IBM QRADAR SIEM AND CYOLO PRO INTEGRATION SOLUTION

Cyolo | IBM

Organizations today connect a myriad of users, applications and devices, with little visibility or control over the risks they introduce to the business. Security and operational teams struggle to adequately control the people, processes, and technologies within their environments due to lack of visibility and real-time data available to them.

THE CYOLO + IBM ADVANTAGE

Cyolo, the leading provider of safe and secure privileged remote access for operational technology (OT) and industrial control systems (ICS), announced its new Device Support Module, allowing seamless integration with IBM Security's on-premise QRadar Security Information and Event Management (SIEM) platform. Together, the Cyolo PRO (Privileged Remote Operations) secure remote access platform and IBM's QRadar SIEM will enhance cybersecurity capabilities like threat detection, access control and supervisory requests, and process control changes in critical OT/ICS environments.

The integration comes at a time when Industry 4.0 is under heavy regulatory scrutiny, and organizations urgently need advanced security tools to remain compliant and protected. Security and operations teams are also overwhelmed by the expanding number of connected devices and volume of data in their environments, hindering their ability to manage risk and ensure operational efficiency. The current OT skills gap exacerbates these challenges, necessitating third-party contractors to assist with critical operations. This consequentially adds more risk as many CISOs do not have oversight of third-party activity in their enterprise's network.

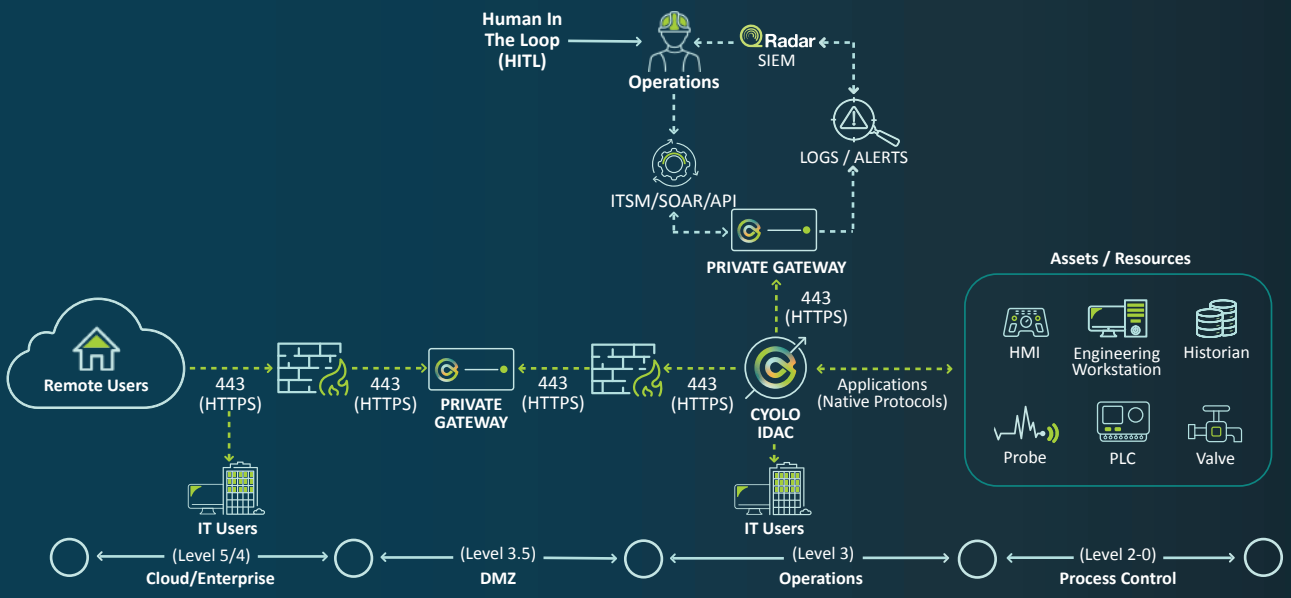
This new integration unlocks:

- **Actionable Intelligence:** Even more efficient and secure analysis of critical OT environments is now possible, allowing swift data extraction from locations that previously required on-site access.
- **Improved Decision-Making:** Greater visibility, control, and speed now enable even more informed decision-making in critical environments.

