IronNet™

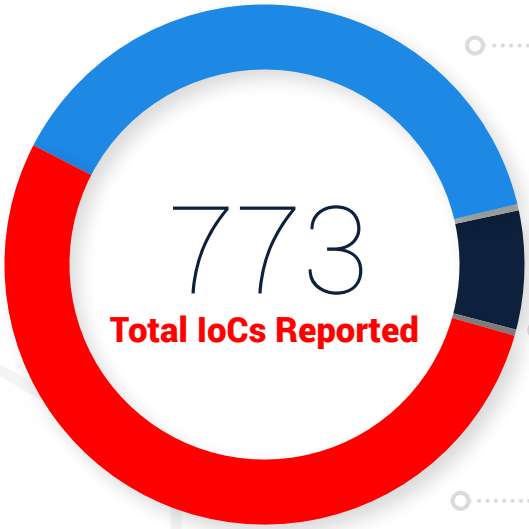
Edition #22: October 2021

IronNet:
Threat Intelligence Brief

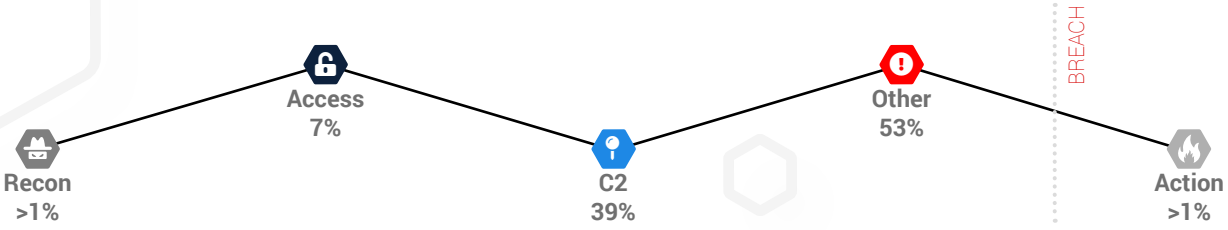
Top Observed Threats from IronNet Collective Defense Community
September 1 – September 30, 2021

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: **299 IoCs**
- Action **3 IoCs**
- Access **57 IoCs**
- Recon **3 IoCs**
- Other: **411 IoCs**



Recent Indicators of Compromise

Domain/IP	Rating	Analyst Insight
windowsupdatesupport[.]org	MALICIOUS	The request for "windowsupdatesupport[.]org/d/loader[.]sh" triggered the Suspicious File download analytic. The file download was blocked by the company's firewall. We recommend blocking the domain.
kerrytj[.]com	MALICIOUS	This domain hosts two malicious macro-enabled Word documents (invoice.doc/use.doc). At time of triage, the domain was not used for benign purposes and only hosted redirects and the malware previously noted.
browndangerexact[.]top	MALICIOUS	This domain is associated with Terraclicks, a browser redirect that can be a strong indicator that there is adware actively running on the endpoint. We recommend investigating any redirects and blocking the domain.
youxjiauun[.]work	MALICIOUS	This domain has been seen hosting an abundance of phishing sites. We recommend blocking the domain.
amibios-updater[.]com	MALICIOUS	The domain is a potential Cobalt Strike Command and Control (C2) domain. If seen on your network, investigate any traffic and block the domain.
openeyeastrology[.]com	MALICIOUS	This domain and its path information indicate its involvement in hosting a Microsoft credential phishing page. If seen in your network, investigate traffic for loss of personally identifiable information (PII) and block the domain.
x8il-pm[.]top	MALICIOUS	This is a credential phishing domain impersonating a Microsoft site. If seen in your network, investigate traffic for loss of personally identifiable information and block the domain.
thyrsi[.]com	MALICIOUS	This is a GET request for an image (JPG and PNG) from an official Microsoft forum. However, the image is a known malicious file (urlhaus) that carries executable file format (ELF) malware and types of cryptomining malware by the Rocke group. At time of triage, the image was blocked but it may still be active on the site.
atomictrivia[.]ru	MALICIOUS	Several malicious files were communicating using this domain, which has been blocked by companies like Quad9 and Akamai, among others. We recommend blocking the domain.
kerrytj[.]com	MALICIOUS	This domain is part of a phishing and social engineering redirect campaign. Ensure connections to this domain and the related IP 143.110.147.132 are blocked.

