STRIKEREADY

Cyber Escalation amid US-Israel & Iran Conflict

By: StrikeReady Research
Published: March 17, 2026

Executive Summary

On February 28, 2026, the US and Israel launched a joint military campaign, Operation Epic Fury/Roaring Lion, against Iran. As the conflict escalated into direct kinetic warfare, cyber operations have increasingly shifted toward a full-scale cyber war. The initial coordinated US and Israeli strikes disrupted IRGC command-and-control infrastructure and significantly reduced domestic connectivity to a critical 4% in Iran. Since then, the digital battlespace has evolved beyond traditional state-led espionage into a decentralized threat landscape targeting governments, critical infrastructure, and private sector organizations.

With the recently established Electronic Operations Room, state-sponsored actors, affiliated hacktivists, and cybercriminal groups are operating with overlapping objectives to target Israeli, Western, and Gulf-region infrastructure. Concurrently, the Middle East, Turkey, and Africa (META) region has experienced a drastic surge in conflict-themed social engineering campaigns, enabling threat actors to conduct intelligence collection while capitalizing on escalated geopolitical urgency. StrikeReady brings actionable visibility into this volatile cyber activity, enabling organizations to operationalize threat intelligence into defensive and strategic readiness.

Threat Landscape Overview

As cyber operations emerge as the primary theatre of active conflict in the Iran-Israel geopolitical landscape, let us take a deep dive into StrikeReady's latest intelligence and operational capabilities aimed at strengthening organizational security posture.