KEY BENEFITS

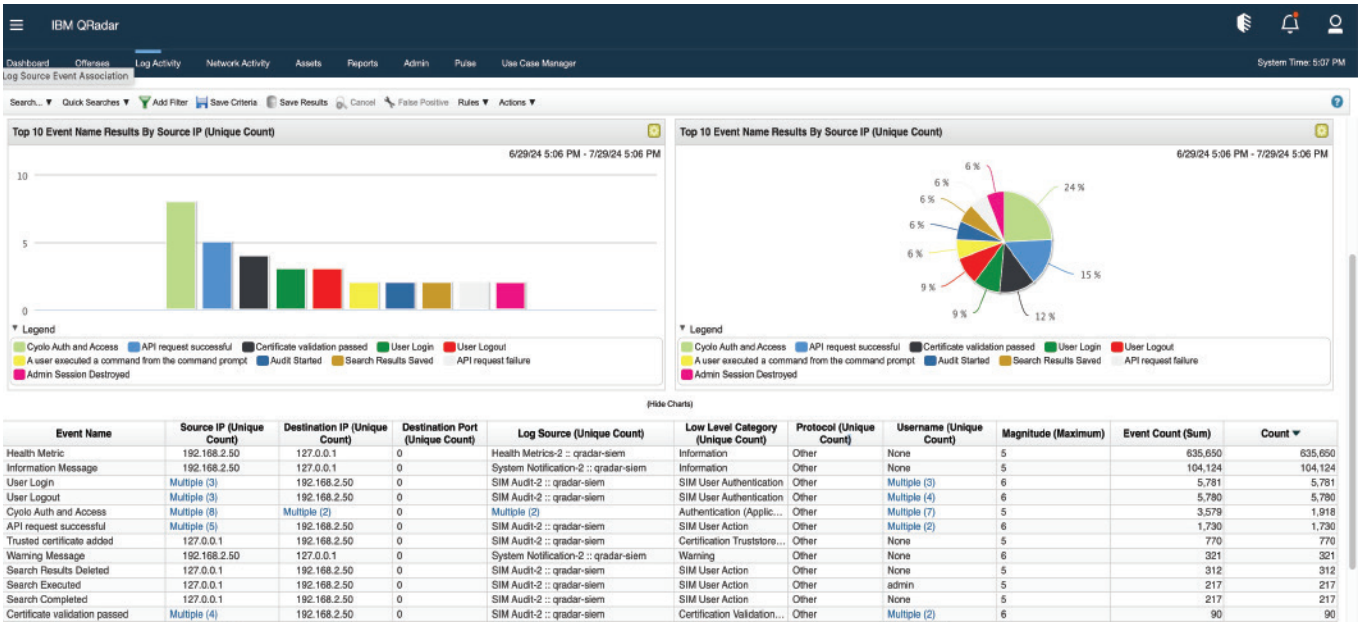
- Proactively and dynamically manage security controls based on vulnerability, risk profile, threats, and regulatory / compliance requirements
- Detect and prioritize threats and vulnerabilities, leveraging IBM Security QRadar SIEM real-time and AI/ML enhanced intelligence
- Safely enforce user, application, and device threat-mitigation changes within the Cyolo PRO platform in conjunction with QRadar threat intelligence
- Control user, application, device and resource access in the Cyolo PRO platform through robust QRadar integration
- Maintain baselines and mitigate deviations using Cyolo PRO with event-driven data provided from the QRadar SIEM platform

UNIFIED INDUSTRIAL CYBERSECURITY CONTROL



IBM QRADAR SIEM PRESENTS CYOLO DATA USING DSM PLUG-IN

The Security Intelligence Platform provides a unified architecture for integrating security information and event management (SIEM), log management, anomaly detection, incident forensics, and configuration and vulnerability management allowing organizations to identify security, policy, and compliance risks in the environment.

