IronNet™

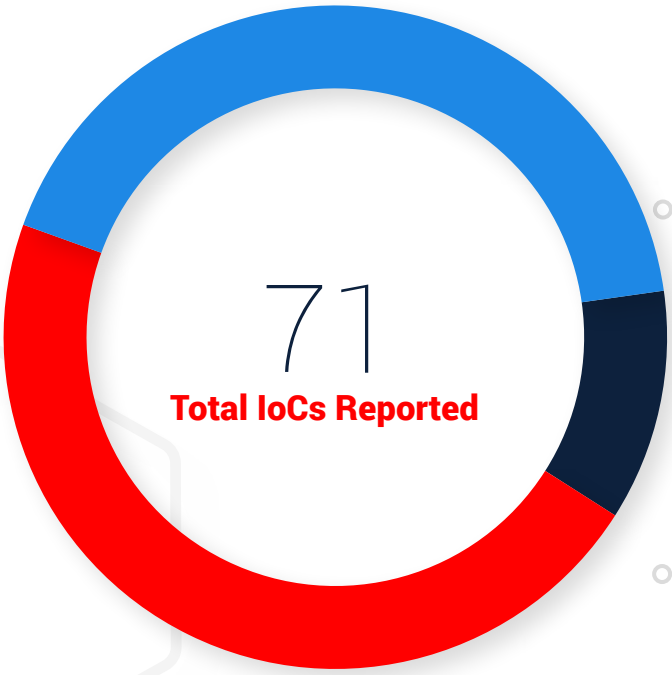
Edition #13: January 2021

IronNet:
Threat Intelligence Brief

Top Observed Threats from IronNet Collective Defense Community
December 1 – December 31, 2020

Significant **Community Findings**

This month, IronDefense deployed across IronDome participants' environments identified a number of network behavioral anomalies that were rated as Suspicious or Malicious by IronNet and/or participant analysts.



C2:
30 IoCs

Access
8 IoCs

Other:
33 IoCs

Recent Indicators of Compromise

Domain/IP	Rating	Analyst Insight
avsvmcloud[.]com	MALICIOUS	This is a known-bad domain that was used for command and control (C2) communications in the SolarWinds SUNBURST attack. For more information about SolarWinds, please see this blog post on IronNet's website.
downlinks[.]me	SUSPICIOUS	This domain is known to host malicious files. If seen in your network, we recommend investigating for any successful file downloads.
idorenu[.]top	SUSPICIOUS	This domain has been labeled Malicious by multiple antivirus engines due to its relation to spyware. The domain supplies JavaScript that reports back referred webpages via xmlhttprequest. This could be the result of adware within a recently downloaded program or browser extension.
letsmakeparty3[.]ga	SUSPICIOUS	The presence of this domain in your network traffic could indicate that a user has visited a hacked WordPress site. If seen in your network, investigate for any unwanted redirections and block the domain.
66.96.147[.]144, dealctr[.]com	SUSPICIOUS	The presence of these IoCs on your network may indicate that an unwanted application has been installed. The application is related to the Google Chrome/Mozilla Firefox extension Oxford Dictionary and can exfiltrate inputted URLs. If seen in your network, we recommend blocking the domain and investigating the associated endpoints.
ein-gov-online[.]com	SUSPICIOUS	After researching multiple OSINT resources, the IronNet Hunt team determined that ein-gov-online[.]com and e-filings[.]us are phishing sites. Although there is a disclaimer that states the website is not affiliated with the IRS, it provides a phone number and link to a breast cancer clinical trial site (breastcancer-clinicaltrials[.]com) which is also phishing for information. These are the typical patterns of phishing sites and they should be blocked.
gnogle[.]ru	SUSPICIOUS	According to OSINT resources, this domain has a malicious reputation. It is unclear if the user sent credentials or downloaded malicious content as the PCAP had aged off by the time of alert triage. If activity to this domain is seen in future traffic, it should be investigated extensively.
182.127.161[.]91	SUSPICIOUS	This IP address is related to scanning activity from the Mozi botnet. The Mozi botnet is a rapidly-growing peer-to-peer (P2P) malware largely targeting Internet of Things (IoT) devices.
ajax[.]googapi[.]com	SUSPICIOUS	This activity is related to the MageCart credit card skimming campaign. A JavaScript associated with this domain sends purchase-related details to the domain via POST requests.
xmax88[.]com	SUSPICIOUS	This domain is associated with phishing sites targeting Microsoft account holders.