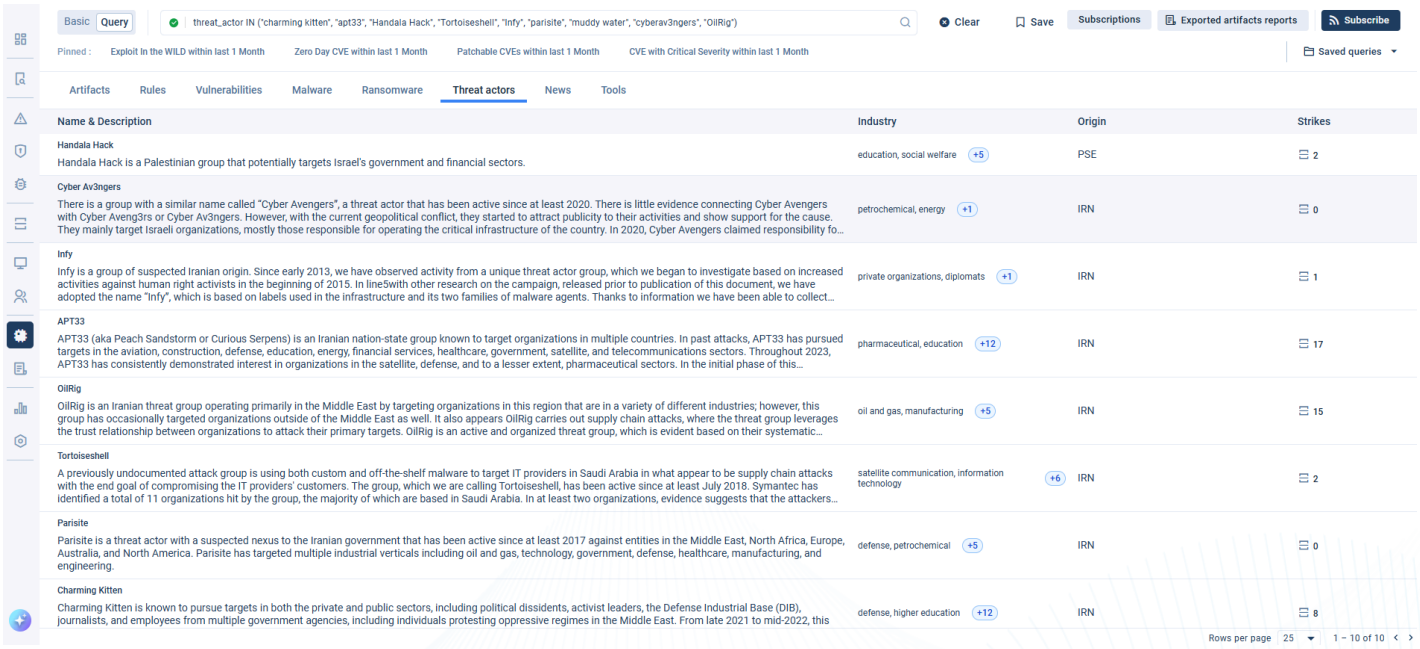
Iran-aligned threat actors

Threat Actor	Details	Recent Activity (March 2026)
Handala Hack	**Aliases:** Void Manticore, Banished Kitten, Red Sandstorm, Storm-0842, Dune, Karma **Focus:** Healthcare, Medical Equipment, and Services across Asia (Israel), North America (US), and Europe (Albania) **Observed TTPs:** T1485: Data Destruction, T1072: Software Deployment Tools, T1491.002: External Defacement, T1078.002: Valid Accounts	Responsible for a massive wiper attack on Stryker Corp (US). Claimed a breach of Verifone, allegedly leaking transaction data. Abused Microsoft Intune to push malware and broadcast threats.
MuddyWater	**Aliases:** Mango Sandstorm, Static Kitten, Seedworm, Mercury, TEMP.Zagros, Earth Vetala, Yellow Nix **Focus:** Governments, Financials, Transportation and Logistics in Asia (Israel, UAE, Jordan, Turkmenistan), North America (US), and Europe (UK, France) **Observed TTPs:** T1059.001: PowerShell Command & Scripting, T1027: Obfuscated Files or Information, T1102.003: Web Service, T1557: Adversary-in-the-Middle	Deployed a previously unknown backdoor named Dindoor against US banks and airports. Currently deploying BugSleep and MuddyViper backdoors against Israeli maritime logistics. Observed using AI-assisted malware iteration to bypass EDR signatures during the blackout.

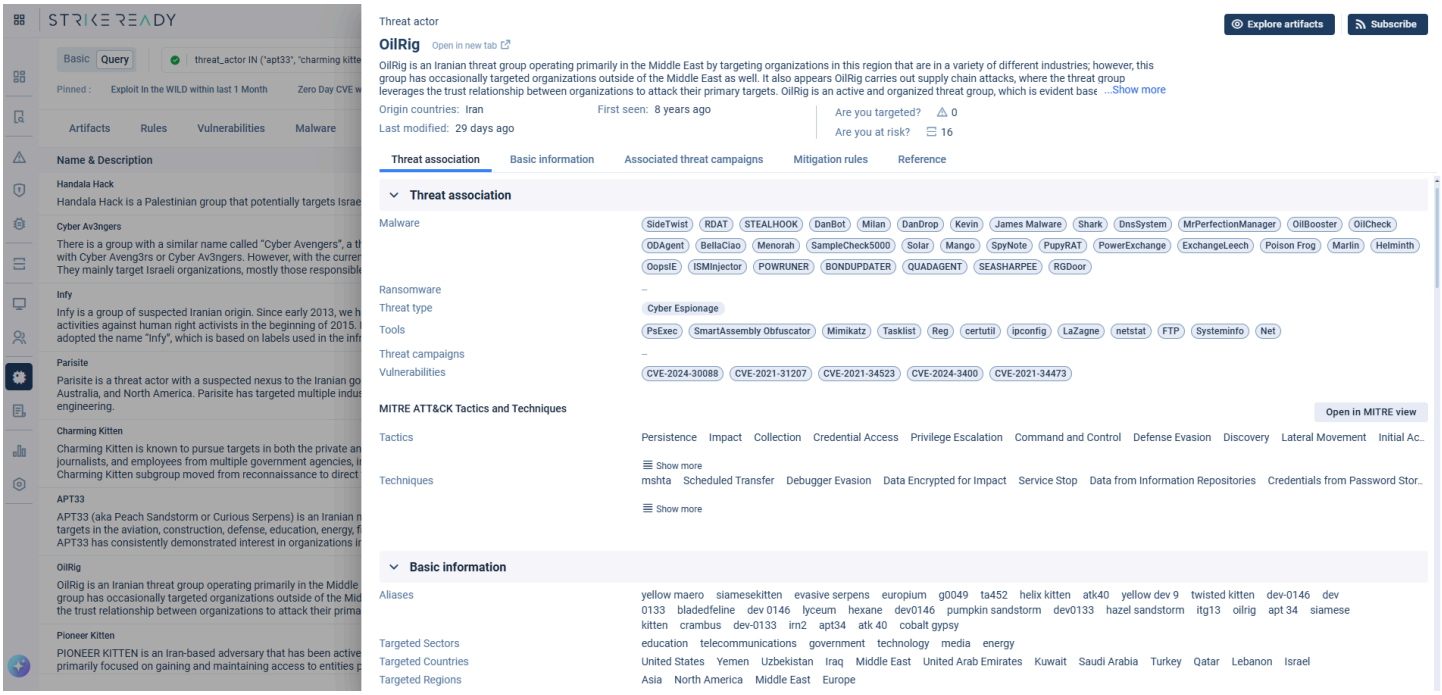
Charming Kitten (APT42)	**Aliases:** Mint Sandstorm, Newsbeef, Phosphorus, TA453, Rocket Kitten, Charming Cypress **Focus:** Government, Technology, Research & Development, and diplomatic entities in Asia (Saudi Arabia, Kuwait, Qatar), and North America (US) **Observed TTPs:** T1566: Phishing, T1137.006: Office Application Startup Add-ins, T1102: Web Service, T1114.002: Remote Email Collection, T1555.003: Credentials from Web Browsers	Conducted credential phishing campaign targeting prominent US/Israel think tanks using fake roundtable invites focused on Middle East air defense to harvest military strategy data.
APT33 (Peach Sandstorm)	**Aliases:** Elfin, Magnallium, Refined Kitten, Holmium **Focus:** Government, Financials, Telecommunication, and Energy in Middle East (Saudi Arabia, Kuwait, Qatar), and North America (US) **Observed TTPs:** T1485: Data Destruction, T1567.002: Exfiltration to Cloud Storage, T1098: Account Manipulation, T1528: Steal Application Access Token	Iran's primary kill-switch threat to Gulf Energy and Aviation networks if the conflict widens. Pivoted to identity-centric targeting and cloud-native persistence (ALMA backdoor) to prepare destructive wiper operations against Western-aligned maritime and energy infrastructure.
APT34 (OilRig)	**Aliases:** Hazel Sandstorm, Helix Kitten, Crambus, IRN2, Cobalt Gypsy, Pumpkin Sandstorm, ATK40 **Focus:** Governments, Telecommunications, and Media across Middle East (UAE, Saudi Arabia), North America (US), and Europe. **Observed TTPs:** T1566: Phishing, T1071.001: Web Protocols, T1568.002: Domain Generation Algorithms, T1078.002: Domain Accounts	Specializes in deep persistence in Middle Eastern government and diplomatic networks. Utilizing CVE-2024-30088 to monitor diplomatic ceasefire negotiations and coalition internal communications

