Threat Intelligence Security Center

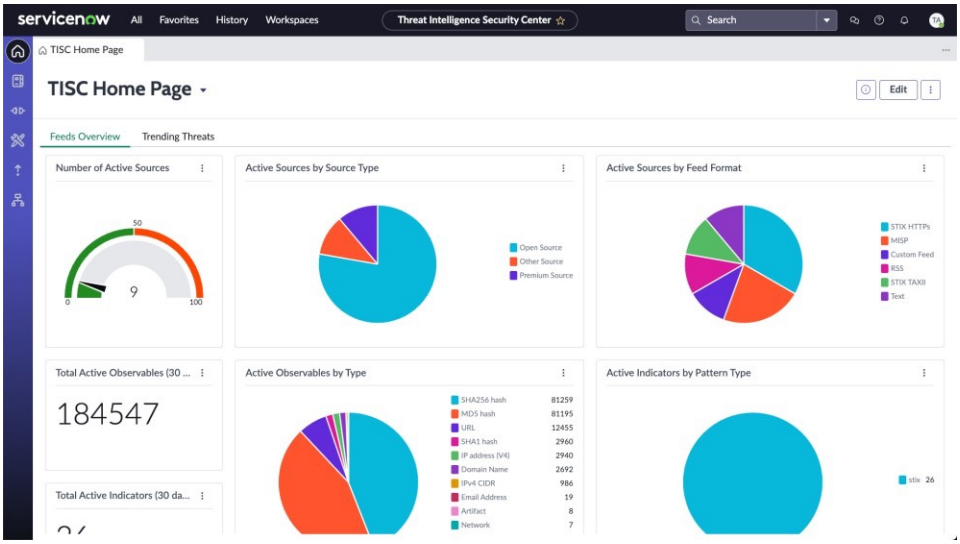
Stay Ahead of Threats and Attackers

Security teams sit at the frontlines of providing timely and accurate response to threats targeting their organization, while also defending their networks and assets daily. With limited availability of qualified resources- automation, orchestration, and AI-driven solutions are more important than ever in staying ahead of threats and vulnerabilities. At a time when personnel staffing problems are at their greatest, the antiquated idea of simply throwing resources at the issue isn't a viable solution. According to TechBeacon[1], this is not an issue reserved for large corporations…companies and organizations of all sizes are now faced with these difficulties:

- 70% of SOCs are in-house
- Nearly three-quarters of SOCs (74%) operate on a round-the-clock basis
- The ability to monitor cloud applications and endpoints are a key SOC requirement for security leaders
- Organizations rarely have the ability for multi-tier, more experienced personnel to get into things like investigation and threat hunting

Transform Threat Intelligence Management

ServiceNow Threat Intelligence Security Center (TISC) provides security teams with the necessary set of tools to create a Threat Intelligence driven security operations program. Threat Hunting, one of the key new capabilities in TISC, is the action of proactively searching to discover, identify, and isolate advanced threats that elude current security products and solutions to improve defensive posture. With a Threat Intelligence solution built directly into the ServiceNow platform, organizations achieve the ability to perform advanced threat intelligence actions such as hunting, modeling, analysis, and monitoring.



Threat Analyst Workspace
Centralized operations to perform threat modeling, threat hunting, and visualize threat intelligence in a purpose-built workspace for threat analysts

Integrations with Major Security Tools
Integrate with various TIPs, SIEMs, EDRs, Firewalls and other network intelligence solutions

Dashboards & Reporting
Persona-specific dashboards, insights, and reporting to measure and monitor progress against key metrics, and get real-time, actionable insights

Threat Intelligence Management
Data collection, aggregation, normalization, correlation, and enrichment from various sources, including SIR, MITRE ATT&CK, and CMDB

Threat Specific Playbooks
Scale team capacity and efficiency with threat intelligence specific automated actions and playbooks