Threat Rules Developed

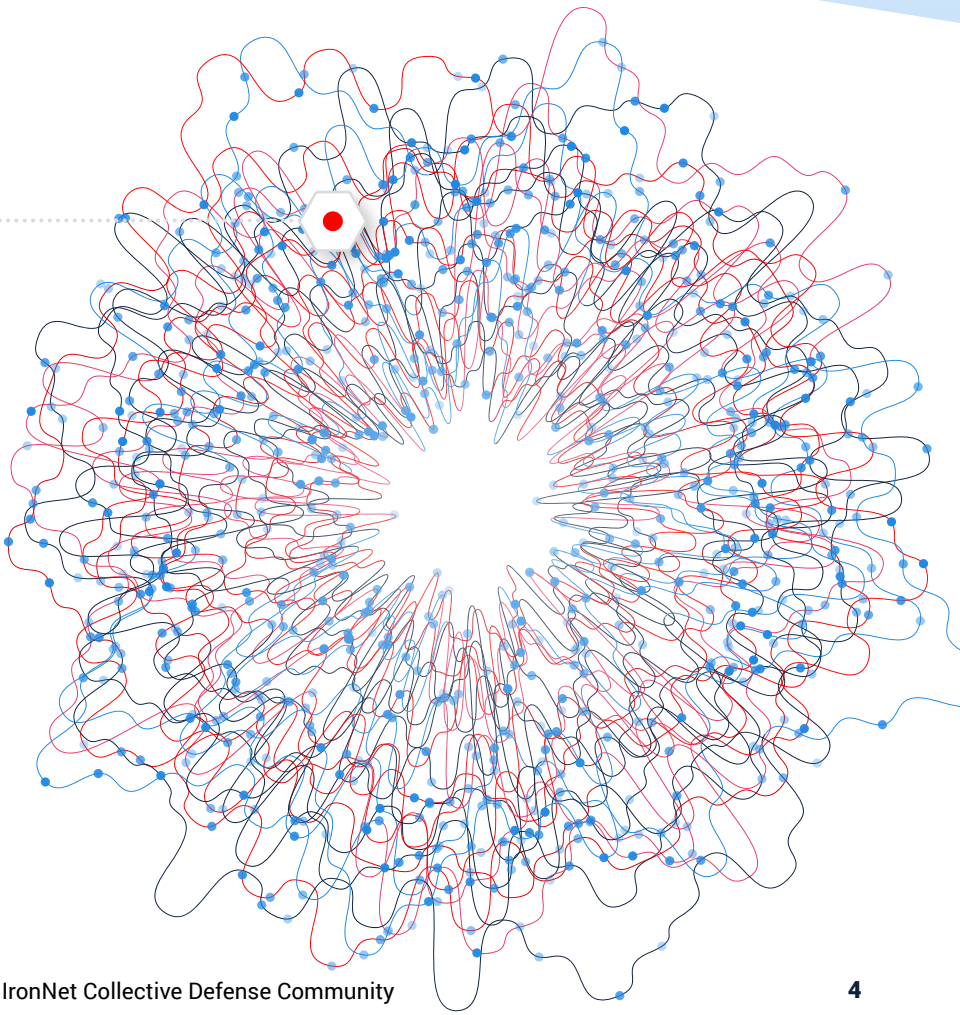
Every month, IronNet's expert threat analysts create threat intelligence rules (TIRs) based on significant community findings from IronDome, malware analysis, threat research, or other methods to ensure timely detection of malicious behavior targeting an enterprise or other IronDome community participants. 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.

