

# Real-Time Alerting, Actionable Intelligence with ThreatConnect and Dataminr

## The Challenge

Cybersecurity teams need real-time visibility into potential threats and impactful events against their organization. Collecting, aggregating, analyzing, and alerting on threats is resource-intensive without the right solutions that are integrated together to help analysts work more efficiently and effectively.

## Why ThreatConnect + Dataminr?

Dataminr Pulse for Cyber Risk is a real-time external risk detection solution that uses AI across public data. ThreatConnect's Alerts App integration with Dataminr Pulse for Cyber Risk enables cybersecurity teams to quickly connect and aggregate, enrich, analyze, and respond to real-time Pulse alerts, all from a single platform. Dataminr Pulse for Cyber Risk alerts are converted into actionable threat intel data in ThreatConnect, along with associated context, enabling cybersecurity teams to know and take action when events are happening that could potentially threaten and impact their organization.

## Key Benefits

- ♦ Eliminate existing blind spots of risk and strengthen organizational resilience with real-time, external cyber event, risk, and threat detection that can be enriched with unified threat intelligence and context, enabling enhanced prioritization and response.
- ♦ A customized Dataminr Pulse for Cyber Risk threat feed that only delivers alerts relevant to your organization, resulting in less noise and more actionable alerts your team can act upon.
- ♦ Enable analysts to centrally manage, analyze, and respond to threats and events in a single platform.
- ♦ Get granular control and performance insights of the integration from a single dashboard.

# Get Results with ThreatConnect + Dataminr

The power of ThreatConnect and Dataminr enables analysts to assess, prioritize, and respond to threats and events with precision and efficiency across a variety of use cases:

- **Threat Detection and Prevention** - Know about threats in real time. Take proactive action on emerging threats and reduce the time to respond to active threats.
- **Alert Triage** - Analysts are constantly overwhelmed with alerts and struggle to prioritize the most critical ones. Automated enrichment of alerts with context is vital to prioritizing the threats that matter.
- **Incident Response** - A fast response to threats is vital to minimize the impact to the organization's digital assets. Leveraging Workflows and Automation in ThreatConnect TI Ops enables a fast and consistent response to active threats.
- **Vulnerability Prioritization** - Cybersecurity teams must triage hundreds of vulnerabilities every week. Assessing and prioritizing the ones that need remediation requires significant resources. Leveraging a continuous monitoring approach to detect real-time changes to a vulnerability in a unified source of threat and vulnerability intel, along with automated contextualization, supports a proactive response to major shifts in a vulnerability's lifecycle.

Groups

hasIndicator() and tag in("Category: Network Scans","Category: Phishing")

1-100 of 10882 total results

Type TI	Summary TI	Tags
Event	Newly observed malicious IP 4.236.188.25 hosted on AS8075 in ...	10
Event	Phishing URL detected impersonating Netflix: Sensor via uriscan.	5
Event	Phishing URL detected impersonating Booking: Sensor via uriscan.	4
Event	Phishing URL detected impersonating Credit Agricole: Sensor via...	4
Event	Phishing URL detected impersonating Amazon: Sensor via uriscan.	4
Event	Phishing URL detected impersonating Verizon: Sensor via uriscan.	5
Event	Phishing URL detected impersonating DANA: Sensor via uriscan.	4
Event	Phishing URL detected impersonating PayPal: Sensor via uriscan.	4
Event	Phishing URL detected impersonating DANA: Sensor via uriscan.	4
Event	Phishing URL detected impersonating DANA: Sensor via uriscan.	4
Event	Phishing URL detected impersonating DANA: Sensor via uriscan.	4
Event	Phishing URL detected impersonating Line: Sensor via uriscan.	4
Event	Phishing URL detected impersonating DANA: Sensor via uriscan.	4
Event	Phishing URL detected impersonating Verizon: Sensor via uriscan.	5

Phishing URL detected impersonating Netflix: Sensor via uriscan.

Visual Analysis

Create Custom Report

Company	2024-07-18	Netflix, Inc.
Location Name	2024-07-18	Netflix, Inc. HQ, Los Gatos, CA, USA
IP Geo Latitude	2024-07-18	37.2593139
IP Geo Longitude	2024-07-18	-121.9619835
Source	2024-07-18	https://app.dataminr.com/#alertDetail/5/99838042821316370926169-1721331332811-1
Priority	2024-07-18	Alert
Source Channel	2024-07-18	sensor
Additional Analysis and Context	2024-07-18	

Timestamp	Link
2024-07-18T19:35:32Z	https://uriscan.io/result/65605ceb-628e-4911-bd24-48ea15a9c52f/

Associated Indicators

Type		Owner	Date Added
Address	2606:50c0:8003:0:0:0:153	Dataminr Pul...	2024-07-17
ASN	ASN54113	Dataminr Pul...	2024-07-17
URL	https://laxmparmer260.github.io/netflix_cl...	Dataminr Pul...	2024-07-18

## How to Get Started

ThreatConnect's Dataminr Pulse Alert Engine App is available via the App Catalog in the TI Ops Platform. To learn more about [ThreatConnect TI Ops](#), take the [interactive tour](#) or [contact sales](#) for a demo. To learn more about [Dataminr Pulse for Cyber Risk](#) or get a demo, please [contact sales](#).



ThreatConnect enables threat intelligence operations, security operations, and cyber risk management teams to work together for more effective, efficient, and collaborative cyber defense and protection. With ThreatConnect, organizations infuse ML and AI-powered threat intel and cyber risk quantification into their work, allowing them to orchestrate and automate processes to get the necessary insights and respond faster and more confidently than ever before. More than 200 enterprises and thousands of security professionals rely on ThreatConnect every day to protect their organizations' most critical assets.

[sales@threatconnect.com](mailto:sales@threatconnect.com) | +1-646-701-7826 | [www.threatconnect.com](http://www.threatconnect.com)



Dataminr delivers the earliest warnings on high impact events and critical information far in advance of other sources. Recognized as one of the world's leading AI businesses, Dataminr enables faster response, more effective risk mitigation and stronger crisis management for public and private sector organizations spanning global corporations, first responders, NGOs, and newsrooms.

[info@dataminr.com](mailto:info@dataminr.com) | +1-646-701-7826 | [www.dataminr.com](http://www.dataminr.com)