CROWDSTRIKE

THREAT INTEL PROGRAM DEVELOPMENT

Establish an effective threat intelligence program across your organization

UNDERSTANDING TODAY'S THREAT LANDSCAPE

Organizations need to determine the depth and breadth of the threat landscape by understanding how their organization could be targeted by adversaries. Many organizations simply don't understand the scale and impact of potential cyber threats, given the lack of relevant context to their business.

Security teams also struggle to keep pace with the latest and most relevant tactics, techniques and procedures (TTPs) used by adversaries, and how to implement effective security controls to defend against these types of attacks. These teams need to ensure that key lessons are learned from threat detections, and attacks can be attributed to likely adversaries and tactic classifications. The security team must also develop a strategy and repeatable process to apply threat intelligence to their cyber defenses.

ESTABLISH BEST PRACTICES FOR HIGHLY EFFECTIVE THREAT INTEL

The CrowdStrike® Threat Intel Program Development service helps organizations create or mature an existing threat intelligence program by incorporating the best practices of highly effective intel programs.

The methodology is based upon many years of combined consultant and practitioner experience, in conjunction with CrowdStrike's front-line incident response (IR) and threat intelligence expertise.

KEY BENEFITS

Maps your business, its critical assets and its attack surface to relevant adversarial behavior to understand the threat landscape and your organizational risk

Develops a tailored and informed governance model for threat intelligence to support your security operations in a sustainable manner

Defines priority intelligence questions and what threat information you should collect to answer those questions

Identifies which stakeholders will benefit from threat intelligence and how intel can inform their decisions through intelligence reporting

KEY CAPABILITIES

CrowdStrike partners with your team to develop a program that is tailored to your security organization, technologies and business needs to improve your security posture going forward. The Threat Intel Program Development service takes place over two phases.

PHASE 1 — Threat Intelligence Program Assessment: In this phase, the CrowdStrike Services team reviews existing documentation and conducts a threat intelligence workshop to discuss the program, identify the threat profile, determine intel requirements, and identify current maturity levels and improvement areas.

PHASE 2 — Program Development: In this phase, the Services team builds a program to support the prioritized recommendations for improvement identified in the first phase. Through workshops and iterative reviews, the team develops a framework for a threat intelligence program that is tailored to meet your organizational needs, guided by the four phases of the intelligence lifecycle: Planning and Direction, Collection and Processing, Analysis and Production, and Dissemination and Feedback.

The CrowdStrike Services team guides you through the assessment and development of a threat intel program to deliver:

- **Program scope and priorities:** Priority intelligence requirements that are relevant to the organization and stakeholder needs are defined.
- **Governance foundations:** A strategic governance model for threat intelligence is created to support your security operations in a sustainable manner.
- **Tactical insight:** The tactics needed to understand where and how threat information can be processed are identified to inform relevant intelligence reporting.
- **Operational resources:** Repeatable procedures are created and resources are defined to support threat intelligence operations along the intel lifecycle.

ABOUT CROWDSTRIKE SERVICES

CrowdStrike Services equips organizations with the protection and expertise they need to defend against and respond to security incidents. Leveraging the cloud-delivered CrowdStrike Falcon® platform — including next-generation endpoint protection, cyber threat intelligence gathering and reporting operations, and a 24/7 proactive threat hunting team — the CrowdStrike Services team helps customers identify, track and block attackers in real time. This unique approach allows CrowdStrike to stop unauthorized access faster and prevent further breaches. CrowdStrike also offers proactive services so organizations can improve their ability to anticipate threats, prepare their networks, and ultimately stop breaches.

Learn more at www.crowdstrike.com/services/

Email: services@crowdstrike.com

WHY CHOOSE CROWDSTRIKE SERVICES?

The CrowdStrike Services team leverages the power of the CrowdStrike Falcon® platform, CrowdStrike Intelligence and the Falcon OverWatch™ team to help organizations implement best practices for threat intelligence and threat hunting.

Expertise: Delivers unrivaled threat intel expertise and knowledge drawn from CrowdStrike IR, managed detection and response (MDR), and Falcon OverWatch™ threat hunting teams

Speed and precision: Enables immediate real-time visibility into your environment, identifying potential threats and visibility gaps to inform threat intel priorities

Methodology and approach: Provides expert security consulting, development of foundational intelligence practices, and awareness of emerging threats to support a reactive and proactive security organization