IronNet

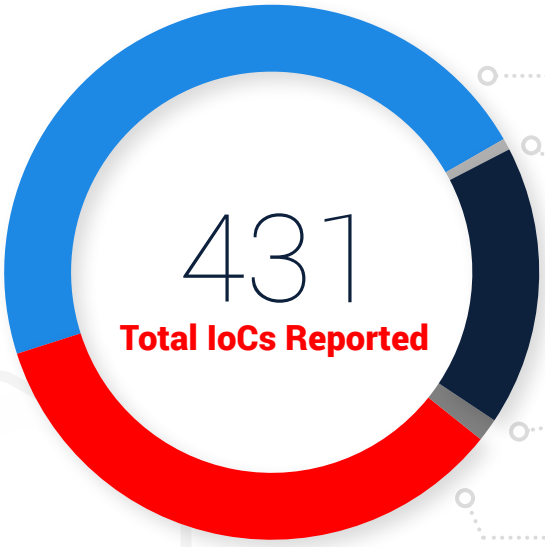
Edition #27: March 2022

IronNet:
Threat Intelligence Brief

Top Observed Threats from IronNet Collective Defense Community
February 1 – February 28, 2022

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.



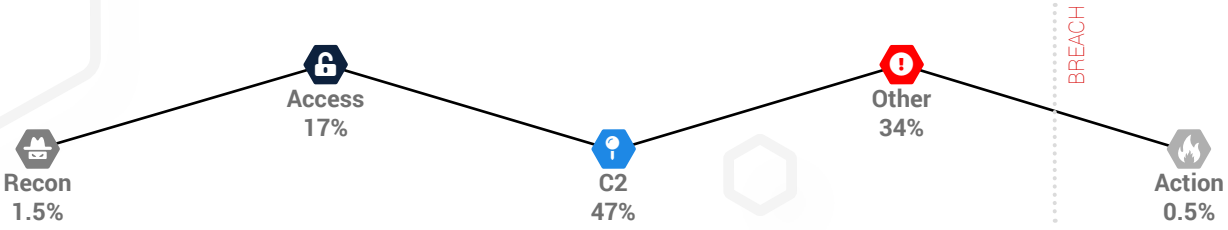
C2
201 IoCs

Action
3 IoC

Access
73 IoCs

Recon
6 IoCs

Other
148 IoCs



Recent Indicators of Compromise

Domain/IP	Rating	Analyst Insight
findquickresultsnow[.]com	MALICIOUS	This is a parked domain that contains associated malicious files, such as Trojans. We recommend blocking this domain.
0g3wn9mr3cab[.]top	MALICIOUS	This is potentially an Apple-themed phishing attack. We recommend blocking the domain.
wcomhost[.]com	MALICIOUS	At the time of triage, the full URI 046f38b.wcomhost[.]com that was accessed by the client appeared to host a legitimate financial institution site. However, the site is actually a copy of novel[.]mn, a domain that hosts fake account login pages to lure clients into inserting personally identifiable information (PII) into form fields. We recommend ensuring no PII was entered within form fields and blocking the domain.
73dkt-vwrqs[.]xyz	MALICIOUS	After investigation, the domain was determined to have malware attached to it. We recommend blocking this domain.
shopsvip4a[.]cf	SUSPICIOUS	This is a potential scam merchant site that did not resolve during triage. We recommend using caution when browsing this site.
ccloswx[.]xyz	SUSPICIOUS	This domain redirected the user to a deceptive social media page. Interactions may result in downloads of unwanted software or social engineering. We recommend blocking the domain.
planeta-nk[.]ru	SUSPICIOUS	This domain redirects users through multiple domains and stops at a Google Play store page. VirusTotal shows that multiple vendors have reported malware being associated with this domain. We recommend investigating traffic and blocking the domain.
aurumship[.]com	SUSPICIOUS	This domain has historically hosted sites used to bait users into downloading malicious PDFs and other file types. We recommend blocking the domain.
claspedtwelve[.]com	SUSPICIOUS	This is a Terraclicks-related domain. Terraclicks is a browser redirector known to redirect to malicious sites. We recommend investigating traffic and blocking the domain.
fadedcovertrefuse[.]com	SUSPICIOUS	This is a Terraclicks-related domain. The IP associated with this domain has been linked to malicious files as recently as February 19, 2022. We recommend investigating traffic and blocking the domain.