Operationalization with StrikeReady

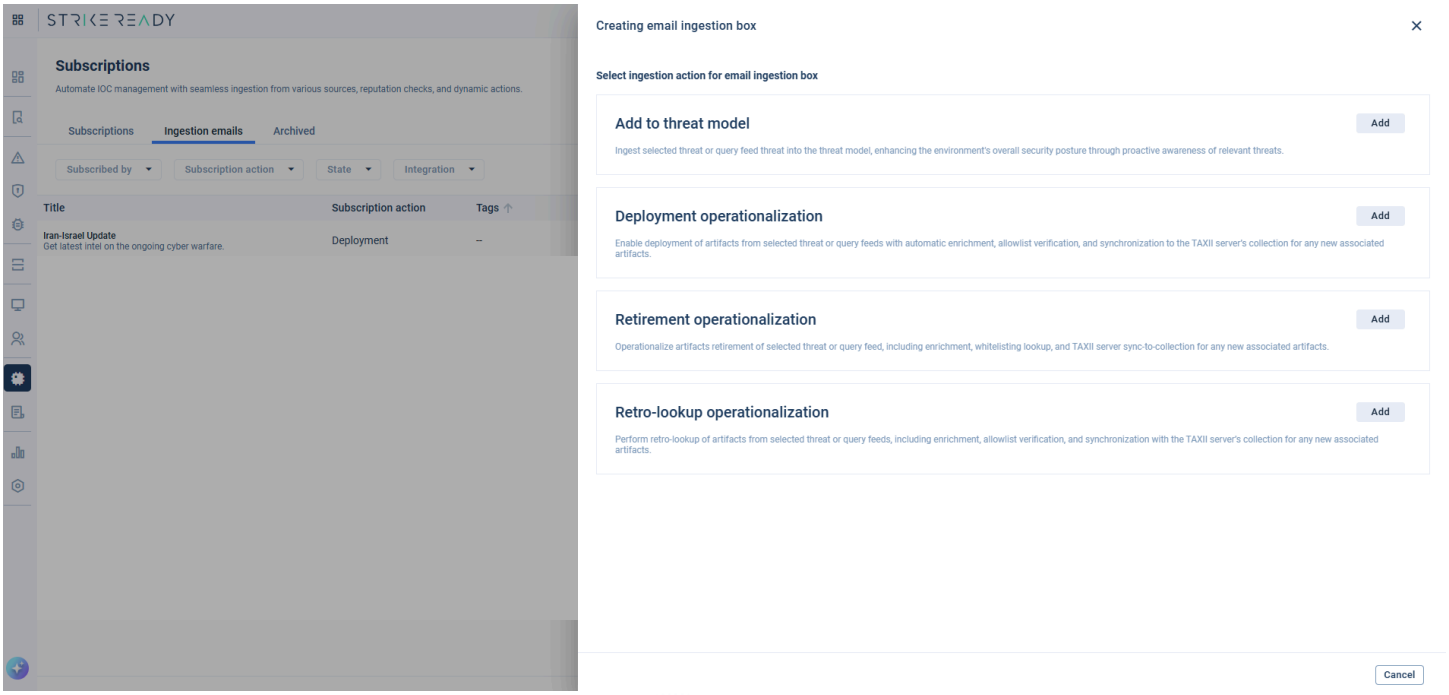
StrikeReady Recon StrikeReady Recon provides relevant activity linked to all the active threat actors. It also provides insights into emerging threat intelligence to help security teams monitor how detection and response technologies are being utilized.