Threat Rules Developed

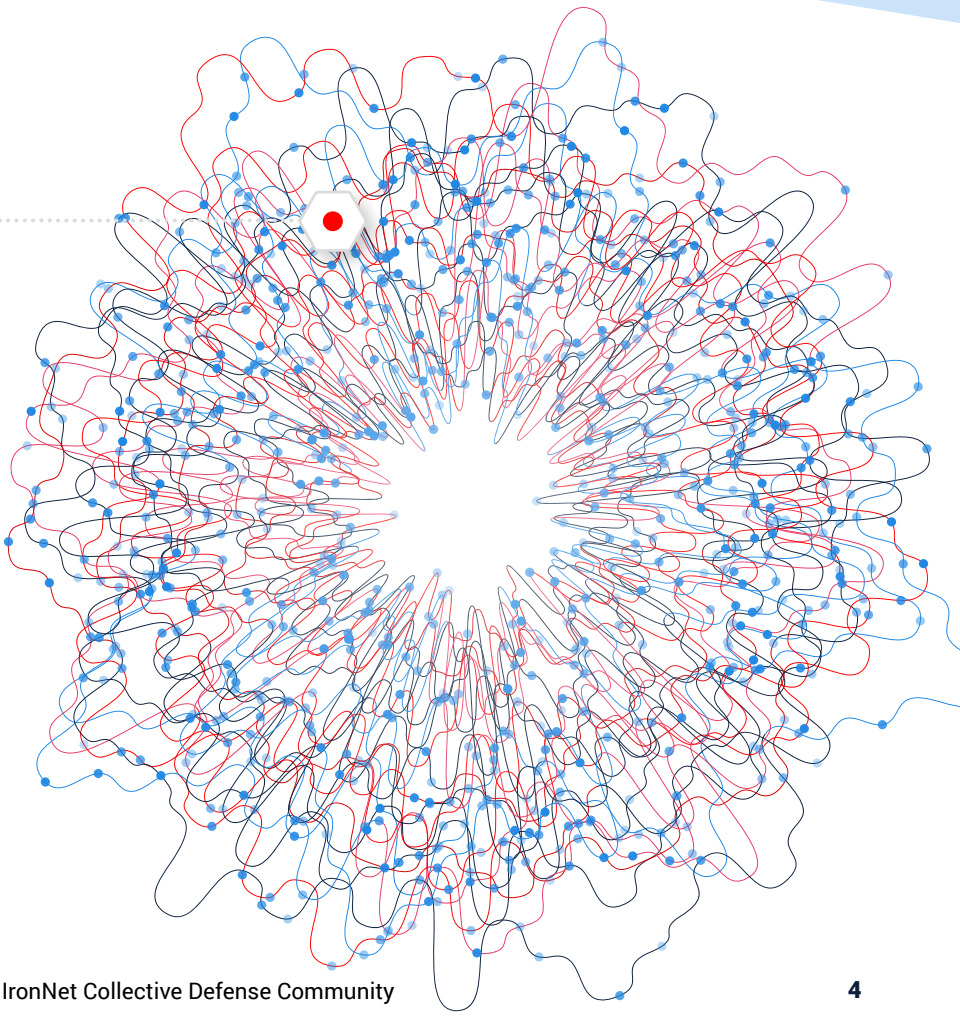
Every month, IronNet's expert threat analysts create threat intelligence rules (TIRs) based on significant community findings from IronDome, malware analysis, threat research, or other methods to ensure timely detection of malicious behavior targeting an enterprise or other IronDome community participants. These TIRs are continually distributed to each IronDefense deployment as they are created, ensuring that customers receive the most up-to-date detection capabilities.

