MALTEGO

SIX KEY PHASES OF THE CYBER THREAT INTELLIGENCE CYCLE

PHASE	APPLICATION	CONSIDERATIONS	MALTEGO IN ACTION
DIRECTION (PLANNING)	An example of goal could be "Identifying potential adversaries"	• Check assets and business processes • Conduct risk assessment • Identify the intelligence needs of your organization for threat protection and response • Establish priorities for protection efforts • Ensure access to diverse data sources	n/a
COLLECTION	Examples of collecting information include: • Extracting metadata and logs from internal networks and security devices • Exploring threat intelligence feeds provided by industry groups and cybersecurity vendors • Checking interviews and discussions with specific sources. • Harvesting new information from online data sources	• Ensure access to multiple sources of intelligence to comprehensively understand both potential and actual threats • Keep in mind the possibility of automating the process with the right tools	With Maltego: 1. Pull key events from SIEMs and log solutions into Maltego. Cultivate additional IoCs by pivoting to external data sources 2. Pull the latest threat reports or observations from your threat Intel feeds and use transforms to find key information and IoCs related to them 3. Automate the most common and repetitive investigative steps using Maltego Machines
PROCESSING	Examples of processing the data include: • Identifying IoCs, enriching them with additional information, and formatting appropriately • Human-generated reports may need correlation, ranking, deconfliction, and verification • Extracted IP addresses should be compiled into a CSV file for importation into a SIEM system	• The method of processing varies depending on the nature of the data • Although this process may entail numerous manual and repetitive tasks, remember that automation is possible with the appropriate tools	With Maltego: 1. Evaluate Entity properties, extract additional details, review Detail View information, and check for any labels/overlay for analysis of importance
ANALYSIS (PRODUCTION)	Examples of analysis output include: • Detailed formal reports • Live video feeds • Written briefings	• Identify the intended recipients of the intelligence and the decisions they are expected to make based on it • Ensure that the analysis provides actionable insights, rather than theoretical or academic content.	With Maltego: 1. Use views, labels, notes to help clarify key information on the graph 2. Refine the graph through cleaning unnecessary Entities and selecting Entities to be moved to their own sub-graph for easier comprehension
DISSEMINATION	Example of sharing frameworks and standards: • MISP • STIX • TAXII • OpenIOC	• Determine the specific needs of the intelligence team • Decide on the methods for distributing or disseminating intelligence, such as newsletters, web forums, slide presentations, documents, or oral briefings • Establish the frequency at which collectors or analysts should refresh or update intelligence • Figure out how to render the intelligence actionable for operational use	With Maltego: 1. Share graphs with fellow investigators or other teams for continued use 2. Screenshot graphs for reports, or export results to a CSV 3. Build custom integrations that connect to your threat databases or other security tools to push IoCs directly to them
FEEDBACK (REVIEW)	n/a	• Set up channels to consistently gather feedback from every team involved	n/a

SecurITy made in Germany

ISO 27001:2022 Certified.