[1] TechBeacon, https://blogs.opentext.com/category/technologies/security/

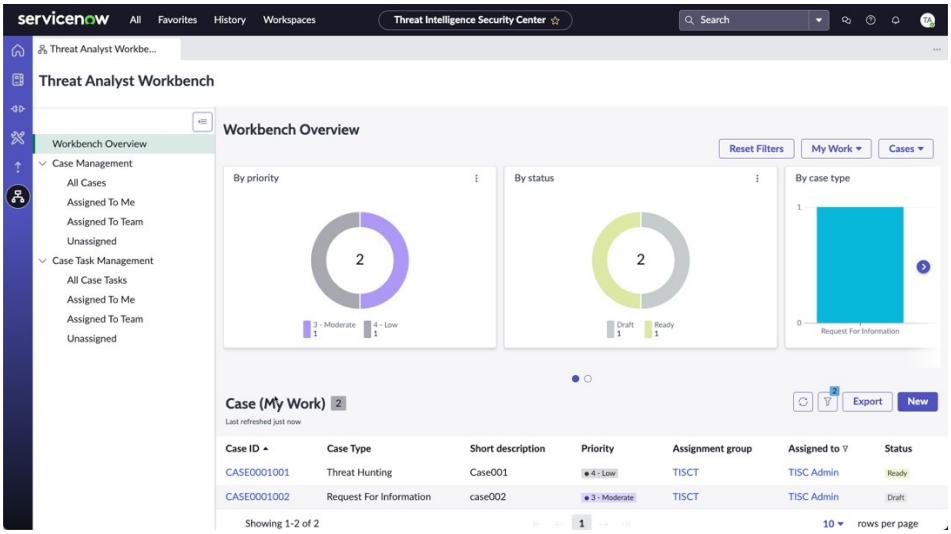
The Threat Intelligence Security Center further drives the maturity of an organization's security operations program by providing advanced capabilities for incident response, threat intelligence, and vulnerability response into one centralized platform. Cases and observables can be prioritized and worked based on assigned threat scores. Unlike most competitors' basic approach, the TISC Threat Score Calculator is a customizable, weighted calculation that can be tailored to deliver precise risk scores for observables, further adding in prioritization.

Use orchestration and automation to drive threat intelligence

Automation and orchestration help your workforce scale to succeed in an environment that is constantly changing and evolving. With the use of automation, Threat Analysts can eliminate basic, repetitive tasks, and aggregate, correlate and normalize data, freeing them to focus their efforts on more significant risks. By employing Inbound Filtering Rules, based on conditions or lists, administrators can curate a refined data stream to alleviate noise from various sources.

Integrate with major tools to get the data you need

Through both internal and external intelligence sources only achievable through TISC and our comprehensive suite of platform products threat teams can gain the necessary data needed to make timely and actionable decisions. ServiceNow TISC provides a seamless integration of external threat data with internal information such as affected Cis, vulnerabilities, and security incident data which is highly impactful. Integrations with a variety of security tools such as SIEMs provide additional resources for managers and analysts to gather pertinent data. Adding Threat feeds is also a simple task administrators can take to important data, with a curated list of popular data sources, easy to configure interface and support to popular and expanding list of feed formats.



Take Control of threats using a tailormade threat analyst workspace

Our case management feature empowers analysts to seamlessly create and oversee diverse cases, fostering collaboration across multiple teams and facilitating through threat investigations. With a dedicated Threat Analyst Workspace analysts can perform the daily tasks of threat analysis, hunting, correlation, and collaboration. Here analysts can view open cases and tasks assigned to them and track cases throughout their lifecycle from beginning to end. The TISC workspace also offers the ability to be modified and customized to meet each analysts' specific needs and requirements.

Gain valuable insight and visibility into your threat program

ServiceNow delivers the ability to quantify processes and capture key metrics and indicators to provide visibility into what is happening, what is working, and what could improve a program's performance. Built-in analytics, persona-specific dashboards, and reporting provide insight to leaders and analysts to identify trends and deficiencies.