ANOMALI

Data Sheet

ANOMALI DARK WEB THREAT INTELLIGENCE

CLOSE INTELLIGENCE GAPS

Anomali Dark Web Threat Intelligence delivers five intelligence feeds that address material gaps in crimeware, nation-state actor coverage, pre-compromise alerting, and credential monitoring, all integrated directly into ThreatStream Next-Gen. The feeds are powered by Flashpoint and Team Cymru.

These feeds provide outside-in monitoring of the open internet, dark web, underground forums, and adversary infrastructure. Unlike generic threat feeds, Anomali delivers deep crimeware and nation-state actor coverage with threat actor attribution, pre-ransomware early warning alerting, command and control (C2) infrastructure indicators, and automated dark web credential monitoring.

WHAT MAKES THIS DIFFERENT

Most commodity threat feeds lack depth on crimeware and nation-state threat actors and do not provide pre-compromise visibility. These ThreatStream Next-Gen feeds close those gaps with high-fidelity observables linked to actor profiles and campaign context, structured narrative intelligence, and customer-specific alerting for credentials and initial access broker listings, plus C2 indicators you can match against your own telemetry.

All five feeds integrate into ThreatStream Next-Gen's existing workflows. Anomali Dark Web Intelligence delivers crimeware and nation-state IOCs to enrich suspicious IPs with actor attribution. Anomali Early Warning Alerts provide a 24–72 hour warning before ransomware access is sold. Anomali C2 Detection delivers hourly C2 indicators your SIEM and firewall can match against your own logs to find compromised hosts. Anomali Credential Monitoring alerts prompt password resets before business email compromise. Anomali Threat Briefings deliver executive-ready intelligence as ThreatStream Next-Gen Threat Bulletins.

DARK WEB THREAT INTELLIGENCE AT A GLANCE

Anomali Dark Web Threat Intelligence addresses five material gaps in the ThreatStream Next-Gen feed ecosystem:

- C2 infrastructure indicators providing a curated list of known command and control servers to match against your own logs (Anomali C2 Detection)
- Dark web compromised credential monitoring and alerting (Anomali Credential Monitoring)
- High-fidelity crimeware and nation-state threat actor coverage (Anomali Dark Web Intelligence)
- Pre-compromise initial access broker early warning alerting (Anomali Early Warning Alerts)
- Structured narrative intelligence linked to observable data (Anomali Threat Briefings)

Anomali customers gain access to specialized monitoring infrastructure and analyst expertise that close the visibility gaps most organizations face when defending against nation-state and ransomware threats.

KEY BUSINESS VALUE

- Early detection of adversary access leading to ransomware (24–72 hour lead time)
- Earlier detection and blocking of crimeware and targeted-attack C2 traffic by matching known C2 indicators against your own telemetry and security controls
- Proactive credential compromise alerting before BEC or account takeover
- Deep crimeware and nation-state coverage (e.g., Iranian/APT35 coverage for Middle East energy and critical infrastructure)
- Executive-ready threat intelligence reports as Threat Bulletins
- Automated compliance evidence for SOC 2, ISO 27001, and cyber insurance

KEY FEED BENEFITS

- C2 indicators to match against your own telemetry
- Adversary infrastructure coverage, such as APT35/ Charming Kitten and BellaCiao, with threat actor attribution
- Pre-ransomware Anomali Early Warning Alerts when your network has been compromised for initial access (e.g., VPN access points)
- Per-customer Anomali Credential Monitoring alerts with complete credential records
- Threat reports with tactical and strategic intelligence linked to IOCs
- Customer-specific filtering (Anomali Early Warning Alerts, Anomali Credential Monitoring)
- High-fidelity observables with confidence scoring
- Integration with existing ThreatStream Next-Gen workflows

KEY USE CASES

PRE-RANSOMWARE DETECTION

- SOC manager receives an Anomali Early Warning Alert that the company network access is compromised. Security team investigates and remediates before ransomware deployment.

NATION-STATE ATTRIBUTION

- Threat hunter bulk-loads APT35 IOCs and retrospectively hunts 90-day log history for prior compromise with immediate actor attribution.

C2 INFRASTRUCTURE MATCHING

- The SOC matches hourly C2 indicators against its own logs, finds a host contacting a known controller, and pivots to the linked malware family.

CREDENTIAL COMPROMISE

- Security team receives an Anomali Credential Monitoring alert that 15 employee credentials appeared in a dark web dump. Identity team forces password resets before BEC or account takeover.

EXECUTIVE BRIEFINGS

- CISO uses Anomali Threat Briefings on APT35 targeting energy sector to brief executive leadership on active nation-state threats relevant to the business.

COMPLIANCE AUDIT

- Compliance officer uses Anomali Credential Monitoring alert logs as audit-ready evidence of credential monitoring for SOC 2, ISO 27001, and cyber insurance requirements.

THE FIVE FEEDS

ANOMALI C2 DETECTION

Hourly C2 IP and domain indicators with confidence scores and malware family context. Your SIEM and firewall can match them against your own logs to flag connections to active controllers and link hosts to the malware family.

Available to: All Customers (opt-in)

ANOMALI CREDENTIAL MONITORING

Alerts when employee credentials appear in dark web dumps or infostealer logs. Targeted alerts per customer based on email domain scope (no noise from other organizations). Complete credential records delivered in ThreatStream Next-Gen for immediate password reset action.

Available to: All Customers (scoped per registered email domain)

ANOMALI DARK WEB INTELLIGENCE

Posts from underground forums, chat channels, paste sites, and illicit marketplaces where threat actors trade access, tools, and stolen data. Analysts can search adversary conversations, trace actors across communities, and add underground context to investigations.

Available to: All Customers

ANOMALI EARLY WARNING ALERTS

Alerts when your organization, domains or brands are named in underground listings, including initial access broker posts.

Available to: Customers who register terms to monitor (opt-in)

ANOMALI THREAT BRIEFINGS

Structured threat intelligence reports (e.g., APT35/KittenBusters targeting the Middle East energy sector). Published as ThreatStream Next-Gen Threat Bulletins with direct links to IOCs and actor profiles. Tactical and strategic intelligence: what the adversary is doing, why it matters, and which IOCs to hunt.

Available to: All Customers

WHAT'S INCLUDED

FEED	AVAILABILITY	WHAT YOU GET	WHY IT MATTERS
Anomali C2 Detection powered by Team Cymru	Opt-in (IP scope required)	Hourly C2 IP and domain indicators with confidence scores and malware family context	Lets your SIEM and firewall flag connections to active controllers
Anomali Credential Monitoring powered by Flashpoint	Domain registration required	Complete credential records from dark web dumps	Prompts password resets before business email compromise or account takeover
Anomali Dark Web Intelligence powered by Flashpoint	All Customers (default)	Vetted crimeware and nation-state indicators with MITRE ATT&CK techniques and malware configurations	Gives analysts the adversary's tooling and techniques, not just an address to block
Anomali Early Warning Alerts powered by Flashpoint	Opt-in (register terms to monitor)	Alerts when your organization is named in underground listings, including initial access posts	Surfaces chatter about your organization that internal tooling cannot see
Anomali Threat Briefings powered by Flashpoint	All Customers (default)	Structured Threat Bulletins with linked IOCs	Turns raw indicators into context that SOC teams and leadership can act on

SEE ANOMALI IN ACTION

Anomali.com

© Copyright 2026 Anomali Incorporated®. All rights reserved. ThreatStream® is a registered trademark of Anomali Inc. Anomali Match™ ("Match"), Anomali Lens™ ("Lens"), and Anomali Copilot are trademarks of Anomali Inc.