Recorded Future® | Module Overview

	BRAND INTELLIGENCE	THREAT INTELLIGENCE	SECOPS INTELLIGENCE	THIRD-PARTY INTELLIGENCE	GEOPOLITICAL INTELLIGENCE
Challenge	Blindsided by brand attacks: lack of visbility needed to identify cyber attacks targeting their brand - **For novice teams:** lack of cybersecurity expertise: users don't know what to do with available data without clear context, out-of-the-box alerting queries, and prescriptive workflows - **For advanced teams:** spending too much time pulling together disparate data points vs. doing the advanced threat hunting and reporting for which they are trained. Need on structured source of truth.	Manual threat research is time consuming, incomplete, and static **Pain Points:** - Highly trained analysts are spending too much time manually collecting data points leading to incomplete analysis. Many are duplicating work thats already been done - Static intelligence reports dont capture the rapidly evolving nature of threats and contain incomplete or outdated info - Lack of access to high-confidence intelligence results in missed threats	A growing attack surface and abundance of alerts slows detection and response **Pain Points:** - Growing threat landscape - Abundance of alerts - Lack of high-confidence indicators - Research and other tasks are labor intensive and inefficient	Limited visibility, point-in-time evaluations, and manual workflows **Pain Points:** - Lack of visibility into constantly evolving third-party risk landscape - Current risk assessment methods are point-in-time and prone to error - Manual review efforts are resource intensive and inefficient	Disparate sources in local languages makes it impossible to gather and analyze info before insights become outdated **Pain Points:** - Dynamic regional risks are difficult to keep up and respond to - Insights become outdated quickly when teams must manually analyze different sources in different languages - Without a collaborative and efficient way to share and report on risks, organizations are left exposed to potentially dangerous circumstances
Use Cases	- Domain Abuse - Data Leakage Monitoring - Brand Attack Mitigation - Digital Asset Monitoring - Monitoring Threats to your Industry - Fraud Detection	- Advanced Threat Research & Reporting - Advanced Detection 7 Validation - Dark Web Investigation	- Alert Triage - Threat Detection - Threat Prevention	- Continuous Third-Party Risk Management - Procurement Assessment	- Location-Based Monitoring
Features	- Broadest source coverage - Closed forum & dark web monitoring - Customizable queries - Real-time alerting - Takedown services - Industry threat views	- Real-time search and alerting - Closed forum & dark web monitoring - High-confidence threat hunting and detection - Over 1 billion intelligence cards - Risk scores and transparent source evidence	- Broadest source coverage - Real-time risk scores and context - Block-grade indicators - 10+ SIEM and SOAR integrations	- Continuous monitoring of over 350,000 companies - Real-time alerting on risk indicators - Transparent evidence - Insikt research for in-depth company analysis	- Real-time geopolitical monitoring - Location-based intelligence cards and scoring - Broadest source coverage in every language
How RF Helps	- Identify threats in real-time - Threats identified 10x faster - 22% more threats identified before impact - Available as a managed service	- Reduce time compiling reports by 34% - Identify threats 10x faster - Expanded visibility of the threat landscape - 22% more threats identified before impact - Available as a managed service	- Up to 50% more alerts reviewed - Fewer false positives - Detection of previously undetected threats	- Replace a static, reactive approach with proactive real-time monitoring - Complete risk assessments up to 50% faster	- Reduce time compiling reports by 34% - Identify threats 10x faster - Understand the complete threat landscape
Ideal Prospect	Any organization wanting to proactively protect their brand from cyber threats	Advanced threat intelligence teams who need to proactively investigate emerging threats and define tailored alerting rules.	- Security operations team - SOC team - Incident response team that may be using a SIEM, SOAR, IR, or TIP solution	Owns responsibility to manage the security risk of their third parties. Looking to level up program.	Responsible for reporting on the events and threats in a specific area and understanding potential risks to the organization's operations
Roles	- IT security analyst - junior/senior threat - intelligence analyst - security engineering team	- Threat intelligence analysts - Threat research analysts - Information security analysts	- Security operations analyst - Security analyst - Security operations engineer - Security operations specialist - SOC Tier 1-3, level 1-3, or shift analyst - Incident response analyst - Incident responder - IR manager	- Governance, risk, and compliance analyst (GRC) - Third-party risk analyst - Vendor assurance - CISO - Security anaylst	Public sector all-source and open source intelligence analysts
Keywords	- Brandjacking, typosquatting, phishing	- Threat hunting, threat reporting, malware analysis rules (like Yara, Snort, and Sigma)	- Triage, response, remediation - IOC, events, alerts - Incidents, Incident response - Malware analysis - False positives - Mean time to detection (MTTD) - Mean time to response (MTTR) - SIEM (Security Information and Event Management) - SOAR (Security Orchestration, Automation and Resposne)	- Third-party risk, questionnaires, slow assessments	- Location based monitoring - Protests - Terrorist attacks - Geofencing - First responders - OSINT - Area of responsibility - Prioritized information requests - Parallel reconstruction