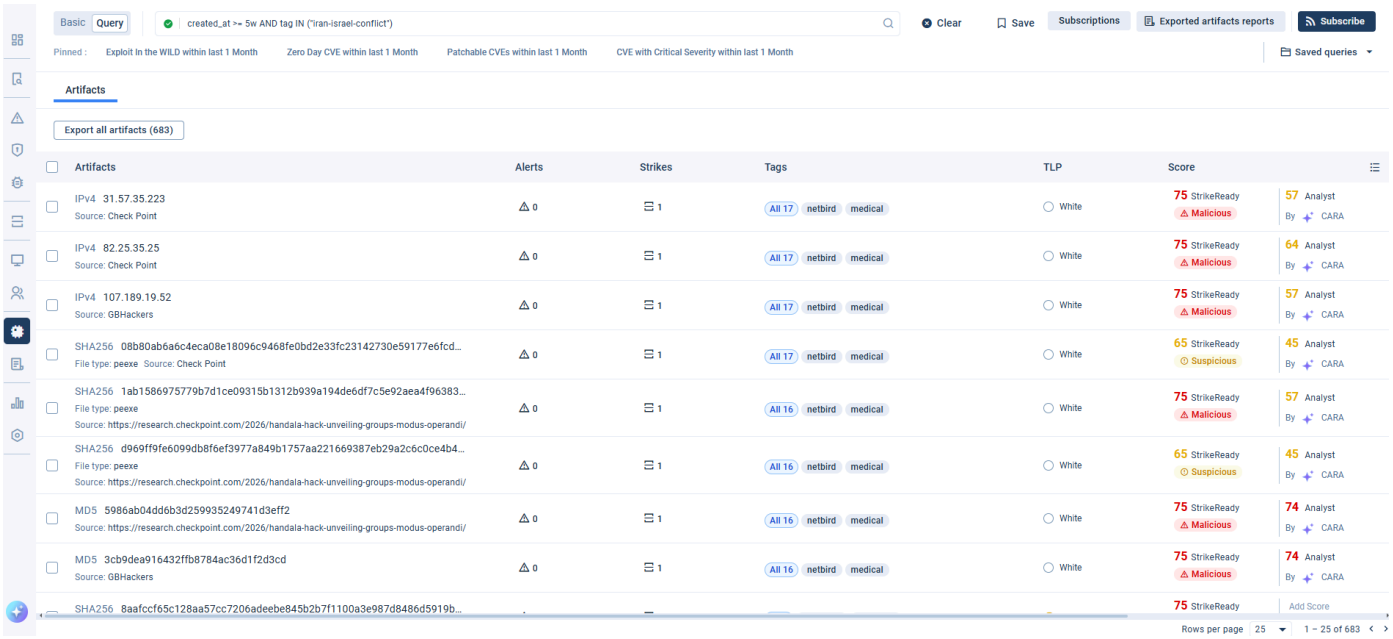
Users can navigate to Threat actor page for a detailed overview including its basic information, threat association, and more.



