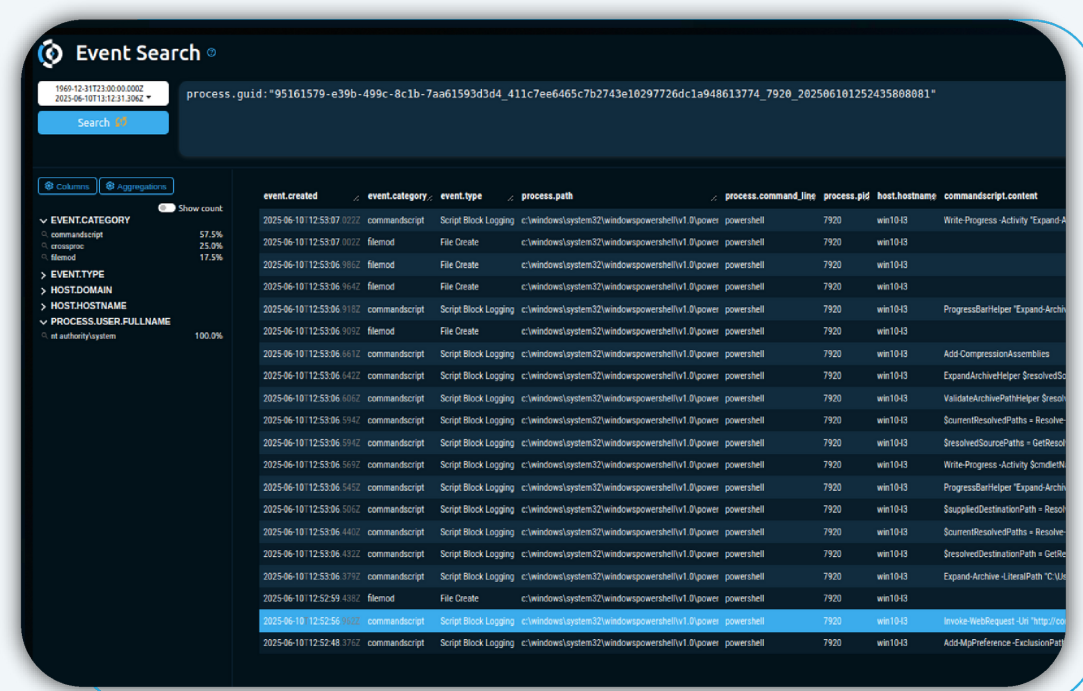


Halo

Visibilità avanzata dei dati telemetrici degli endpoint

Progettato per gli analisti di Certego

- ✓ **Soluzione su misura:** personalizza e sfrutta al massimo le capacità delle soluzioni EDR:
 - Supera le **restrizioni black-box** dei tradizionali sistemi EDR
 - Definisci e applica regole di detection adatte al tuo contesto operativo
- ✓ **Riduzione dei falsi positivi:** ottimizza i carichi di lavoro:
 - **Correlazione avanzata** - Aggrega molteplici eventi in un unico allarme
- ✓ **Applicazione di IOC e BIOC da più fonti senza limiti di importazione**