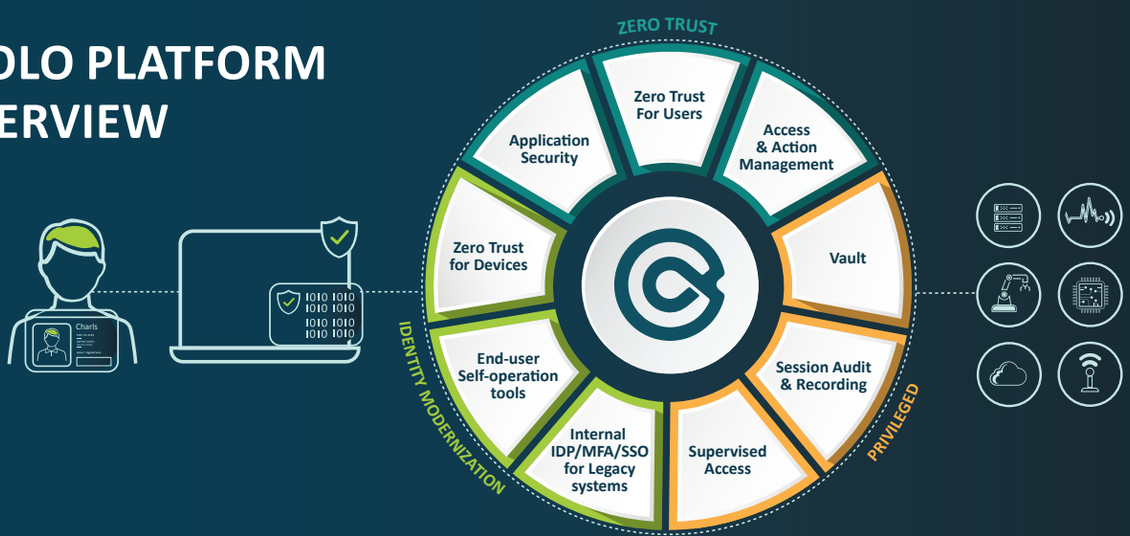


Event Name	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Log Source (Unique Count)	Low Level Category (Unique Count)	Protocol (Unique Count)	Username (Unique Count)	Magnitude (Maximum)	Event Count (Sum)	Count
Health Metric	192.168.2.50	127.0.0.1	0	Health Metrics-2 :: qradar-siem	Information	Other	None	5	635,650	635,650
Information Message	192.168.2.50	127.0.0.1	0	System Notification-2 :: qradar-siem	Information	Other	None	5	104,124	104,124
User Login	Multiple (3)	192.168.2.50	0	SIM Audit-2 :: qradar-siem	SIM User Authentication	Other	Multiple (3)	6	5,781	5,781
User Logout	Multiple (3)	192.168.2.50	0	SIM Audit-2 :: qradar-siem	SIM User Authentication	Other	Multiple (4)	6	5,780	5,780
Cyolo Auth and Access	Multiple (8)	Multiple (2)	0	Multiple (2)	Authentication (Applic...	Other	Multiple (7)	5	3,579	1,918
API request successful	Multiple (5)	192.168.2.50	0	SIM Audit-2 :: qradar-siem	SIM User Action	Other	Multiple (2)	6	1,730	1,730
Trusted certificate added	127.0.0.1	192.168.2.50	0	SIM Audit-2 :: qradar-siem	Certification Truststore...	Other	None	5	770	770
Warning Message	192.168.2.50	127.0.0.1	0	System Notification-2 :: qradar-siem	Warning	Other	None	6	321	321
Search Results Deleted	127.0.0.1	192.168.2.50	0	SIM Audit-2 :: qradar-siem	SIM User Action	Other	None	5	312	312
Search Executed	127.0.0.1	192.168.2.50	0	SIM Audit-2 :: qradar-siem	SIM User Action	Other	admin	5	217	217
Search Completed	127.0.0.1	192.168.2.50	0	SIM Audit-2 :: qradar-siem	SIM User Action	Other	None	5	217	217
Certificate validation passed	Multiple (4)	192.168.2.50	0	SIM Audit-2 :: qradar-siem	Certification Validation...	Other	Multiple (2)	6	90	90

ENABLE SECURE, AGENTLESS ACCESS TO ANY CRITICAL OT/ICS ASSET WITH CYOLO PRO

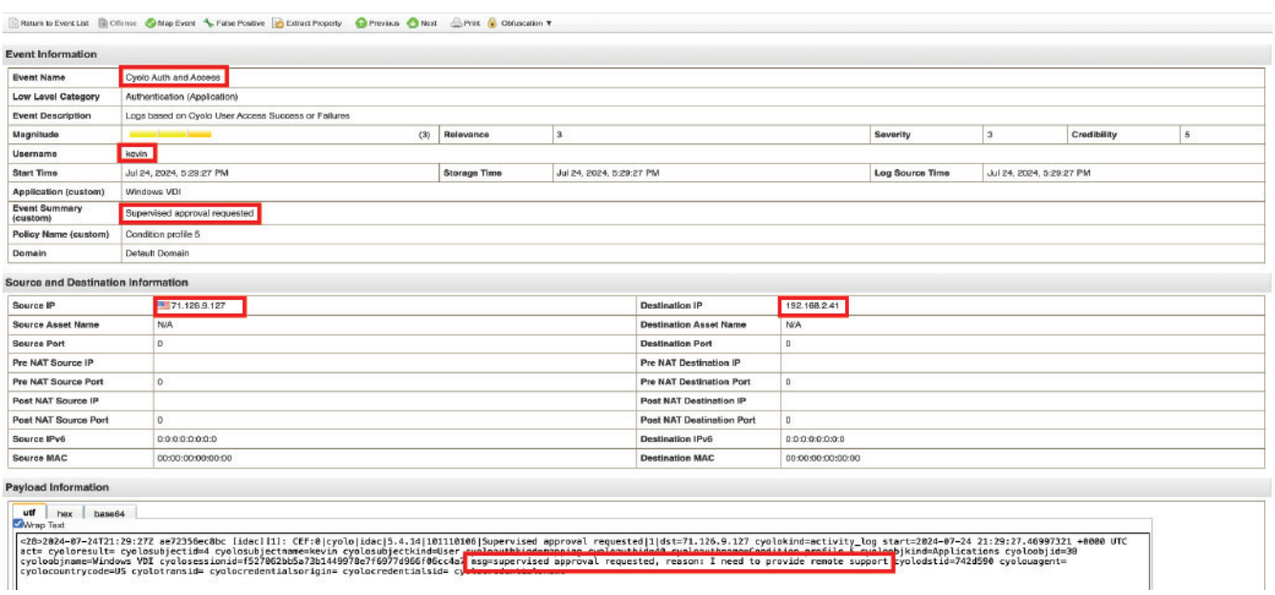
Cyolo PRO (Privileged Remote Operations) is a lightweight, infrastructure-agnostic remote access solution that brings identity-based authentication, access control, and crucial oversight capabilities to OT/ICS.