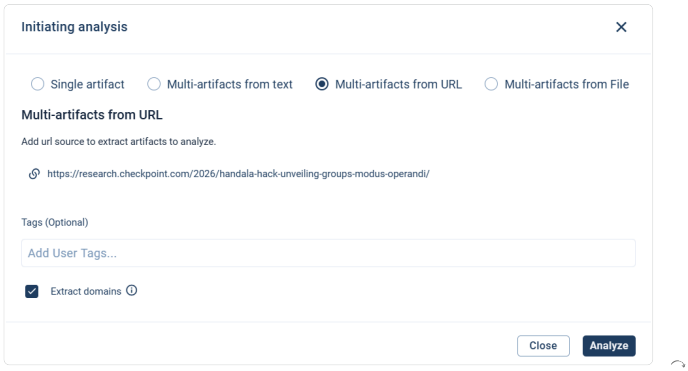
StrikeReady enables organizations to operationalize external intelligence feeds through an automated **Threat Advisory Deployment** via Email Ingestion to streamline their workflow. If configured, extracted artifacts can be automatically enriched, deployed or retired across integrated security controls. Each ingestion creates a case and notifies users in real-time.

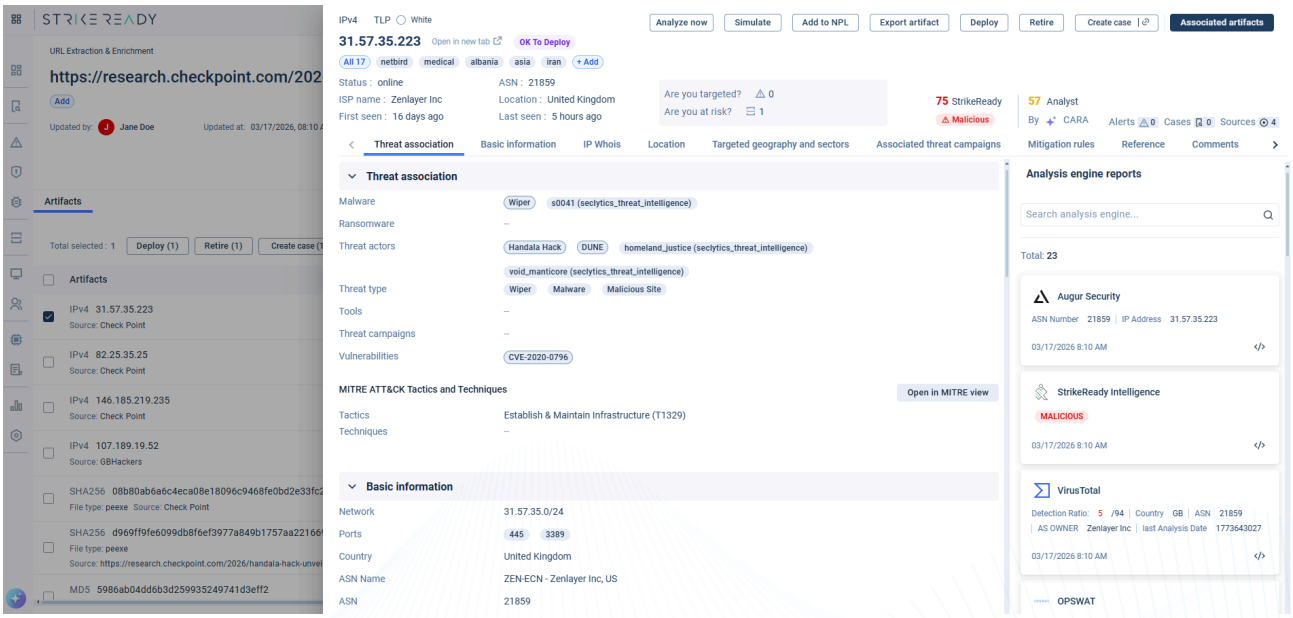


StrikeReady has introduced a new tag "**Iran-Israel-Conflict**" that help analysts quickly filter all the threat intelligence associated with the ongoing geopolitical escalation.This query can be subscribed to in Recon to stay protected from new threats.