event.created	event.category	event.type	process.path	process.command_line	process.pid	host.hostname	commandscript.content
2025-06-10 12:53:07.002Z	commandscript	Script Block Logging	c:\windows\system32\windowspowershell\v1.0\powershell	powershell	7920	win10-43	Write-Progress -Activity "Expand A
2025-06-10 12:53:07.002Z	filemod	File Create	c:\windows\system32\windowspowershell\v1.0\powershell	powershell	7920	win10-43	
2025-06-10 12:53:06.161Z	filemod	File Create	c:\windows\system32\windowspowershell\v1.0\powershell	powershell	7920	win10-43	
2025-06-10 12:53:06.161Z	filemod	File Create	c:\windows\system32\windowspowershell\v1.0\powershell	powershell	7920	win10-43	
2025-06-10 12:53:06.110Z	commandscript	Script Block Logging	c:\windows\system32\windowspowershell\v1.0\powershell	powershell	7920	win10-43	ProgressBarHelper "Expand-Arch
2025-06-10 12:53:06.109Z	filemod	File Create	c:\windows\system32\windowspowershell\v1.0\powershell	powershell	7920	win10-43	
2025-06-10 12:53:06.161Z	commandscript	Script Block Logging	c:\windows\system32\windowspowershell\v1.0\powershell	powershell	7920	win10-43	Add-CompressionAssemblies
2025-06-10 12:53:06.142Z	commandscript	Script Block Logging	c:\windows\system32\windowspowershell\v1.0\powershell	powershell	7920	win10-43	ExpandArchiveHelper -ResolvedSo
2025-06-10 12:53:06.109Z	commandscript	Script Block Logging	c:\windows\system32\windowspowershell\v1.0\powershell	powershell	7920	win10-43	ValidateArchivePathHelper \$resol
2025-06-10 12:53:06.194Z	commandscript	Script Block Logging	c:\windows\system32\windowspowershell\v1.0\powershell	powershell	7920	win10-43	SourceResolvePaths - Resolve
2025-06-10 12:53:06.194Z	commandscript	Script Block Logging	c:\windows\system32\windowspowershell\v1.0\powershell	powershell	7920	win10-43	ResolvedSourcePaths - GetResol
2025-06-10 12:53:06.169Z	commandscript	Script Block Logging	c:\windows\system32\windowspowershell\v1.0\powershell	powershell	7920	win10-43	Write-Progress -Activity "Scandi
2025-06-10 12:53:06.142Z	commandscript	Script Block Logging	c:\windows\system32\windowspowershell\v1.0\powershell	powershell	7920	win10-43	ProgressBarHelper "Expand-Arch
2025-06-10 12:53:06.109Z	commandscript	Script Block Logging	c:\windows\system32\windowspowershell\v1.0\powershell	powershell	7920	win10-43	SuppliedDestinationPath - Resol
2025-06-10 12:53:06.140Z	commandscript	Script Block Logging	c:\windows\system32\windowspowershell\v1.0\powershell	powershell	7920	win10-43	SourceResolvePaths - Resolve
2025-06-10 12:53:06.132Z	commandscript	Script Block Logging	c:\windows\system32\windowspowershell\v1.0\powershell	powershell	7920	win10-43	ResolvedDestinationPath - GetRe
2025-06-10 12:53:06.179Z	commandscript	Script Block Logging	c:\windows\system32\windowspowershell\v1.0\powershell	powershell	7920	win10-43	Expand-Archive -LiteralPath "C:\Us
2025-06-10 12:52:59.439Z	filemod	File Create	c:\windows\system32\windowspowershell\v1.0\powershell	powershell	7920	win10-43	
2025-06-10 12:52:56	commandscript	Script Block Logging	c:\windows\system32\windowspowershell\v1.0\powershell	powershell	7920	win10-43	Invoke-WebRequest -Uri "http://se
2025-06-10 12:52:48.176Z	commandscript	Script Block Logging	c:\windows\system32\windowspowershell\v1.0\powershell	powershell	7920	win10-43	Add-MpPreference -ExclusionPat



