CASE STUDY: CRIMINAL IP

Strengthening State-Level Threat Intelligence Operations with Criminal IP TI

USE CASE
Threat Intelligence–Driven System Analysis

INDUSTRY
Government Cybersecurity

REGION
Germany

SOLUTION
Criminal IP Threat Intelligence

Overview

A German state cybersecurity authority has expanded its threat intelligence capabilities by integrating **Criminal IP Threat Intelligence (TI)** into its operational workflows. The solution now supports analysts with enriched, context-driven insights that significantly improve the accuracy, reliability, and depth of system assessments across the state's digital footprint.

Pre-Adoption Challenges

Prior to adopting Criminal IP Threat Intelligence, analysts faced several challenges in accurately identifying, attributing, and assessing external systems relevant to the state's cybersecurity responsibilities.

Insufficient Context for System Analysis

Existing tools provided only superficial insights into domains, IPs, and hostnames, limiting analysts' ability to determine relevance, severity, and operator attribution

Inaccurate Locality Assessment

Difficulty distinguishing between infrastructure inside or outside the state led to uncertainty in determining responsibility boundaries

Limited Attribution Capabilities

Without reliable WHOIS, infrastructure history, or operator detail, analysts struggled to classify whether assets belonged to public or private sector entities

Fragmented Threat Information

Malware evidence, CVE intelligence, and other threat indicators lacked unified context, slowing down statutory processes such as vulnerability assessments and warning notices

Solution

The authority integrated **Criminal IP TI** into daily operational workflows, establishing a reliable source of contextual intelligence that elevates both strategic oversight and individual case assessments.

Key capabilities include:

- **Accurate Locality Mapping** for identifying systems relevant to the state's area of responsibility.
- **Operator Attribution & Classification** for determining ownership and affected stakeholder groups.
- **In-Depth Threat Context** combining CVEs, malware history, passive DNS, and domain/IP reputation.
- **Holistic Case Assessment** supporting statutory processes that require complete situational context.

Criminal IP TI delivers the depth of analysis previously unavailable through legacy or procured tools, enabling analysts to conduct comprehensive evaluations rather than surface-level assessments.

Adoption

The deployment of Criminal IP Threat Intelligence led to measurable improvements in how external systems were identified, analyzed, and validated across the state's digital infrastructure.

Contextual Threat Scoring & Indicator Enrichment

Domains, IPs, and hostnames are automatically enriched with threat scores, malware intelligence, CVE analysis, and historical infrastructure context. This enables far more reliable evaluation than previously possible.

Enhanced Locality Verification

Location-aware intelligence allows analysts to distinguish state's systems from those outside the state's responsibility, reducing false classifications and enabling precise jurisdictional mapping.

Operator & Ownership Attribution

Criminal IP's WHOIS, behavioral metadata, and infrastructure history support improved identification of system operators, enabling faster differentiation between public sector and private sector assets.

Search-Driven Deep Investigation

Analysts use the Criminal IP search engine to perform detailed, case-bycase investigations, uncovering related infrastructure, historical behaviors, and hidden associations that were not previously detectable.

Unified Contextual Visibility

Criminal IP TI consolidates contextual factors—malware, vulnerabilities, operator data, locality, and threat indicators—into a single intelligence layer that supports statutory duties such as information notices, vulnerability management, and early warning processes.

Outcomes

The deployment of Criminal IP Threat Intelligence led to measurable improvements in how external systems were identified, analyzed, and validated across the state's digital infrastructure.

Key outcomes included:

- **Unified Contextual Visibility**
  Criminal IP TI consolidates contextual factors into a single intelligence layer that supports statutory duties such as information notices, vulnerability management, and early warning processes.
- **Greater Precision in System Identification**
  Improved locality and operator attribution reduce misclassified assets and enhance the accuracy of state-wide assessments.
- **Streamlined Statutory Processes**
  With richer context, analysts can more efficiently issue information or warning notices and conduct vulnerability management.
- **Holistic Risk Assessment**
  Analysts now maintain a comprehensive understanding of each system's risk posture, supported by unified threat scoring and contextual metadata.

WHY CRIMINAL IP?

With healthcare systems increasingly targeted by ransomware, phishing, and supply chain attacks, the organization's use of **Criminal IP TI** demonstrates how threat intelligence can be embedded into day-to-day operations to protect sensitive data, improve detection, and strengthen cyber resilience.

Powered by AI and OSINT, Criminal IP delivers threat scoring, reputation data, and real-time detection of a wide array of malicious indicators, **ranging from C2 servers and IOCs to masking services like VPNs, proxies, and anonymous VPNs**, across IPs, domains, and URLs. Its API-first architecture ensures seamless integration into security workflows to boost visibility, automation, and response.

Start your threat intelligence journey with a personalized demo of Criminal IP

Get your Demo