ThreatVision

A Portal to See Through the Chaos

SAFA | TEAMT5

Email hello@safateam.com

A Deep Dive into ThreatVision's Reports

ThreatVision's intelligence reports fall under three categories: APT in Asia, Vulnerability, and Cyber Affairs. These reports provide invaluable insights for decision-making and response.

APT in Asia Flash Reports

deliver timely, accurate, and actionable intelligence with just-in-time alerts for the latest APT intrusions, publishing twice a week and detailing specific targeted attacks with essential IoCs.

Cyber Affairs Biweekly Reports

provide strategic cyber intelligence on the Chinese-speaking cyber world, giving insights into China's cyber capabilities, publishing every two weeks and recapping cybersecurity news, policies, regulations, and incidents.

Vulnerability Insights Reports (VIR)

share technical details about critical vulnerabilities, providing possible attack scenarios and detection tools, published every two weeks, focusing on one critical vulnerability each time.

APT in Asia Monthly Reports

offer strategic intelligence in the Asia Pacific region, connecting cyberattacks to recent political events, policies, and foreign affairs, published monthly and summarizing 13-16 APT attack cases in the past month.

APT Campaign Tracking Reports (CTR)

enhance understanding of significant threat groups and campaigns in the APAC region, publishing two CTRs per quarter with in-depth analyses on threat groups, tactics, targets, and an APT Threat Landscape report at the end of Q2 and Q4.

Patch Management Reports (PMR)

supply information on critical vulnerabilities, helping prioritize patch management, updated biweekly, summarizing around 100 critical vulnerabilities with affected products and patching details.

The Importance of Threat Intelligence

TeamT5 recognizes the significance of each type of intelligence, including:

Strategic Threat Intelligence

Vital for C-level executives responsible for decision-making, strategic threat intelligence provides insights into an organization's threat landscape, identifies malicious actors targeting the organization, and sheds light on their objectives.

Operational Threat Intelligence

Crucial for SOC leaders and analysts, operational threat intelligence focuses on understanding hacker techniques and actively preventing potential threats.

Tactical Threat Intelligence

Essential for rapid incident response teams, tactical threat intelligence provides precise threat indicators to assess the current situation and take appropriate measures to mitigate the impact and resolve the situation at hand.

Getting Started with ThreatVision

To get started, contact your SAFA representative and apply for a 14 day ThreatVision trial account, or email us at hello@safateam.com if you are new to our products and wish to learn more.

We look forward to working with you to keep your organization safe from cyber threats.

ThreatVision

A Portal to See Through the Chaos

SAFA | TEAMT5

Email hello@safateam.com

What is ThreatVision?

ThreatVision is a comprehensive intelligence platform that specializes in providing Asia-Pacific-centered cyber threat intelligence. With over a decade of experience in researching malicious code, APT (Advanced Persistent Threat) groups, and cyber threats in the Asia-Pacific region, ThreatVision offers a wealth of intelligence resources for organizations. The platform caters to different roles within the cybersecurity landscape, including decision-makers, risk managers, and incident responders, by offering strategic, operational, and tactical threat intelligence. It aids C-level executives, risk managers, and incident responders in understanding the threat landscape, identifying malicious actors, and deploying effective defenses against cyber threats. ThreatVision's customizable intelligence investigation and consulting services, along with its user-friendly interface and curated reports, empower organizations to make informed decisions, allocate security resources effectively, and enhance their cybersecurity.

ThreatVision’s Core Features

01

Indicators of Compromise (IoCs)

IoCs provide rapid threat identification and serve as essential clues for tracing attack sources within an enterprise.

02

Threat Hunting Tools

These tools offer direct detection capabilities to quickly understand the current environment and identify potential issues.

03

Intelligence Reports

Intelligence reports offer analysis of hacker behavior, providing a deeper understanding of attacks and the motives behind them.

04

Adversary & Malware Gallery

A library of first-hand files on malicious groups and programs, enabling understanding of threats.

05

RFI Service (Request for Information)

Analysts provide customized reports and tool services to customers, allowing personalized intelligence.

06

API Service

Allows for quick integration of platform resources to facilitate intelligence automation.