7,829

Threat Intel Rules Developed This Month

172,887

Threat Intel Rules Developed to Date



THREAT RULES DEVELOPED

This month's threat intelligence rules include signatures looking for Indicators of Compromise as identified by IronNet analytics including Domain Generation Algorithm, Domain Analysis HTTP, and Suspicious File Download. Additionally, rules were created for indicators identified by the IronNet Threat Research team as associated with phishing or malware delivery. Finally, IronNet threat intelligence analysts routinely monitor research distributed by the wider cybersecurity community and ensure rules are created for documented indicators. Some examples of this month's research include:

- Identifying domains spoofing the World Health Organization and an associated phishing campaign delivering malicious Java attachments
- Tactics, techniques, and procedures (TTP) and command and control infrastructure associated with Egregor and Prolock ransomware campaigns
- Details on a cryptocurrency mining botnet dubbed Xanthe, which has been observed exploiting Docker installations with an exposed web API
- Analysis of the malicious tools used by the Iranian Ministry of Intelligence and Security (MOIS) front company Rana Corp, which was identified as the APT39 group
- Identification of social engineering and malware propagation sites used by Vietnam-linked APT32/ OceanLotus
- Details on a recent Linux-based cryptocurrency mining botnet, dubbed PGMiner, that exploits PostgreSQL database servers for cryptojacking
- Indicators associated with recent phishing campaigns attributed to the Russia-linked Gamaredon group
- Analysis linking the recent Pay2Key ransomware campaign to the Iranian Fox Kitten APT group
- Details on a credential stealing campaign leveraging the AutoHotkey (AHK) scripting language
- Indicators associated with the wAgent and Bookcode malware being used by the North Korea-linked Lazarus group
- Analysis of a Negasteal (also tracked as Agent Tesla) malware variant observed using Hastebin, an open source Pastebin alternative, to deliver the Crysis (also known as Dharma) ransomware
- Identification of a new campaign conducted by the criminal group UltraRank targeting e-commerce websites using JavaScript-scraping attacks

This Month in the IronDome

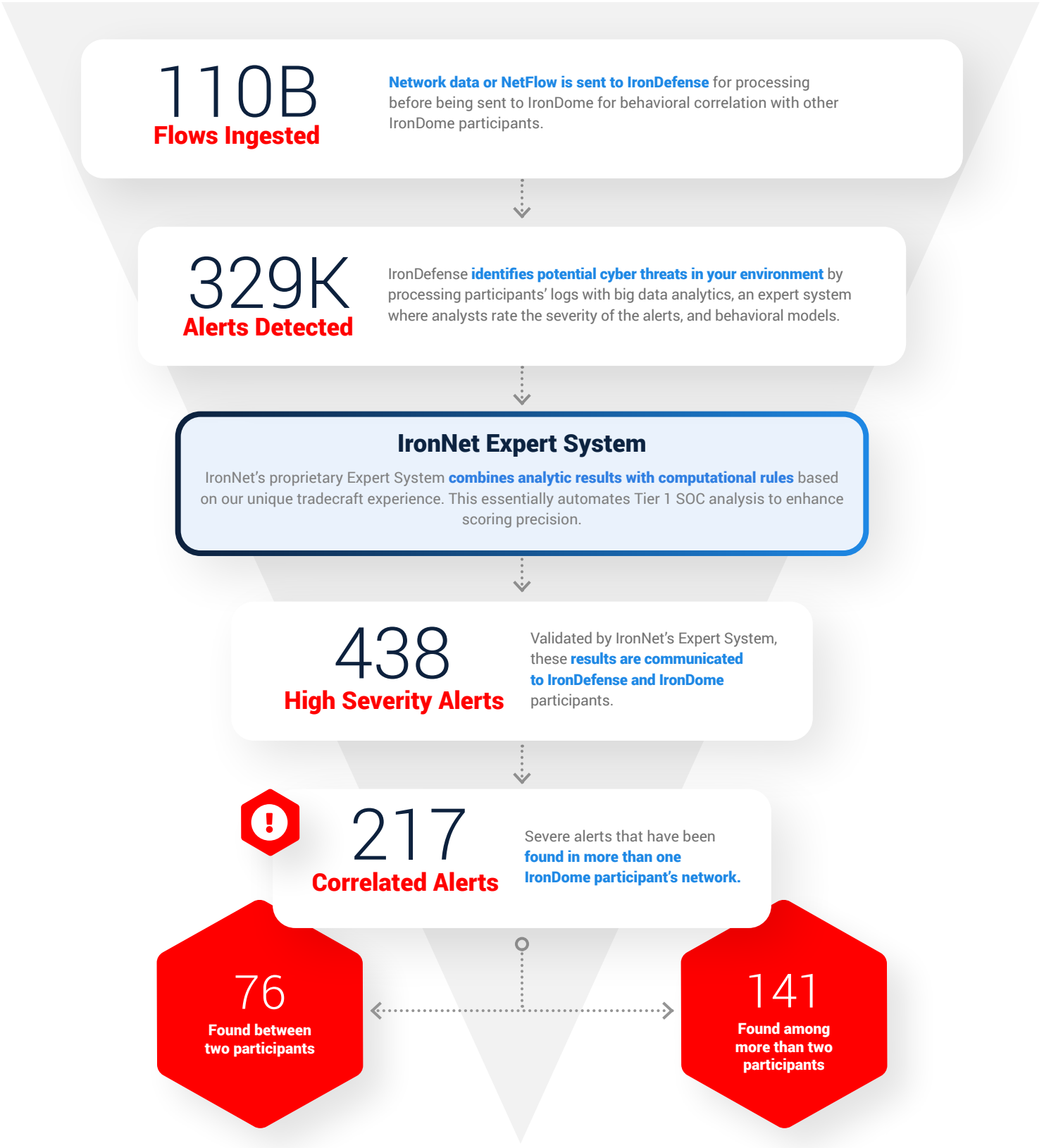
The IronDefense network detection and response solution detects behavior-based anomalies as follows:

- The NetFlow or enriched network metadata (“IronFlows”) collected by IronNet sensors is analyzed by a participating enterprise’s IronDefense instance before being sent to IronDome for higher order analysis and correlation with other IronDome members.
- IronNet’s IronDome Collective Defense platform delivers a unique ability to correlate patterns of behavior across IronDome participants within an enterprise’s business ecosystem, industry sector, or region.

This ability to analyze and correlate seemingly unrelated instances is critical for identifying sophisticated attackers who leverage varying infrastructures to hide their activity from existing cyber defenses.

On the following page is a snapshot of this month’s alerts.

Monthly Alert Snapshot



Tracking **Industry Threats**

Russian Actors Breach SolarWinds, FireEye, and U.S. Government Agencies

Information regarding a series of high-profile intrusions has come to light. On December 8th, the U.S. cybersecurity company FireEye disclosed that it was the victim of a sophisticated network breach resulting in the theft of software tools used by FireEye's Red Team to test and assess their customers' security. FireEye simultaneously released various signatures to assist in detecting or blocking the tools that they believe were stolen. These tools appear to exploit well-known vulnerabilities that recently have been used by state-sponsored threat actors. The concern is that the threat actors would use these tools in an attempt to mask or disguise their true identity during future intrusions.

On December 13th, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued an alert indicating that SolarWinds Orion Platform software was being actively exploited by malicious actors. The Department of Homeland Security (DHS) issued an emergency directive instructing U.S. federal agencies to immediately disconnect all SolarWinds Orion products. FireEye also published technical details indicating that a software supply chain compromise which occurred earlier in 2020 resulted in a Trojanized version of SolarWinds Orion being distributed to customers, which they have dubbed SUNBURST. Media reporting has linked the SolarWinds compromise to the previously reported FireEye breach and has attributed these compromises to threat actors associated with Russian intelligence services, specifically APT29 (also tracked as Cozy Bear).