Threat Rules Developed

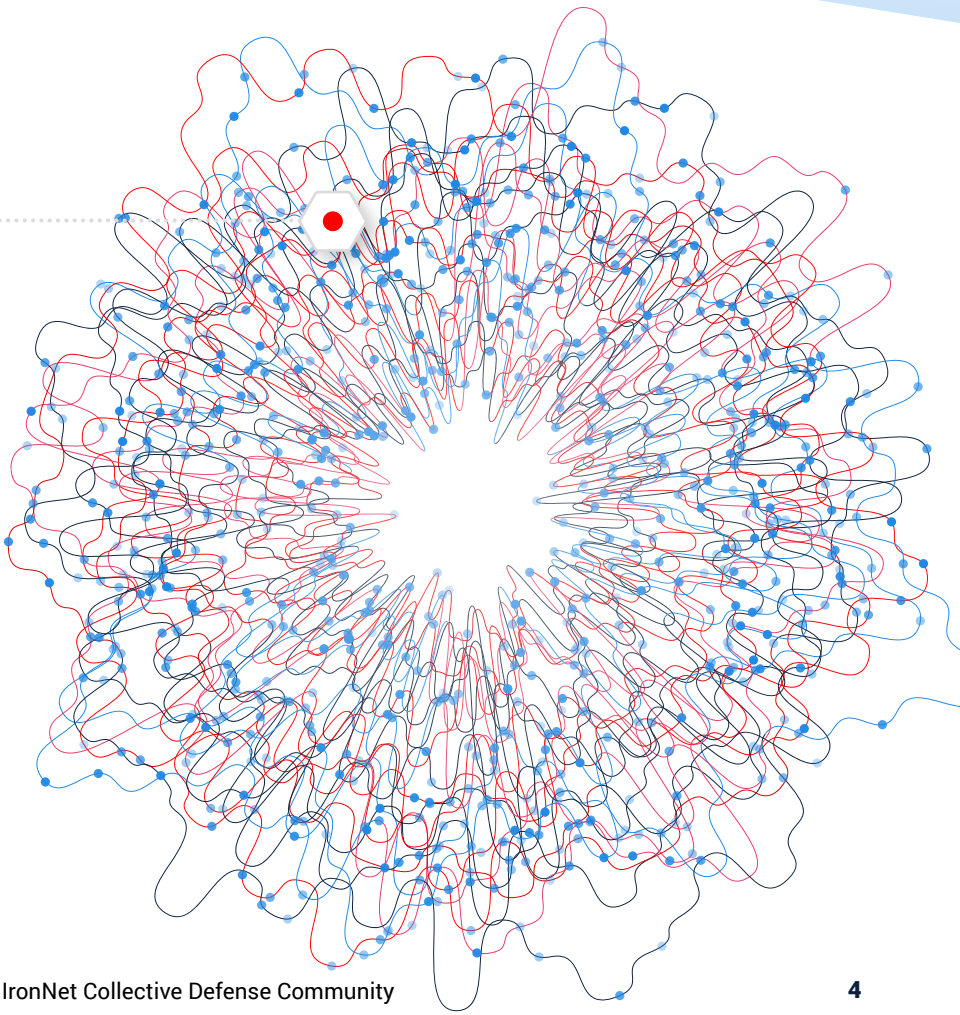
Every month, IronNet's expert threat analysts create threat intelligence rules (TIRs) based on significant community findings from IronDome, malware analysis, threat research, or other methods to ensure timely detection of malicious behavior targeting an enterprise or other IronDome community participants.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

