Resecurity

Powered by Context

Cyber Threat Intelligence Platform

The appearance of new threats and security challenges requires effective tools for their timely identification and in-depth analysis. Without proper contextualization, an overload of raw intelligence can become a burden, leading to lack of actionable data and incorrect resource planning, which may increase the probability of risk and negative outcome.

Context - is an intelligence platform enabling enterprises and governments to accelerate analysis, prevention and investigation workflows with the goal of discovering valuable insights, and supporting better decision-making, using lightning-fast search and data science. The product is oriented towards intelligence analysts, investigators, SOC/DFIR teams, risk management and C-level security executives.

Unlike other platforms, Context is based on a classic six-step process called the Intelligence Cycle used by government agencies and industry experts, providing a balanced and comprehensive approach to intelligence gathering and analysis.

PLANNING

Context receives subjects of interest from the user enabling definition of criteria and directions for further intelligence collection. Depending on these factors, the platform will prioritize relevant sources and formulate logic to provide the most relevant and adequate results. It leverages a broad set of AI and ML mechanisms to narrow down search.

COLLECTION

Context harnesses a constantly-expanding cloud of indexed threat artifacts and associated adversaries collected from a variety of public and private sources. The platform will capture the results based on source criteria for further enrichment and tagging.

PROCESSING

The third step, processing, involves converting the vast amount of information collected to a form usable by analysts through decryption, language translations, and data reduction in a format that is suitable for the production of intelligence. During this process, incoming information is converted into formats that can be readily used by intelligence analysts.

ANALYSIS AND PRODUCTION

To enable organizations to make strategic and timely decisions, intelligence has to be current, objective and actionable with enough context for interpretation. To be effective, intelligence production must focus on the consumer's needs. It should be objective, timely, and, most importantly, accurate.

DISSEMINATION

The final step of the intelligence cycle is dissemination. Dissemination is the conveyance of intelligence to the consumer in a usable form. Intelligence can be provided to the consumer in a wide range of formats. Context provides flexible workspace for collaboration between team members and an internal case-management system to store and distribute the final intelligence product.

EVALUATION

You may provide feedback on whether your requirements are being met, and if any adjustments or improvements are needed regarding the provided intelligence. We use this information for results scoring and training of our ML engine based on your input. Context also allows the user to evaluate intelligence received from third-party sources – you may import intelligence reports, documents and other files containing subjects of interest for further correlation.

Resecurity www.resecurity.com info@resecurity.com (800) 781-5698 445 S. Figueroa Street, 31st Floor, Los Angeles CA 90071, USA

Resecurity

Feel the difference

Use Cases

ANTI-PIRACY

Hollistic approach to piracy and counterfeit monitoring for various industry verticals. Prevent illicit distribution and use of your products, using actionable intelligence.

INVESTIGATIONS

Built-in case management system allows tracking of subjects of interest (SOI) in real-time and the centralization of collected intelligence with proper tagging and context for further analysis.

SECURITY INTELLIGENCE

Manage multiple internet and external threat intelligence feeds and enrich circulating threat telemetry in your SOC/SIEM/TIP for strategic decision making and proactive incident response.

DATA BREACH INTELLIGENCE (DRM)

Identify the exposure of sensitive data, such as intellectual property, confidential documents, customer and employee data. Prevent the risk of data breaches in your infrastructure or clouds.

DARK WEB MONITORING (DWM)

Lightning-fast search in the darkest corners of the internet. The biggest and constantly updating repository of underground communities and marketplace (TOR, 12P, Freenet, IRCm IM-based)

FRAUD & RISK INTELLIGENCE

Discover the latest tools, tactics and procedures (TTPs) of fraudsters and cybercriminals targeting your enterprise. Use our SDK and the REST API in your apps and services to strengthen anti-fraud.

DIGITAL RISK MONITORING

Inventory your digital assets and control the risk across a variety of digital channels. Set up the settings of your digital footprint and get early warning notifications.

BRAND PROTECTION

Protect your brand from abuse, reputational risks, copyright infringement and intellectual property (IP) violation. Minimize loss of revenue, brand damage and lost of customer trust.

Context draws on data comprising

5B+

Threat artifacts, including indicators of compromise (IOCs), indicators of attacks (IOAs), tools, tactics and procedures (TTPs) of adversaries with valuable meta-data stored in historical form used for deep-dive investigations

9M

Profiles of threat actors collected from various underground communities and criminal marketplaces, intelligence reports and security expert community with associated metadata

300M+

Fully indexed and translated Dark Web data entries with extracted artefacts, graphical screenshots and links visualization

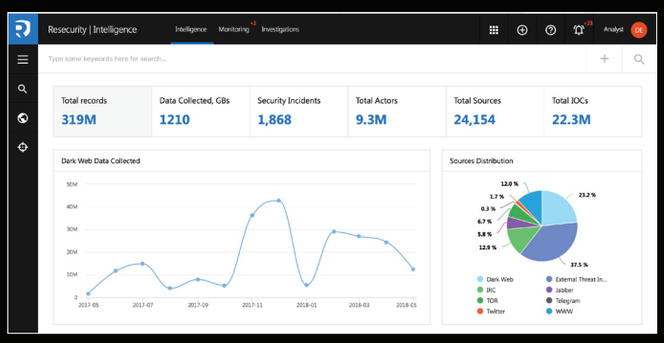
40
LANGUAGES

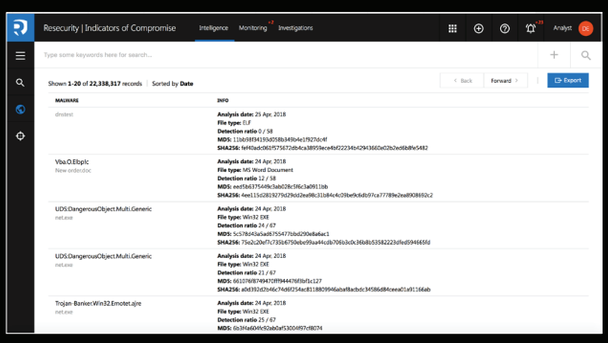
A built-in offline translation solution and unique linguistic expertise in order to provide details on threat actors' chatter

20K+
SOURCES

A constantly updated repository of Dark Web sources, including: Tor; I2P, Freenet, IRC, IM groups (Telegram).

Screenshots





Resecurity www.resecurity.com info@resecurity.com (800) 781-5698 445 S. Figueroa Street, 31st Floor, Los Angeles CA 90071, USA