5,871

Threat Intel Rules Developed This Month

269,067

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:

- Malware delivery domains for Gafgyt, AgentTesla, Sabsik, Socelars, and Bian malware
- IoCs related to Cobalt Strike beacon payload distribution and Command and Control
- IoCs surrounding a widespread credential phishing campaign abusing open redirector links
- IoCs surrounding the Raccoon Stealer malware campaign
- IoCs surrounding the FerociousKitten APT Group
- IoCs surrounding the BlackMatter ransomware group

This Month in the IronDome

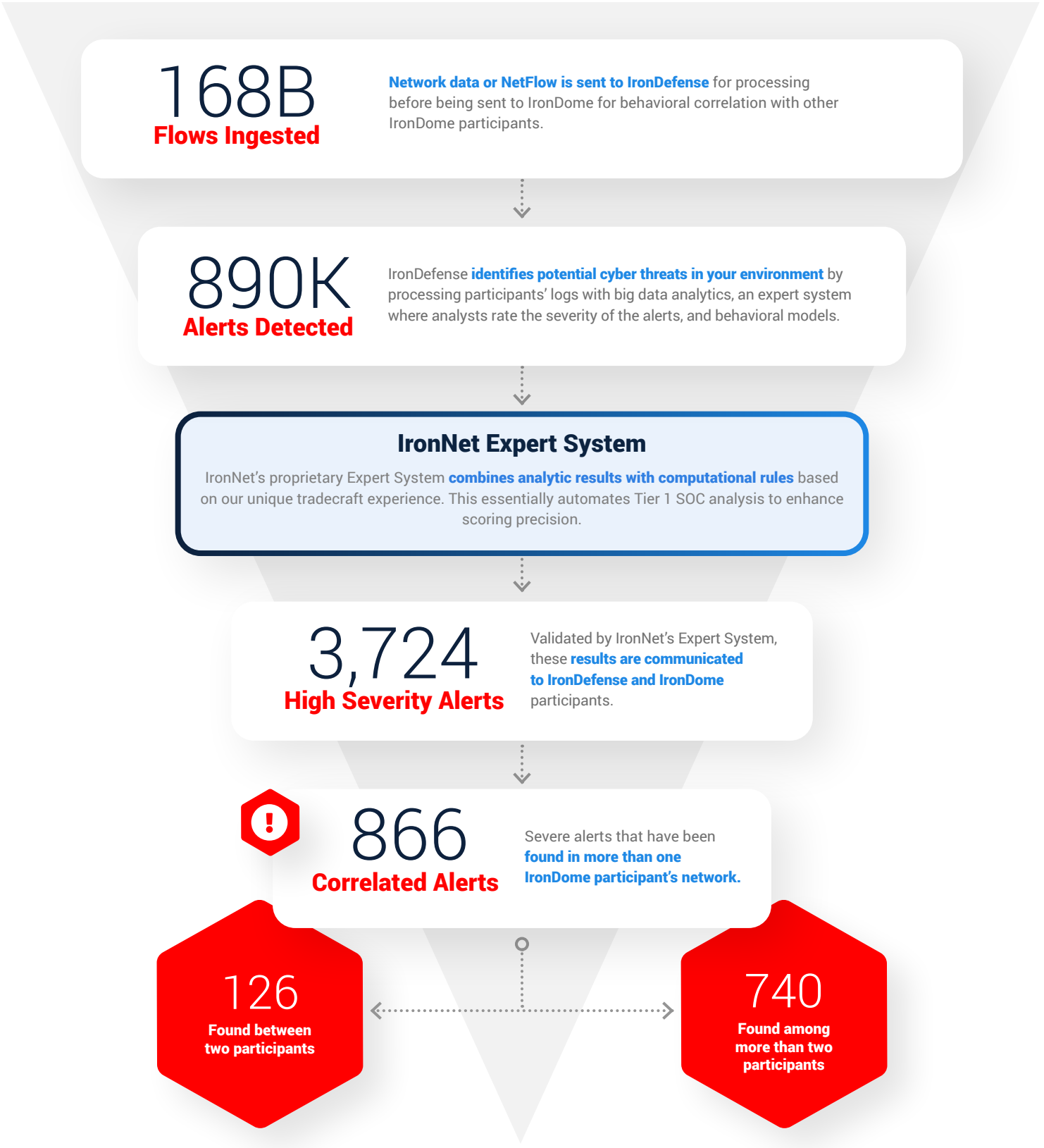
The IronDefense network detection and response solution detects behavior-based anomalies as follows:

- 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.