4,388

Threat Intel Rules Developed This Month

298,297

Threat Intel Rules Developed to Date



THREAT RULES DEVELOPED

This month's threat intelligence rules include signatures looking for Indicators of Compromise identified by the IronNet Threat Research team as associated with phishing or malware delivery. IronNet threat intelligence analysts also 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 indicators associated with the following threats and campaigns:

- IoCs related to Cobalt Strike beacon payload distribution and Command and Control (C2)
- Malware delivery domains for Gafgyt, DarkStealer, Emotet, Quasar, and DDoSTF malware
- IoCs related to the Gamaredon threat group
- IoCs related to the ModifiedElephant threat group
- IoCs related to the Russian APT Gamaredon
- IoCs related to the Russia-Ukraine conflict from CERT Orange Cyberdefense
- IoCs related to the Evil Corp cybercrime group and Emotet malware

This Month in the IronDome

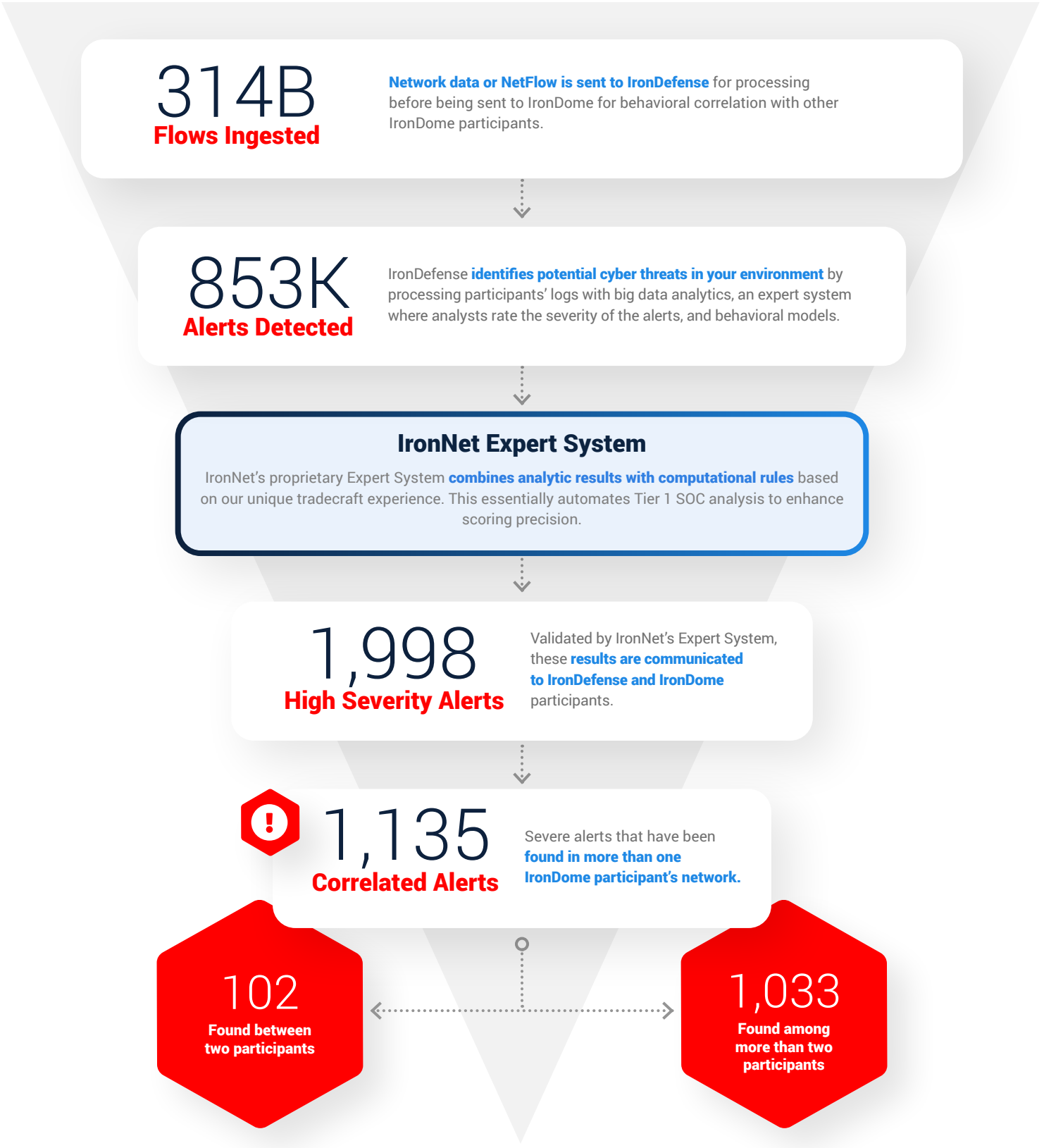
The IronDefense network detection and response solution detects behavior-based anomalies as follows:

- 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



Top Most Frequent Behavioral Analytics

IronDome's unique cross-sector visibility and Collective Defense capabilities highlight each month's most frequent behaviors, enabling us to track trends over time.

- Data Exfiltration 55.9%
- New and Suspicious Domains 11.7%
- Credential Phishing 9.6%
- DNS Tunneling 9.3%
- External Scanning 6.8%
- C2 Rendevous (DGA) 4.7%
- Beaconing 1.4%
- Suspicious File Downloads 0.6%

Tracking Industry Threats

Gamaredon Targets Ukrainian Organizations

In the past week, a series of reports have been released detailing recent Russian state-sponsored cyber activity by the Gamaredon threat group targeting Ukrainian organizations. Palo Alto's Unit 42 report gives insight into two recent Gamaredon (aka, ACTINIUM, Primitive Bear, Shuckworm) phishing attempts. One targeted the State Migration Service of Ukraine on December 1, 2021 using a Word document as a lure to install the open-source UltraVNC virtual network computing (VNC) software for maintaining remote access to infected computers. The other phishing attempt took place on January 19, 2022 and targeted an unnamed Western government entity operating out of Ukraine. In this attempt, rather than emailing the downloader directly to their target, the actors instead leveraged a job search and employment service within Ukraine. In doing this, the threat actors searched for an active job posting, uploaded their downloader as a resume, and submitted it through the job search platform to the Western government entity.

In addition to this report by Unit 42, Microsoft released a report on February 4, 2022 detailing additional Gamaredon attacks. Since October 2021, Microsoft has observed Gamaredon targeting Ukrainian organizations in sectors such as government, military, law enforcement, non-profit, and NGOs, which are organizations that are vital to emergency response and security in Ukraine, as well as organizations that coordinate humanitarian and international aid in Ukraine during a crisis. Microsoft states the primary goal behind these attacks over the last six months is to exfiltrate sensitive information, maintain access, and to move laterally into related organizations.

Unit 42 observed an interesting approach used by Gamaredon when it came to building and maintaining its infrastructure. Most actors choose to discard domains after using them in a campaign to distance themselves from any possible attribution, but Gamaredon appears to recycle their domains by consistently rotating them across new infrastructure. Altogether, Unit 42 observed both new

and old domains leveraged by the group, and mapped out three large clusters of currently active infrastructure used by Gamaredon to support its various phishing and malware campaigns. These clusters link to over 700 malicious domains, 215 IP addresses, and over 100 samples of malware.

Similar to Unit 42, Microsoft determined Gamaredon maintains a lot of variation of its operational infrastructure to evade detection, including many domains and hosts to facilitate payload staging and C2. In a single 30-day snapshot, Microsoft saw Gamaredon utilizing over 25 new unique domains and over 80 unique IP addresses, demonstrating that the group frequently modifies or alters its infrastructure. All in all, these reports show that Gamaredon is staying very active and is consistently updating its tactics and infrastructure to stay under the radar and target various Ukrainian entities.