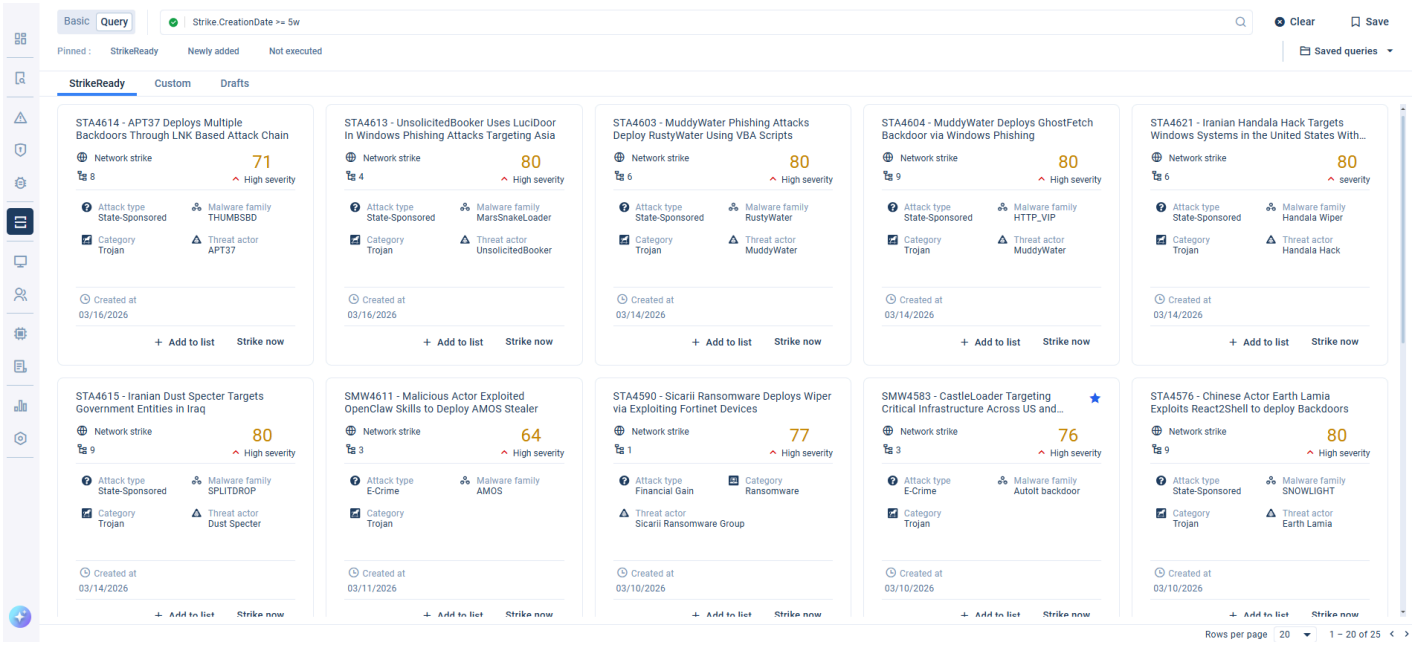


StrikeReady Analysis Engine Tool provides analysis (single or multiple artifacts) for suspicious files, domains, IPs, or URLs from external sources that could pose security risks. Users can view details of all extracted artifacts and may Analyze, Simulate, Export, Deploy, Retire, or View associated artifacts of any selected artifact as shown:

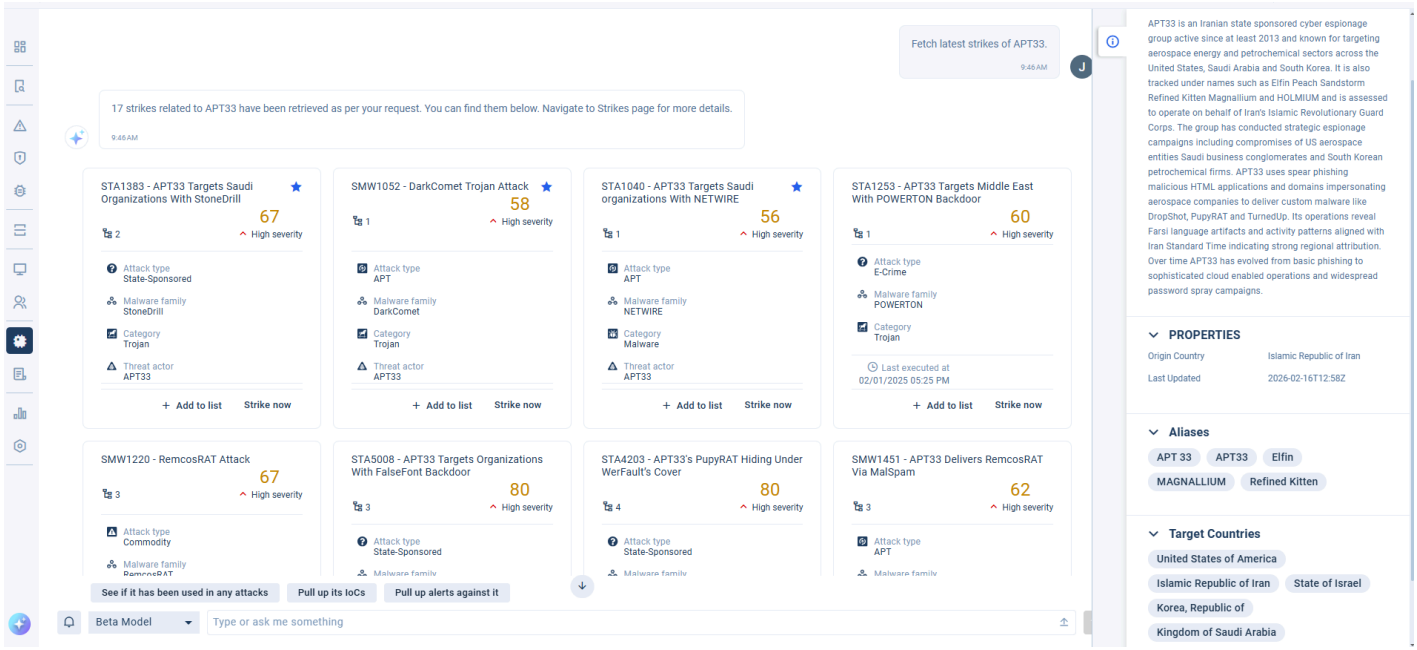




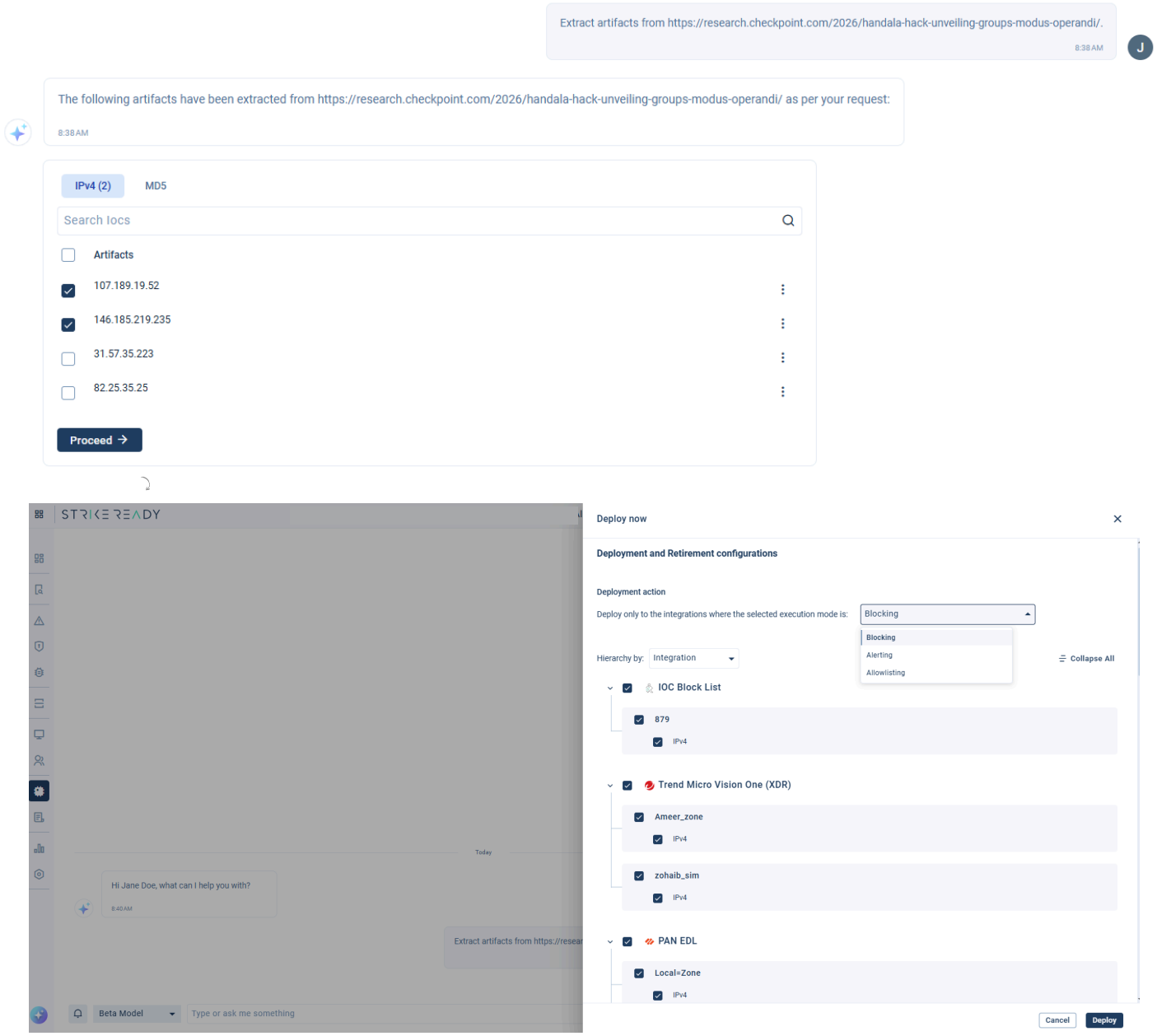
StrikeReady Assessment allows users to monitor their security posture with its Stats Dashboard, Strikes, and Plan Execution workflows. It helps understand the effectiveness of your organization's security measures and identify areas that may need attention.



