Maltego for Cyber Security Operations

Accelerate complex SOC investigations from hours to minutes.

Reduce Your Cyber Risk with Maltego

Maltego is a graphical link analysis software with data mining and mapping capabilities that can help improve and speed up a multitude of tasks within the SOC team, from monitoring to evidence gathering, and from alert investigation to identification of the source of threats endangering an organization.

With its integration and data ingestion capabilities, Maltego is the user interface where all the data and intelligence needed for complex investigations can be made readily available and queryable, effectively enhancing the analyst's ability to contextualize and analyze events while reducing tool fatigue and time spent on tool alternation.

By adding Maltego to their toolkit, cyber analysts and security operations centers alike can move away from simply implementing basic detection and focus their efforts on the investigation and remediation of severe incidents, directly enhancing the value their SOC provides towards maintaining their organization's cybersecurity posture.

Streamline Security Operations and Cyber Investigations with Maltego: Remediate Complex Threats Faster

Maltego helps streamline the complete security operation life cycle by helping analysts during determination of use cases for monitoring systems, incident confirmation with rapid response data, data enrichment with threat intelligence, threat monitoring, and threat hunting.

Improve Detection Rules and Reduce False Positive Alerts Maltego can help the SOC team better discern between important and ordinary events to tackle alert fatigue. To this end, Level 1 analysts and SOC engineers can use the insights provided by Maltego to tune their security systems. For instance, by periodically running network footprints with Maltego Machines, they will be able to evaluate their current attack surface and build use cases into their systems when reviewing their rules and alert configurations. This will in turn result in the improvement of alert legitimization and reduction of redundant and false positive alerts, as well as the elimination of blind spots in the organization's security.

Increase SOC Efficiency and Effectiveness by Improving and Developing new Playbooks While SOAR solutions enable SOC teams to highly automate and streamline time-consuming workflows for a variety of use cases, their successful implementation requires the team to have clearly defined manual processes after which playbooks can be modeled. Thanks to its data mapping capabilities, Maltego can help SOC Engineers charged with developing/updating playbooks with the validation of their use cases before implementation. Additionally, Maltego can be integrated into a playbook's workflow when human intelligence and decision-making instead of automation are required for further analysis of complex cases.

Integrate Maltego into your Existing Workflows and Reduce Incident Response Time Maltego enables Level 2 analysts and incident responders to perform more efficient evaluations on the scope and severity of incidents thus allowing them to focus their valuable time on remediation. Thanks to its data ingestion capabilities, Maltego can become the one platform where the enrichment, contextualization, and human analysis of complex alerts takes place, thus contributing to the reduction of tool fatigue.

Mine and ingest data

from various sources such as threat intelligence providers, internal SIEM data, OSINT, and other internal logs, systems, and data repositories.

Merge link, and enrich data relationships

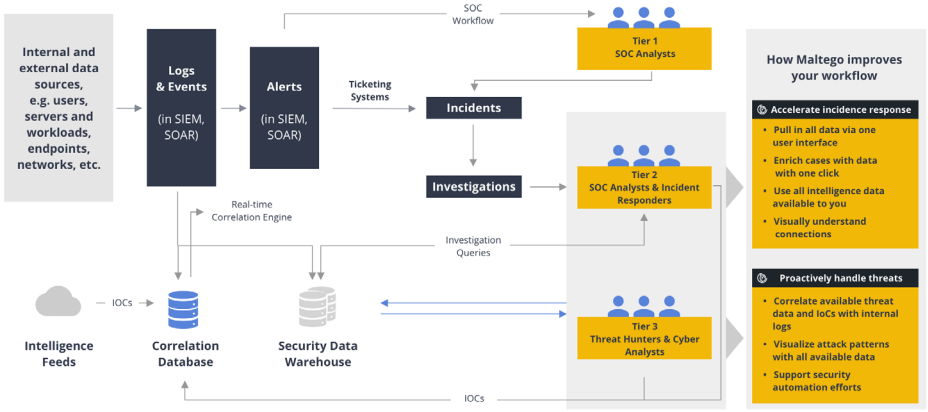
on a graph automatically and collaborate in real-time with team members.

Map and explore relationships and patterns

in your data using different visual layouts and export findings for reporting and documentation

Features	Benefits
Link Analysis	Discover hidden relationships, patterns, and clusters within your data with an intuitive visual analysis interface
Collaboration	Share encrypted graphs and insights with access authentication with your teams and organizations
Automation	Automate standardized investigative processes and re-allocate analyst time from data gathering to data analysis
Stealth Mode	Conduct investigations anonymously and safely without risk of exposing analyst's identity to malicious targets
Export	Share list of IOCs with other teams to easily adjust security rules or update security devices.
Reporting	Generate detailed reports with one click for incident reporting, use case documentation, and playbook improvement

Additionally, with its out-of-the-box integrations and easy-to-implement data integration model, Maltego facilitates the analysts' exposure to a wider array of OSINT sources, threat feeds, and intel providers in order to broaden their expertise and effectiveness.



Contextualize Root Causes of Threats and Identify Unknown Security Gaps

Maltego allows threat intelligence analysts and threat hunters to conduct more effective investigations of anomalies and evidence left in the organization's network by stealthy threat actors. With its data mapping and visualization capabilities, analysts may be able use Maltego to find digital artifacts that other automated tools implemented within the SOC have missed thus far. They will also be able to perform deep dives into datasets internal and external to the organization in order to explore what happens during and after attacks and build up a landscape of potential attacks with insights that can support the rest of the SOC team.

Data at Your Fingertips: Seamlessly Integrate Disparate Data into One Interface

splunk> · servicenow · SHODAN · VIRUSTOTAL · ATT&CK · MISP Threat Sharing
CROWDSTRIKE · DOMAINTOOLS · FORESIGHT SECURITY · FIREEYE · RISKIQ · PASSIVE TOTAL
Recorded Future · THREAT CONNECT · ThreatGRID · INTEL471 · ...and more

Simplify and expedite your investigation by seamlessly integrating your preferred SIEM, threat intelligence provider or internal ticketing systems into Maltego.

Maltego provides enterprise-grade cloud and on-premise deployment as well as options for custom data integrations, in-person trainings, and expert support. Deploy your Maltego solution in a performant way that is also compliant with the needs and privacy guidelines of your organizations.

Download Maltego for free now or **schedule a personalized demo** with our Maltego experts to learn how Maltego increases the speed and precision of complex SOC investigations.

Make it your own:

The Maltego Solution Customized for Your Needs

- Maltego Desktop Client
- Data Integration
- Deployment & Infrastructure
- Support & Services
- Learning & Training

About Maltego

Maltego empowers investigators worldwide to speed up and increase the precision of their investigations through easy data integration in a single interface, aided by powerful visualization and collaborative capabilities to quickly zero in on relevant information. Maltego is a proven tool that has empowered over one million investigations worldwide since its first launch in 2008. Due to its wide range of possible use cases ranging from threat intelligence to fraud investigations, Maltego is used by a broad audience, from security professionals and pen testers to forensic investigators, investigative journalists, and market researchers.

Learn more about how we can empower your investigations on **https://www.maltego.com**

Maltego.com
support@maltego.com