Win Stories	Metlife described a major Brand module win in which they were able to leverage the domain Abuse alerts for a successful takedown. The team indicated the alert had triggered on a suspiscuous domain, which includes the text & quotdumpmetlife.&quot After an in depth review by their team, it was concluded that the domain was stood up for a former disgruntled emploree posting a manifesto critical of the bosrd of directors. Metlife was able to gather all the data from the alert and submit it for a succesful takedown. Multiple Metlife teams were involved in this effort as it was a high priority for leadership. Overall, the team was very satisfed with the workflow and outcome resulting in a great win for Recorded Future.	Kapsch MSSP recently requested for us to support some prospect work they have with an arms manufacturer, focusing on arms being sold on the dark web market place. The client was very happy with an advanced query that we sent them to show the sheer number of relavent results our platform holds. Weeks later, Insikt published a report "The Interconnectedness of the Dark Web Marketplace" with details on the Hyenas market. The report included coverage of the prospects firearms for sale. We forwared the Insikt report to Kapsch with a new advanced query including images of firearms for sale. Kapsch was supremely thankful for all of the above support.	HealthEquity mentioned the Triage Sandbox has been awesome and is quickly becoming one of their favorite tools. It has contributed to a number of outcomes for positive malware verdicts and maliscious phishing domains. Most recently, they were investigating a malicious file downloaded by one of their users. The file was quarntined by Microsoft Defender. They submitted the file to Triage and it quickly categorized the file as Qakbot, which saved a lot of time in thier investigation. The extracted indicators were also very useful to confirm the malware had been contained. They mentioned that they haven't had to log into Threat Grid because Triage is so much faster.	A transportation company had a third-party vendor Impacted by Lockbit 2.0. Summary: The customer contacted us on Monday to inquire about a ransomware attack that impacted Wabtec. Insider knowledge: Wabtec was impacted by Lockbit 2.0. The customer then utilized the hunting packages and YARA rules from our Threat/SecOps modules for Lockbit ransomware variants. According to internal communications our customer was not impacted and the ransomware event was localized to a single Wabtec plant.	With a wide physical presence, Samaritan's Purse has teams located in hostile environments around the globe. With some direction within the platform, we were able to provide context on any coup-related violence in Myanmar that SP's physical security team was not able to see -- any proactive information we can provide helps keep their workers safe.

	VULNERABILITY INTELLIGENCE	IDENTITY INTELLIGENCE	PAYMENT FRAUD INTELLIGENCE	ATTACK SURFACE INTELLIGENCE
Challenge	An overwhelming abundance of critical vulnerabilities and limited resources to patch **Pain Points:** • Too many "high" and "critical" vulnerabilities discovered each year • Prioritized based on CVSS scores alone is ineffective • No visibility into what vulns are actually exploited	Strong identity authorization is more important than ever before. Missed threats, delayed responses, Increased Risk **Challenges:** • Expanding attack surface • Dynamic ecosystems of employees, customers, and third parties • Increase in account takeovers • Growth in remote work **Pain Points:** • Compromised data is often not discovered until it is actively being used to attack an organization • Customers and partners expect the organization to protect their identities and detect fraudulent activities. Failure to do so will result in financial, legal, and reputational damage. • Manually collecting, collating, and analyzing compromised identity information is time consuming and prone to human error. Potentially leading to security breaches while wasting IT resources and valuable time.	Proactively identify and mitigate risks from card fraud **Pain Points:** • High cost of fraud coming from cards that have been compromised in CP and CNP breaches • Limited data on dark web card shops and card checker services • Large number of customers at risk per day • Reactive an/or manual approaches to mitigating payment card fraud • Limited info on merchants that have been compromised • Inability to scan merchants for live infections	Discover and defend your entire attack surface **Pain Points:** • Lack of visibility of exposed assets • Incomplete or out of date asset lists • Lack of context around assets • Hard for organizations to maintain a persistent view of their Internet-facing assets • Orgs struggle with dynamically updated asset inventory (ephemeral cloud assets, employees using remote access services, M&A, etc etc)
Use Cases	• Vulnerability prioritization • Monitoring Vulnerabilities in your tech stack	• Account takeover prevention • Personnel identity monitoring • Third-party identity monitoring	• Card fraud prevention • Compromised merchant monitoring • Underground cybercriminal reporting	• External asset discovery and management • Attack surface monitoring and reduction • M&A - Independent discovery of M&A assets, both pre- and post-acquisition. Tracking of divestitures to ensure full deprecation of sold-off assets • SOC - Streamline SOC processes by automating the identification of risky public-facing assets. Integrate API for domain and IP enrichment. • Vuln Mgmt - ASI will discover new company assets to fuel more complete vulnerability scanning