While information on these intrusions is still incomplete, IronNet is taking proactive steps to ensure the security of our internal networks and our customers' networks. IronNet hunters have conducted targeted queries to identify any recent network traffic associated with both historical APT29 IoCs and the SUNBURST backdoor. We have also deployed signature-based rules designed to alert on any future activity associated with known historical APT29 IoCs, the compromised FireEye Red Team tools, and the SUNBURST backdoor.

SolarWinds Breach Continues to Evolve

Numerous reports about the SolarWinds software supply chain breach have been published, providing additional details into this wide-ranging and sophisticated intrusion campaign. Information provided by SolarWinds indicates that up to 18,000 of their customers may have been affected. While the Trojanized version of SolarWinds' Orion software (dubbed SUNBURST or Solorigate) appears to have been distributed between March and May of 2020, one report suggests that the threat actors behind the breach may have had access to SolarWinds' network as early as 2019.

Additional research indicates that the threat actors behind these intrusions have also utilized techniques to abuse authentication services. These tactics were cited in an alert from CISA as well. To further complicate matters, research from Microsoft and Palo Alto have described a second piece of malware, tracked as SUPERNOVA, that affects SolarWinds Orion but is distinct from SUNBURST.

As these points illustrate, the cybersecurity community's understanding of these events is still evolving. IronNet is actively tracking these developments. We are cataloging new and emerging information about this campaign, and are using it to run targeted queries, build and deploy signature-based detections for known Indicators of Compromise, further analyze the related malware, and review the adversarial techniques involved to refine and enhance our behavioral analytics.

Vietnam-linked APT Uses Cryptomining as "Distraction" Technique

An analysis of an intrusion attributed to the Bismuth group (also tracked as OceanLotus and APT32) has revealed some novel tradecraft techniques. During the summer of 2020, Bismuth, which is believed to be a Vietnamese state-sponsored threat, was observed deploying cryptocurrency miners to victim systems during the course of campaigns targeting commercial and government sector entities in France and Vietnam. As cryptocurrency mining is typically not associated with sophisticated state-sponsored threats, the tactic may serve to distract network defenders from the threat actors' more invasive actions or true intent.

The Bismuth actors operated very deliberately, initiating their attacks with targeted email phishing, then spending upwards of a month performing network discovery after they gained a foothold within the victim organization. They would then attempt to move laterally to deploy additional tools on higher value systems.

Multi-faceted and deceptive attacks such as these underscore the value of comprehensive, behavior-based detection, which can assist cyber defense analysts in identifying activity that may otherwise go undetected. IronDefense implements multiple analytics specifically designed to identify techniques such as those observed during this campaign, to include phishing, suspicious downloads, and lateral movement.

SystemBC RAT Linked Ransomware Attacks

British security company Sophos issued a report in December detailing ransomware operators' use of the SystemBC Remote Access Trojan (RAT), which has been linked to recent Ryuk and Egregor ransomware attacks. The malware has been in use since 2019 and is typically bought and sold via criminal forums using a Malware-as-a-Service model. Of note, researchers discovered that newer versions of SystemBC leverage the TOR anonymization network to encrypt and conceal the destination of command and control traffic. Other malware, such as CobaltStrike, Bazar, and ZLoader, were also used by the same actors in combination with SystemBC.

Malware-as-a-Service models have become increasingly popular in recent months. Preventing, detecting, and recovering from such attacks requires a multi-pronged defense-in-depth strategy including robust network traffic analysis, endpoint monitoring, and backup solutions.

Ransomware: New Year, Same Story

A review of 2020's high-profile cybersecurity events shows how ransomware was the dominating threat over the past year. The total volume of attacks and the total costs to victims have grown exponentially over the past couple of years. 2020 saw a wide variety of sectors targeted for extortion, including hospitals, schools, energy companies, and contractors, among others.

Underscoring the fact that such attacks are almost certain to continue unabated into the new year, the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) issued an alert on December 28th warning of scams related to COVID-19 vaccine research. FinCEN indicated they were "aware of ransomware directly targeting vaccine research," and urged financial organizations involved in vaccine manufacturing and delivery operations to remain vigilant of such threats.