Russia-Ukraine Conflict Update

Russian troops continue to amass at the Ukrainian border; there are 130,000 reported troops stationed around Ukraine. Russia has deployed ground forces, Battalion Tactical Groups (BTG), naval warships, air forces, missiles, and supplies to various locations surrounding Ukraine, including the Russia-Ukraine border, Crimea, Ukraine's Donbas separatist area, Belarus, the Black Sea, the Sea of Azov, and more. Troops are also reportedly moving out of staging areas toward combat positions as Russia builds up capacities. Analysts are concerned that the most recent movements indicate a possible Russian invasion within a matter of hours or days.

IronNet continues to closely track the situation and monitor possible implications for our partners. During this time of escalated risk, IronNet urges partners to take necessary precautions, including determining shift schedules for the week, ensuring offline backups, securing out-of-band-communications, and fortifying standard operating procedures (SOP).

GRU DDoS Attacks on Ukrainian Websites

On February 15, 2022, Ukraine's Center for Strategic Communications and Information Security reported that the Ministry of Defense, the Armed Forces of Ukraine, and two of the country's state-owned banks, Privatbank (Ukraine's largest bank) and Oschadbank (the State Savings Bank), were hit by a "powerful DDoS attack on a number of information resources."

The DDoS attacks consisted of three times more traffic than typically observed, 99% of which were HTTPs requests. The DDoS attacks caused interruptions in the Ukrainian Defense Ministry and the Armed Forces sites and made it difficult for bank customers to login to their online banking accounts. Privatbank's web application firewall (WAF) was also updated with a traffic geofencing rule, which automatically removed the site's contents for IP addresses outside of Ukraine and displayed a message reading: "BUSTED! PRIVATBANK WAF is watching you."

U.S. and U.K. governments recently linked the DDoS attacks to Russia's Main Intelligence Directorate, the GRU. Government officials were able to attribute the attacks because GRU infrastructure was observed transmitting high volumes of communications to IP addresses and domains based in Ukraine.

Luckily, the direct impacts of these attacks are low. Though the availability of the data was temporarily compromised, the victims were able to quickly restore access within a few hours, and no information was stolen or altered. However, the intended goal of these attacks was not solely disruption, but rather was more psychological in nature. Considering the ongoing conflict between Russia and Ukraine, the DDoS attacks are likely part of a broader Russian campaign aiming to show Ukraine that it has the capability to overwhelm government systems and possibly conduct even more disruptive or damaging cyberattacks.

Russia Declares War on Ukraine

On February 24th, Russian President Vladimir Putin declared war on Ukraine and approved troops to begin moving into Ukraine-controlled territory. Over the past five days of fighting, Ukraine has succeeded in holding Russian forces off from taking over major cities, including Kharkiv and Kyiv. Dozens of countries and allied bodies have imposed sanctions on Russian entities in response to the invasion and are supporting Ukraine by sending weapons, supplies, and funds to the country. Cyber attacks, including DDoS attacks, the deployment of wiper malware, and phishing campaigns, have targeted both Ukrainian and Russian public and private entities, and several non-state hacking groups have announced support of Ukraine or Russia.

THESE ARE THE LATEST CYBER UPDATES FROM THIS WEEKEND:

The hacker group Anonymous announced it is officially "in cyber war against the Russian government," stating it has already launched a campaign against Russia and that private organizations will be impacted. It has already led multiple attacks, causing outages at state-owned media Russia Today, leaking data from the Russian Ministry of Defense website, carrying out DDoS attacks against multiple Russian government websites, breaching the internal network of Belarusian railways, and releasing roughly 200GB of emails from Belarusian weapons manufacturer Tetraedr.

On the other side, the Conti ransomware group announced "full support of the Russian government" and that if any entity attacks the Russian government, Conti will retaliate and use all possible resources to strike back at Western critical infrastructure. But after Ukrainian Conti affiliates grew upset over the group's siding with Russia, the Conti gang replaced their message with another one, stating that they "do not ally with any government" and that they "condemn the ongoing war" but will still retaliate if the West targets Russian civilians or critical infrastructure. After this announcement, a Ukrainian security researcher leaked over 60,000 internal messages belonging to Conti, which provided researchers and law enforcement a lot of insight about Conti's internal processes.

