ThreatConnect for Case Management

Continuously improve security processes with a single Platform for process documentation, team collaboration, and artifact enrichment.

The ThreatConnect® Platform provides a central location for security analysts and incident responders to record, analyze, and interact with all information related to the case at hand. ThreatConnect allows you to not only enrich cases with both internal and external threat intelligence, but also gives you the ability to generate intelligence from those cases to be added back into the Platform. This leads to a more complete picture and better understanding of your own internal threats. Creating a consistently running feedback loop ensures that you’re squeezing all the intelligence you can from all internal process and applying it for smarter decision making.

Workflow ensures your team follows documented processes with custom or ThreatConnect-built templates.

Defined Associations are done manually or automatically via Playbooks. By defining relationships that exists across Indicators, Groups, and Cases, you can begin to understand the complex patterns that exists across incidents.

Grouping Tasks into Phases allows you to create dependencies and increase process consistency.

Potential Associations happen when ThreatConnect suggests an association may exist without involvement from you or your team. Use these suggestions to manually define new relationships across Indicators, Groups, or other Cases.

Increase team collaboration and dialogue with the ability to add free form Notes to any Case.

As the Case progresses, Artifacts are automatically compiled and stored with relevant analytics provided via your native intel, external feeds, and CAL.

An auto-generated Timeline provides you with a recount of all activity happening in a specific Case.
ThreatConnect drives quicker response times with the following capabilities:

- **Completely Customizable Processes**
  Design Workflow templates or leverage ThreatConnect-built templates, then import those templates into your organization’s instance for further customization and usage.

- **Assign Tasks to Specific Analysts or Playbooks**
  Separate Workflows into manual or automatic tasks; including assigning users responsible for completing them as well as determining requirements and dependencies.

- **Automatic Task Completion and Artifact Creation**
  Automatically complete Tasks with Playbooks and save any relevant information back to the Case as artifacts for further usage and analysis.

- **Remove Silos By Linking Cases to Intel**
  When your Threat Analyst team is looking at a specific Threat Group or Indicator, they can see any previously closed or open cases related to that Group or Indicator. This allows them to understand the complex relationships that exist across Cases and Intelligence.

- **Provide Context and Insight into Artifacts**
  Leverage data from ThreatConnect’s CAL™ (Collective Analytics Layer) to gain more insight into intel-related artifacts such as IP addresses, emails, or URLs.

The combination of automation, orchestration, threat intelligence, and case management empowers your security team to:

- Improve response times with consistent and documented processes
- Reduce the risk of missing critical steps and relevant artifacts
- Decrease the time it takes to uncover relevant threat intelligence
- Maximize the amount of threat intelligence squeezed from day-to-day operations

**Request A Demo**

Call 1.800.965.2708 or visit threatconnect.com/request-a-demo