Threat Intel

CYBER THREAT INTELLIGENCE

Migliora la raccolta, correlazione, arricchimento e analisi degli IOC



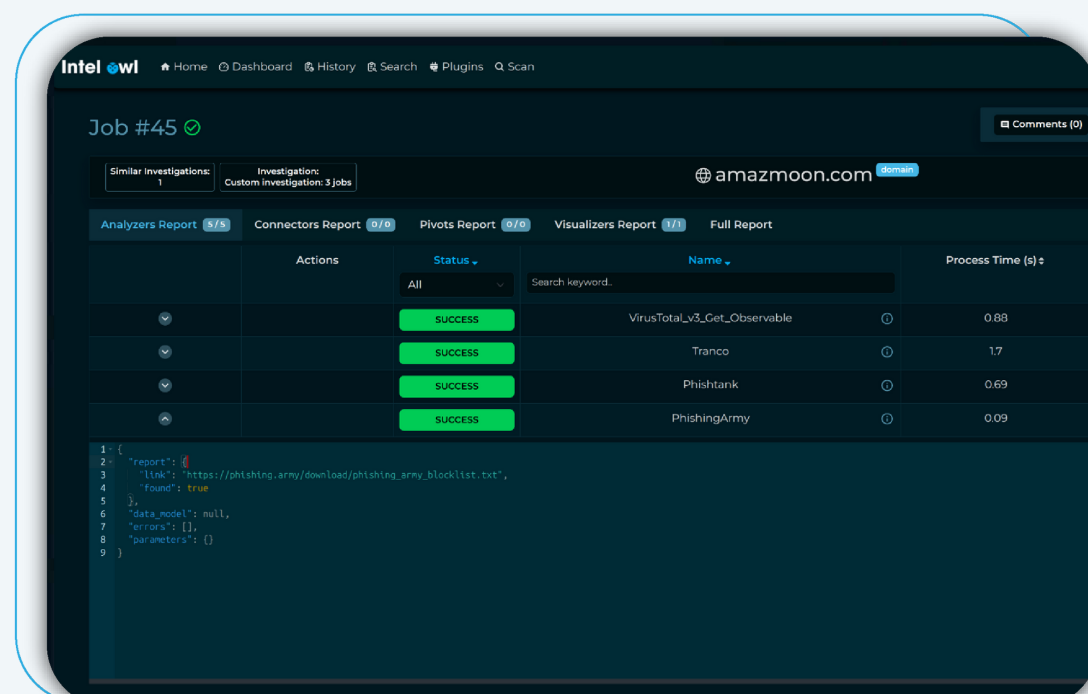
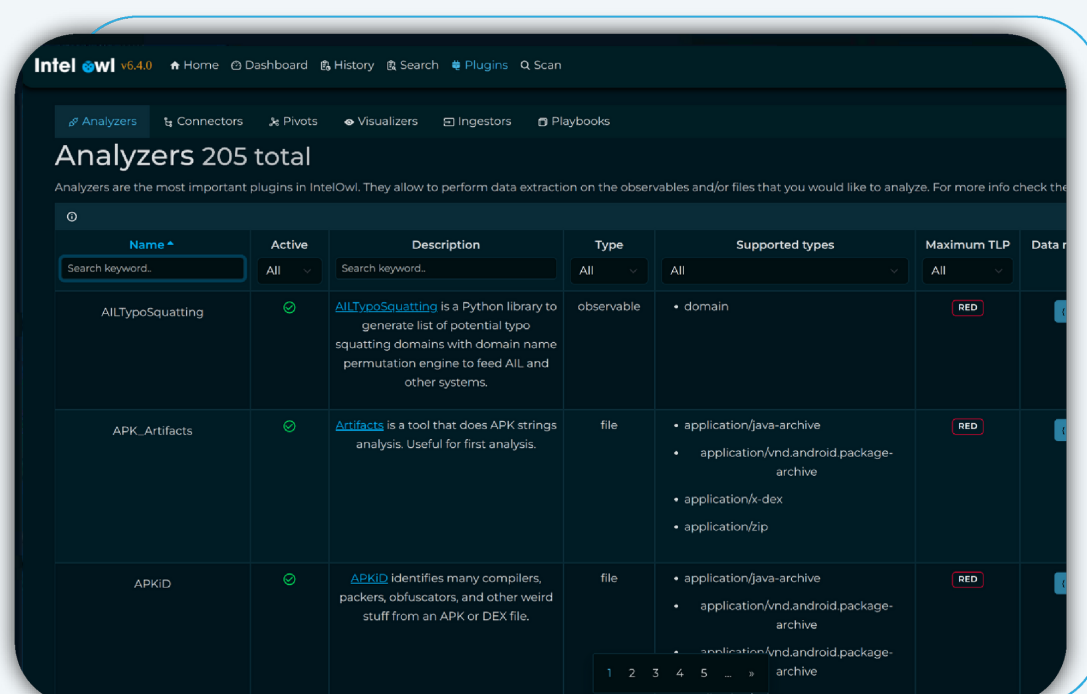
Quokka



Intel Owl

Consentono di raccogliere e correlare dati da honeypot, sensori, info-sharing e dark web, ottenendo **verdicti affidabili** e contestualizzati.

Permettono di **arricchire e validare** i dati di Threat Intelligence, automatizzando l'analisi di IOC tramite fonti esterne.





PURE-PLAY

MDR

Scopri di più sul nostro sito web:
www.certego.net