The most effective strategy for countering ransomware attacks is to detect the intruders before they can steal or encrypt an organization's data. IronDefense analytics detect many of the behaviors that represent precursors to such attacks and also leverage open source intelligence to identify known command and control nodes. These known-bad indicators comprise over 1,300 signature-based rules currently deployed in the IronDefense platform.

Why **Collective Defense?**

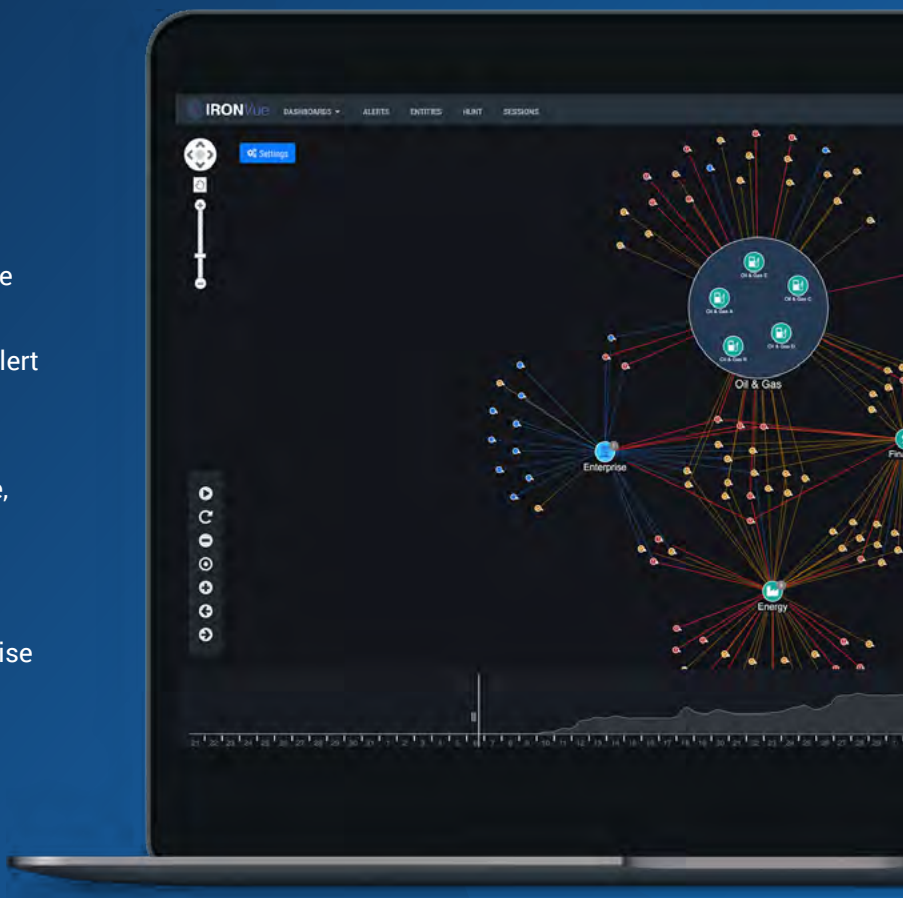
> **IronDome enables us to proactively defend against emerging cyber threats by uniquely delivering machine speed anomaly detection and event analysis across industry peers and other relevant sectors."**
>
> **— CISO, Industry-Leading North American Energy Company**

This report features threat findings, analysis, and research shared across IronDome, the industry's first Collective Defense platform for sharing network behavior analytics and intelligence detected between and across sectors, states, and nations so IronDome participants can work together in near-real-time to collaboratively defend against sophisticated cyber adversaries.

Your Partner in Collective Defense

IronNet's goal is to strengthen Collective Defense by detecting unknown threats using behavior-based analysis, rating these threats to reduce "alert fatigue," and sharing them within the IronDome ecosystem to empower SOC teams across the community to prioritize and accelerate response, and defend better, together.

By working together in this way, we can raise the bar on cybersecurity defense at your enterprise or organization, across sectors at large, and on behalf of nations.



Learn more about Collective Defense in our eBook.

ACCESS THE BOOK →

IronNet™

IronNet.com