On Saturday February 26th, Ukrainian deputy prime minister and minister of digital transformation Mykhailo Fedorov, announced on Twitter that he was creating an "IT Army" to attack major Russian government and business websites. He directed viewers to a channel on Telegram, which includes a list of key Russian government and military sites to target. The channel had over 184,000 subscribers as of yesterday. Additionally, Elon Musk says his company's Starlink satellite broadband service is now "active" in Ukraine, where internet access has been disrupted due to Russia's assault.

IronNet continues to closely track the conflict and assess possible implications for our partners. Please refer to IronNet's "Russian invasion: ongoing updates of cyber actions to track" blog for daily updates on the conflict in terms of politics, economics, kinetic warfare, and cyber warfare.

Why **Collective Defense?**

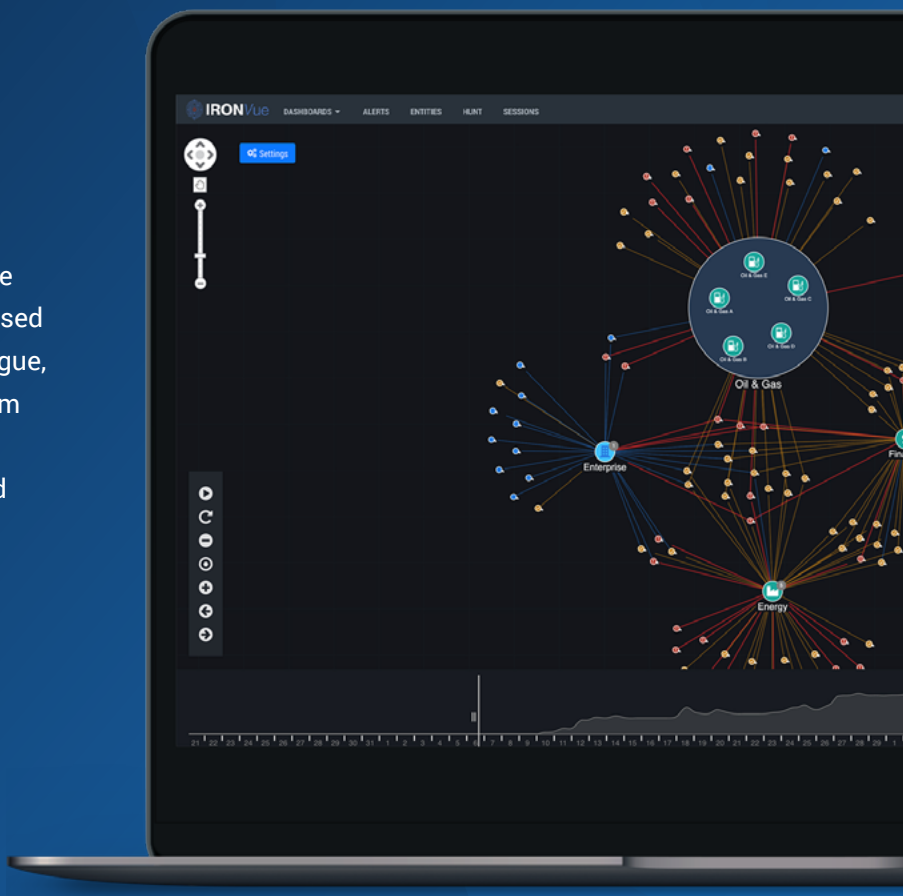
> **IronDome enables us to proactively defend against emerging cyber threats by uniquely delivering machine speed anomaly detection and event analysis across industry peers and other relevant sectors."**
>
> **— CISO, Industry-Leading North American Energy Company**

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. IronDome participants 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, 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