- C2 Rendevous (DGA) 54.3%
- External Scanning 10.1%
- New and Suspicious Domains 12.2%
- Credential Phishing 14.0%
- Encrypted Comms 3.0%
- Beaconing 2.6%
- DNS Tunneling 1.5%
- Suspicious File Downloads 1.4%
- Data Exfiltration 0.9%

Tracking **Industry Threats**

IronNet Blog - Gone Phishing

Microsoft has been actively tracking a widespread credential phishing campaign leveraging open redirects in conjunction with reCAPTCHA, which is a CAPTCHA system that enables web hosts to distinguish between human and automated access to websites. Leveraging one of the cheapest and easiest ways to gain access to a network, threat actors are obfuscating their phishing links via redirection and services like CAPTCHA to thwart traditional email gateways and sandboxes. IronNet has expanded on Microsoft's research to highlight some of the behavior that has been observed in our customer environments.

There are three main malicious flows: Customer Relationship Management (CRM) platforms allowing open redirects; websites redirecting to phishing reCAPTCHA landing pages; and other reCAPTCHAs to phishing sites. The use of CRMs from household-name type companies allowing open redirects to malicious phishing sites seems to have started in Q1 of 2021, with some leading into Q2 of 2021 and many still being exploited today.

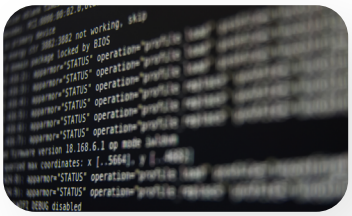
Check out IronNet's Gone phishing? Beware of what you (re)CAPTCHA blog to learn more about the research done by our Threat Analysis and Research Teams and to access IronNet's compilation of more than 1000 IoCs of detected domains and reCAPTCHA site keys from this campaign.

Windows MSHTML (CVE-2021-40444)

Microsoft recently disclosed a new zero-day remote code execution (RCE) vulnerability (CVE-2021-40444) within Windows MSHTML, which is a browser rendering engine also used by Microsoft Office documents. Affecting Windows Server 2008 to 2019 and Windows 8.1 to Windows 10/11, CVE-2021-4044 is being actively exploited by threat actors to execute remote commands on a target's computer via a specially crafted Microsoft Office document or rich text format (RTF) file. Threat actors are actively jumping on this attack vector and are now sharing proofs of concept (PoC), tutorials, and exploits regarding this new CVE on various hacking forums.

Though originally thought to be isolated to Microsoft Office documents and Internet Explorer, the RCE vulnerability was later discovered to permeate through Windows Explorer's preview mode and an RTF file. For Microsoft Office files, no traditional macros are needed for this attack; any way an Office document may call out to a URL can be used to exploit this CVE. Researchers have discovered some samples of this exploit in the wild staging Cobalt Strike. For example, Trend Micro uncovered a weaponized document that was using Cobalt Strike, which can allow an attacker to take control of an infected system.

No official patch has been released by Microsoft, nor are there any real mitigations available yet. Microsoft did publish a few workarounds last week, but these were quickly circumvented by security researchers. For example, Microsoft pushed some recommended Group Policy Objects (GPO) to help mitigate the exploit as they block ActiveX controls. However, this workaround requires a restart, and attackers have already circumvented this by modifying the exploit to not use ActiveX. Until Microsoft releases an official security update, users should treat all Word and RTF attachments suspiciously and manually verify their sources before opening them.



OMIGOD

The cloud security firm Wiz discovered a group of four vulnerabilities, collectively referred to as OMIGOD, in the Open Management Interface (OMI) of Linux-based Azure virtual machines (VM). When customers set up a Linux VM in their cloud, the OMI is automatically deployed without their knowledge when they enable certain Azure services. The OMI agent runs as root with the highest privileges and is basically the Linux equivalent of Microsoft Windows Management Infrastructure (WMI) service, which enables the collection of logs and metrics and some remote management.

