

Intelligence on Demand (Intel on Demand)



Real-time intelligence

Cybersecurity threats are more complex, targeted and persistent than ever, and many organizations face serious challenges when trying to protect their business. However, no matter how many tools, workflows, or automated processes you have in place, you still must rely on the intelligence you receive and your security analysts' ability to utilize that intelligence to identify and investigate threats. Security teams realize their analysts are overworked and some lack the expertise needed to properly examine, analyze, and synthesize intelligence in a timely manner. With the CTIR Intelligence on Demand Service, you receive up-to-date intelligence reporting on the latest threats or net-new custom research based on relevant contextual factors to help give your organization a differentiating edge against your adversaries.

With this service, you receive:

- Direct access to Talos Intelligence analysts who consult with you to provide in-depth review of the latest relevant research.
- Ability to request net-new custom research based on pertinent topics to your organization.
- Presentation of intelligence and insights delivered by a Talos Intelligence analyst.

Benefits

- Gain greater insight into intelligence details so your team can effectively drive change to better protect your organization.

Example topics

- Specific ransomware, malware, or threat actor overviews.
- Intelligence regarding specific exploits or vulnerabilities.
- Specific security best practices overview and an overview of the latest technologies available.

Case study

Challenges

- Large industry-wide cybersecurity event.
- Abundance of government and private-sector guidance.
- Unclear if the organization is at risk or affected.
- Unclear prioritization for mitigation.

Solution

- CTIR Intel on Demand.
- Intelligence briefing on current state of Talos knowledge.
- Specific indicators of compromise research in Talos global telemetry.
- Plan of action review based on government and private sector guidance.
- Review of product alerts.
- Prioritization of mitigation and responses with dedicated incident response consultant.

Outcomes

- Additional threat intelligence context for increased awareness and confidence.
- Identification of customer-specific prioritized actions or investments to take for maximum protection.
- Potential for compromise assessment or emergency response if research finds indications of compromise in customer telemetry.

Actionable information improves security

Your organization's preparedness to respond is critical when you are in the midst of an attack. But sometimes the intelligence you receive may not fully illustrate the vast complexity of your compromise. With this service, you ensure your team receives actionable information they can use to supplement in-house intel, so you bolster your security defenses. A Talos Intelligence analyst will work with you to confirm business objectives, determine logistics and uncover any additional background information they need to further research the topic at hand. Next, they will perform investigations using a variety of available telemetry and intelligence to collate their research in a consumable and actionable way. Once the research phase is complete, the Talos Intelligence Analyst will meet with you to deliver their findings.

Next Steps

To learn more about this service or the Cisco Talos Incident Response Retainer, please contact your account team or visit the [Talos Incident Response web page](#) for more information.