CYOLO PLATFORM OVERVIEW



CYOLO PROVIDES IBM QRADAR SIEM ACTIONABLE EVENT DATA

Together, QRadar and Cyolo PRO allow operational staff (HITL) to approve, deny, or modify access to the environment for users, applications, and resources in a unified pane of glass. It helps security administrators to evaluate and prioritize network security risks and grant granular user access control through Cyolo PRO.



Return to Event List | Offense | Map Event | False Positive | Extract Property | Previous | Next | Print | Obfuscation

Event Information

Event Name	Cyolo Auth and Access						
Low Level Category	Authentication (Application)						
Event Description	Logs based on Cyolo User Access Success or Failures						
Magnitude	(3)	Relevance	3	Severity	3	Credibility	5
Username	kevin						
Start Time	Jul 24, 2024, 5:29:27 PM	Storage Time	Jul 24, 2024, 5:29:27 PM	Log Source Time	Jul 24, 2024, 5:29:27 PM		
Application (custom)	Windows VDI						
Event Summary (custom)	Supervised approval requested						
Policy Name (custom)	Condition profile 5						
Domain	Default Domain						

Source and Destination Information

Source IP	71.126.9.127	Destination IP	192.168.2.41
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	0	Destination Port	0
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port	0	Post NAT Destination Port	0
Source IPv6	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

Payload Information

utf | hex | base64

Wrap Text

<28>2024-07-24T21:29:27Z ae72356ec8bc [idacl@1]: CEF:0|cyolo|idac|5.4.14|101110106|Supervised approval requested|1|dst=71.126.9.127 cyolokind=activity_log start=2024-07-24 21:29:27.46997321 +0000 UTC act= cyoloresult= cyolosubjectid=4 cyolosubjectname=kevin cyolosubjectkind=User cyoloauthbindmapping cyoloauthbind=0 cyoloauthmappingCondition profile 5 cyoloobjkind=Applications cyoloobjid=30 cyoloobjname=Windows VDI cyolosessionid=f527062bb5a73b1449978e7f6977d966f0bcc4a2 msg=supervised approval requested, reason: I need to provide remote support cyolodstid=742d590 cyoloagent= cyolocountrycode=US cyolotransid= cyolocredentialsorigin= cyolocredentialsid= cyolorandomhash=

ABOUT CYOLO

Cyolo provides secure remote privileged access for cyber-physical systems (CPS). Our solution enables industrial enterprises to simply connect employees and third-party vendors to critical assets.

Cyolo meets the needs of both security and operational technology (OT) teams with a solution that's adaptable to any environment and deploys without causing disruptions or requiring change management.

ABOUT IBM

IBM is a leading provider of global hybrid cloud and AI, and consulting expertise. We help clients in more than 175 countries capitalize on insights from their data, streamline business processes, reduce costs and gain the competitive edge in their industries. Thousands of government and corporate entities in critical infrastructure areas such as financial services, telecommunications and healthcare rely on IBM's hybrid cloud platform and Red Hat OpenShift to affect their digital transformations quickly, efficiently and securely. IBM's breakthrough innovations in AI, quantum computing, industry-specific cloud solutions and consulting deliver open and flexible options to our clients. All of this is backed by IBM's long-standing commitment to trust, transparency, responsibility, inclusivity and service.