QOMPLX:

Summary of QOMPLX Managed Detection and Response (MDR) service capabilities

Detection

Intelligence-fed threat hunting	Our analysts hunt for threats using a variety of intelligence sources including the Indicators of Compromise (IOCs) and reports provided by our QOMPLX:Cyber intelligence team.
Custom detection rules	We know that each client environment is different, that's why we develop custom rules based on your unique operational needs.
Data source ingestion	Bring what you have, we will integrate with the security controls that you currently have in place.
Enriched alerting	We investigate and provide additional details on alerts using our enrichment datasets and expertise.
QOMPLX Managed Assurance	Get the most out of the Q:CYBER platform with our team of specialized analysts

Investigation

Correlated analysis	We correlate activity and events across all sources to deliver tailored analysis.
Alert prioritization	We prioritize alerts and call your attention to those that require immediate analysis and response based on the impact to your specific business requirements.
Detailed results	Our analysts provide detailed investigation reports with results and recommendations for improvement.

QOMPLX:

Response

Validation and notification	QOMPLX analysts execute custom incident response plans upon confirmation of an incident.
Remote response	We work with available solutions and client personnel to drive responses to completion.
Containment and remediation actions	We work with your team to contain attacks and execute any remediation/mitigation activities.
Incident response experts[1]	Activate incident response services as needed.

Collaboration

Phone/Slack/email	Easily access SOC Analysts through multiple channels.
Visibility	Obtain the same view that our analysts utilize through the Q:CYBER platform.
Custom incident response plans	Custom-developed Incident response plans and documentation are provided at onboarding. Utilize our playbook library or your existing plans.
Extended team	We seamlessly integrate with your team and operational cadence to provide regular updates and check-ins so you are always informed.

Reporting

Metric-driven dashboard	Easy-to use activities and performance dashboards display identification of incidents, alerts, responses, and action taken.
Attack surface monitoring	Q:SCAN delivery is integrated in QOMPLX MDR services
Security improvement and resilience Recommendations	We provide ongoing recommendations to improve security and resilience of your environment
Intelligence and threat advisories	Receive early access to our threat and intelligence advisories which contain bad actor and threat scenarios alerts.
Custom reporting per incident	Detailed reporting tailored to your business needs.

[1] Additional Incident Response Professional Services may be provided via executed retainer agreement.