StrikeReady's CARA, Cyber AI Response Analyst, can inform you about the relevant threat actors, recent strikes, exploited vulnerabilities, or IOCs and advise the best course of action with real-time actionable insights to improve your response time.



CARA's Blog Analysis automatically extracts from a given blog or URL, enabling users to quickly operationalize it through deployment and retirement configurations as demonstrated:



Mitigation & Remediation

- Enforce phishing-resistant MFA (FIDO2 where possible) across email, VPN, and cloud services.
- Enforce least privilege access and continuous monitoring of administrative actions.
- Implement advanced email filtering for spearphishing links and attachments.
- Monitor outbound traffic for anomalous connections to cloud services, Telegram APIs, or DNS tunneling activity.
- Restrict direct internet exposure of ICS/SCADA management interfaces wherever operationally feasible. Implement network segmentation, VPN-based access controls, and strict authentication for remote industrial system management.
- Alert employees to lures specifically themed around regional air defense, roundtable invites, and military strategy, which are currently used by Charming Kitten to harvest intelligence.
- Prioritize immediate patching of CVE-2024-30088, CVE-2024-24919, CVE-2024-4577, CVE-2026-1731, currently being weaponized for initial access and lateral movement.

Indicators of Compromise (IOCs):

Indicator	IOC Type	Threat Actor
1ab1586975779b7d1ce09315b1312b939a194de6df7c5e92aea4f963835f7b08 aa124a4b4df12b34e74ee7f6c683b2ebecAce9a8edcf9be345823b4fdcf5d868 a2001892410e9f34ff0d02c8bc9e7c53b0bd10da58461e1e9eab26bdbf410c79 c23bac59d70661bb9a99573cf098d668e9395a636dc6f6c20f92c41013c30be8	SHA-256	Handala Hack APT41 MuddyWater MuddyWater
fileportalshare.netlify.app fortigate.forticloud.online airconnectionapi.azurewebsites.net 1stemployer.com bootcamptg.org	Domain	Charming Kitten APT34 (OilRig) Tortoiseshell Tortoiseshell MuddyWater
https://1drv.ms/b/c/cbec61ab8028f986/IQDa9igU3D3BRqiyNtth76AzAbOM6jUpa8apnuRl-zKXKow?e=E8bIfd	URL	Charming Kitten
46.246.3.223 46.246.3.245 146.185.219.235 107.189.19.52 159.198.68.25	IPv4	APT34 (OilRig) APT34 (OilRig) Handala Hack Handala Hack MuddyWater

StrikeReady Research is working day and night to find further information and will keep its customers updated as events regarding this conflict unfold.