·|:|· **Recorded Future**®

Threat Hunting with Recorded Future

Cyber operations require relevant and real-time intelligence. It's critical to ensure the relevance of targets for a successful execution. Before an operation even gets off the ground, expeditiously gathering intelligence is required, providing leaders with decisions on courses of action, while also coordinating with other partners, domestic and foreign.

Illuminating blue, red, and gray space activity in near real-time, Recorded Future provides actionable intelligence. Using our key access to dark web, technical forums, and open and closed sources, the Recorded Future Intelligence Cloud automatically collects, processes, and curates in real-time to help facilitate and evaluate your operations.

Our advanced technology enhances your shop's efficiency, reducing translation time with automated Natural Language Processing — including Optical Character Recognition analysis of images for text and code.

Assist in your planning, development, and execution of cyber operations by:
- Collecting and conducting analysis on cyber, information, and physical collection requirements
- Gaining insights into counterintelligence (CI)
- Tracking, monitoring, and provide indications and warnings (I&W) of supporting infrastructure, targets, companies, and more
- Providing analytics across cyber, information and physical environment to support battle damage assessments (BDA)
- Disseminating key elements with partners due to the open-source nature of collection
- Integrating Recorded Future into your intelligence environment to create a holistic common operating picture

INTELLIGENCE CHALLENGE

Build, conduct, and evaluate cyber operations in a dynamic environment with accurate and timely intelligence.

PROCESS

Collect, process, analyze, and disseminate intelligence across various Political, Military, Economic, Social, Information & Infrastructure (PMESII) sectors. Automatically curate actionable offensive and defensive intelligence for decision-makers in real-time, while collecting Indications & Warnings (I&W) to make decisions for cyber assets and allocation.

RECORDED FUTURE SOLUTIONS

- Streamline tools needed by researching and monitoring physical, cyber, and information operations all in one platform
- Tactical enrichment providing context to entities and specific intelligence with over 8 billion Intelligence Cards updated in real-time
- Access dark-web, technical, and closed forums identifying TTPs, CI concerns, and mis/dis-information
- Operational and analytical fusion through Integrations with leading cyber and OSINT companies
- Reduce need for linguists by searching across numerous languages with Natural Language Processing and machine learning
- Identify text in multimedia with Optical Character Recognition

Enabling Cyber Operations

Recorded Future capabilities expand the breadth of pre-mission, execution, and post-mission analysis to support cyber operations.

Pre-Mission Planning	• Network / Terrain Analysis (Platform / Analyst on Demand) • Intel/Threat Analysis/TTPs/COAs (Platform / Analyst on Demand) • Signature Management / Hunting packages (Platform / Analyst on Demand) • Hunt Kit Preparation: Splunk/MISP/ELK/others (API / Professional Services)
Execution Phase (Survey, Secure, Protect)	• Daily intel/info updates pertinent to mission (Platform) • Researching anomalous activity on location via unclassified sources (Platform) • Threat hunting via hunt kit (API) • Baseline monitoring (API) • Intel support to emerging RFIs (Platform) • Malware Analysis (API / Platform / Analyst on Demand)
Post-Mission	• Incident analysis (Platform) • Parallel Reconstruction: Identifying any threats to Mission Partner (Platform) • Aid in development of hardening recommendations (Platform / Analyst on Demand)

Integrations

With over 140 COTS and GOTS integrations, Recorded Future seamlessly integrates with cyber operations and tools. This integration streamlines access to threat intelligence and analytics within threat hunting workflows, enhancing the overall effectiveness and efficiency of threat hunting missions. Popular integrations include:

Security Onion   Microsoft Sentinel   splunk>   elastic   ANALYST1

Learn how Recorded Future can contribute to cyber operations through a demo with our team, or contact Mike Habte directly at mike.habte@recordedfuture.com. And check out our latest public research such as US Technology Purchased for Chinese Public Security Systems or Iranian information operations, exemplifying some Recorded Future analyses which can be used to support cyber operations.