Features	• Vulnerability risk scores based on exploitation • Real-time alerting before vuln publication • Integrations with vuln management solutions • Browser extension for CVE enrichment	• Broadest source coverage • Automated risk checks for critical events • Automated exposed credential triage • Real-time context for risk mitigation	• Proactive identification of compromised cards • Continuous monitoring of closed forums & the dark web • High fidelity stolen & sold card metrics from the cyber underground • Magecart scanning to uncover infected e-commerce sites	• Continuous scanning of the internet for attack surface blind spots • World's largest archive of past and present DNS history • Persistent view of the attack surface landscape • Transparent context and evidence
How RF Helps	• Prioritize vulnerabilities based on real risk • Access to info on vulnerabilities ~ 11 days faster than the NVD • Available as a managed service	• Detect credential leaks in real-time • Respond to compromises before business impact • Gain unmatched visibility into closed and dark web sources	• Prevent payment card fraud before it can occur • Identify up to 90% of compromised card assets within hours of being on the dark web • Pinpoint compromised common points of purchase (CPPs) • Reduce false positives	• Discover previously unknown shadow IT and out of policy assets • Accelerate vulnerability scanning and incident response • Confidently prioritize assets that may be vulnerable to threats or exploits
Ideal Prospect	Vuln mgmt, SecOps, teams responsible for vulnerability assessment, threat intel teams interested in vulns	Mid to large enterprise, with a security or IT team that builds and manages identity tools and integrations and faces a high risk of account takeover/hijacking (ex. finance & retail)	Banks, credit unions, and payment service providers issuing credit cards with over $250M in annual revenue	• Large organizations with established vulnerability teams • Large organizations in heavy M&A industries • Organizations in highly regulated industries • Some SMB organizations with early adopters
Roles	• Vuln mgmt analyst • Threat and vuln mgmt analyst • IT security analyst • Threat intelligence analyst	• Cyber security/Threat Intelligence (CTI) • Information Security/Systems/Risk, IT • Network Engineering/Infrastructure • Identity & Access Management (IAM) • Global Fraud, Consumer Identity	Fraud specialists, Chief Risk Officer, CFO	• Vuln risk mgmt team • Threat hunters • Soc teams • Tier II SOC analyst
Keywords	Vulnerability, CVSS score, exploit in the wild, proof of concept code	• Identity access, authentication & governance • Privileged access management • Digital Trust • Account Takeovers (ATO) • Business email compromise (BEC) • Identity fraud/theft • Identity compromise & credential leaks	• Chargebacks and fraud investigations • Blocking and reissuance • Fraud management systems (FICO Falcon, INETCO Insights etc) • Partial data elements (Bank identification number (BIN), expiration date, final digits of account number etc. • Compromised common points of purchase (CPP) • Magecart • Card checker services	• Attack surface management (ASM), monitoring, risk reduction, digital risk protection, external asset discovery, asset mapping and monitoring, digital risk monitoring, shadow IT
Win Stories	Wiktor recently joined Aptiv as their new Vulnerability Manager and has limited bandwith to triage all Vulnerability module alerts. He reports that he appreciates the product and CVE intelligence cards because it makes it easy for him to do ad hoc research and make decisions on patching requirements. He said that the intelligence is comprehensive and sufficient for descision making, which gives him confidence that he is effectively managing the security of his tech stack.	During a recent onsite with Multicert PERSON technical POC was grateful and provided great feedback for a recent malware log sample we were able to provide to him when investigating an internal comprise. This helped him identify a developer who did not have EDR installed on one of his machines and reduced the time of IR efforts drastically. PERSON has provided a quote following the demo and that is continued to be discussed internally for Identity module.	When reviewing Recorded Future, the card issuer quickly realized the value of Payment Fraud Intelligence. During the pilot, the issuer was alerted to cards for sale on the dark web, and saw that within minutes of each sale, fraudulent transactions appeared on the cards. Consequently, the issuer was able to block these fraudulent transactions and continously find additional accounts that came up for sale on the dark web. As a result of the findings from the pilot, the card issuer decided to purchase Recorded Future Payment Fraud Intelligence and reported "We were unable to find any other solution that even came close to Recorded Future's offering." The card issuer noted that with the help of Payment Fraud Intelligence, "We have had a significant measurable impact on the amount of fraud we've been able to prevent, and have also been able to further improve our customer experience by preventing disruption due to fraudulent charges."	TD Bank shared that they saw the critical risk rule that triggered for one of their hosts. They pinged their vulnerability team to see if they were tracking it and they did not initially have visibility. Once alerted, they confirmed that the host is in fact vulnerable and they are working on remediating.