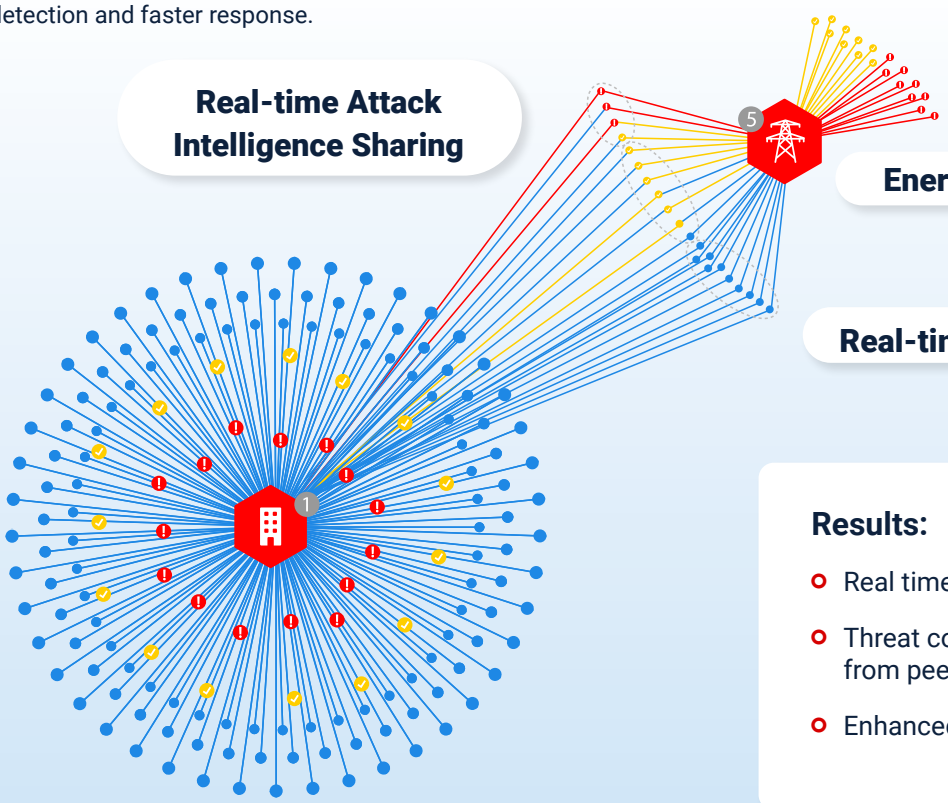
Protecting Energy Infrastructure through Collective Defense

IronNet Cybersecurity **for the Energy Sector**

As the ransomware attack on the Colonial Pipeline made clear, today's critical energy infrastructure depends on cybersecurity solutions that can detect threats early in the intrusion cycle and in real-time. The traditional approach to securing the energy sector, enterprise by enterprise, is transforming. The partnership, collaborative model used for rapid response to weather events is just as crucial for defending against cyber criminals and nation-states in the form of what Southern Company's CISO Tom Wilson calls "cyber mutual aid."

By bringing together the interconnected energy ecosystem in a collaborative community, IronNet's Collective Defense platform provides a secure environment that serves as an early warning system for all members through real-time, correlated detections of new and unidentified cyberattack behaviors. The Collective Defense Community for the Energy Sector also enables real-time collaboration on attack intelligence. Together, threat detections based on behavior analytics and crowdsourced insights provide enhanced visibility across the energy sector's entire attack landscape. The result: faster detection and faster response.



Results:

- Real time discovery of threats
- Threat correlation and insights from peer-SOCs
- Enhanced SOC prioritization

> As we work with IronNet and our other partners, I look forward to more international companies joining us in the spirit of Collective Defense...to give companies more situational awareness of what's happening around the globe and address threats collectively.
>
> – TOM WILSON, VP AND CISO, SOUTHERN COMPANY

> We see IronNet as complementary to our efforts with the O&G ISAC and have bought into the vision of collective defense to better protect ourselves and our sector."
>
> – CISO, FORTUNE 500 ENERGY COMPANY

The IronNet **Difference**

Collective Defense comprises IronDefense for network detection and response and IronDome, for real-time, operational attack intelligence sharing. IronNet's Collective Defense platform complements other sources of threat intelligence such as the E-ISAC and the ONG ISAC, by providing real-time, contextualized attack intelligence that can be integrated with SOC software ecosystems to improve operational agility.

What is the difference between **Collective Defense** and traditional threat sharing groups?

- Be able to answer the question “What is happening now?” in real-time via Collective Defense, which also provides the ability to collaborate (via rating/comments) vs. the standard timeframe: incident happened, time-consuming research conducted, sanitization, sharing via more manual methods.
- Leverage real-time attack intelligence to gain visibility into what is currently happening and what already has happened. Through Collective Defense, IronNet's IronDome delivers more coverage and more resources with less effort.
- Access underlying threat detection data using Collective Defense across all community participants vs. the sharing of signature-based threats.
- Obtain alerts on attack intelligence, via IronDome, for threats that are actually affecting your organization vs. receiving threat intelligence feeds.
- Understand clearly what analysts across the Collective Defense community are actually investigating and drive collaboration before, during, and after an attack vs. the practice of collaborating after an investigation is complete.
- Gather situational awareness that is fundamental to new attack/campaign discovery for detections humans have not seen and alert analysts to campaigns against their industry, supply chain, etc. vs. less specific data around detections of unknown threats.
- Enable SOCs to understand how triaging a specific alert has broader impact than their organization alone vs. responding on an organization by organization basis.

Your SOC multiplied by the power of 100s of analysts, from different industries working with you:

Accelerate investigations by instantly sharing community threat insights and event ratings

See real-time alerts of emerging campaigns

Integrate seamlessly with the IronDefense system for enhanced alert fidelity and prioritization

Take advantage of anonymized sharing with governments, when necessary, for national response

IronDefense

Superior behavioral detection

IronDefense uses proven analytics based on machine learning and artificial intelligence techniques used in real-world defense against sophisticated cyber criminals and nation-state-level threat actors.

Unparalleled scalability

IronDefense scales from small companies to Fortune 100 companies to deliver unmatched detection of threats at enterprises of all sizes.

Real-time visibility

IronDefense works with IronDome Collective Defense solution to deliver dynamic, real-time visibility to threats targeting the supply chain, industry, or region.

End-to-end visibility across environments

IronDefense leverages a broad range of cloud-deployed sensors for public/private cloud, virtual networks, and on-premise networks to help secure infrastructure and provide the flexibility to accommodate distributed teams.

IronDome

Real-time visibility and threat detection

IronDome leverages proven analytics, machine learning (ML), and artificial intelligence (AI) techniques across anonymized participant data to identify threats that may be missed by an individual enterprise.

Reduce the negative impact of a cyber attack

With help from fellow cyber defenders, IronDome enables participants to automatically share real-time detections, triage outcomes, and threat indicators with community members. When suspicious behaviors are identified by any member, IronDome automatically shares a proactive warning to all members.

Improve effectiveness existing cybersecurity investments

Participants receive threat insights and prioritized Indicators of Compromise (IoC) from the IronDome community. This information can be used by their existing network, endpoint, or other security tools to identify and stop adversaries from retargeting their attack.