Unless a patch is applied, attackers can easily exploit these four vulnerabilities to escalate to root privileges and remotely execute malicious code. However, because Azure provides virtually no public documentation about OMI, most customers have never heard of it and are unaware this vulnerability even exists in their environment.

Of the four CVEs, the remote code execution (RCE) vulnerability (CVE-2021-38647) is the most serious issue, as it can allow a threat actor to become root on a remote machine with a single packet by removing the authentication header. In situations where the OMI ports are accessible to the internet to allow for remote management, this vulnerability can be used by attackers to obtain initial access to an Azure environment and then move laterally within it.

New data indicates attackers are actively scanning the Web for Azure Linux virtual machines that are vulnerable to RCE vulnerability. We have recently seen several active exploitation attempts ranging from basic host enumeration to attempts to install a crypto currency miner or file share. While Microsoft has released patches for these four critical OMI vulnerabilities, many Azure Linux VMs remain vulnerable to attacks unless each and every user manually updates the client themselves. Microsoft further urges customers to verify that they are running the latest version of OMI (V 1.6.8.1), to ensure VMs are deployed within a Network Security Group (NSG) or behind a perimeter firewall, and to restrict access to Linux systems that expose the OMI ports (TCP 5985, 5986, and 1270).

TAG-28 Targets India

As the bilateral relations between China and India continue to deteriorate over the Line of Actual Control (LAC) dispute in the Galwan Valley, India has become the target of several Chinese state-sponsored cyber attacks. Researchers at Recorded Future have identified intrusions targeting Indian entities led by suspected Chinese state-sponsored threat activity group TAG-28. The victims of these intrusions include Indian media conglomerate Bennett Coleman and Co. Ltd. (BCCL), a multimillion-dollar news organization commonly known as "The Times Group" that consistently reports on the China-India war. Victims also include the Unique Identification Authority of India (UIDAI), which contains the biometric data of one billion Indian citizens, as well as the Madhya Pradesh Police Department (MPP), whose Chief Minister was critical of China after the border clashes that occurred in the Ladakh region in June 2020.

It is not uncommon for China to target news organizations, especially those that present China in an unfavorable light. The country is interested in accessing these organizations to spy on foreign journalists and their sources. UIDAI is a likely target because of the mass amount of personally identifiable information it holds, which enables threat actors to enrich their data on foreign government officials, identify high-value targets, and lay the foundation for social engineering attacks.

Recorded Future used their Network Threat Analysis (NTA) platform and adversary command and control detection techniques to detect these attacks and identify patterns of suspicious network activity. In this campaign, TAG-28 used Winnti malware, which is a family of malware that several Chinese threat actors have historically used. In relation to the attack on BCCL, between February and August 2021, four IPs were seen communicating with two Winnti C2 Servers and possibly a Cobalt Strike server, which led to approximately 500 MB of data being exfiltrated from the network. From June 10th to at least July 20th, 2021, researchers observed two IPs registered to UIDAI communicating with the same suspected Cobalt Strike C2 server used to target BCCL. Less than 10 MB was egressed from the UIDAI network with an ingress of almost 30 MB, potentially indicating the deployment of additional malicious tools from the TAG-28 infrastructure. As for the targeting of the MPP, the department's website began communicating with a Winnti C2 server on June 1st, 2021. Another MPP IP began talking to the malicious server on July 7th to at least August 9th, with around 5MB of data being transferred.

As tensions increase between India and China, gaining access to key Indian entities—like government departments and media organizations—will likely remain of the utmost importance to Chinese state-sponsored actors. This ongoing dispute between the two nations will demonstrate how China's military may flex its strength within the cyber domain to achieve strategic and tactical objectives. This campaign also highlights that established tooling like Winnti and offensive security tools like Cobalt Strike continue to prove highly effective for Chinese threat groups to carry out targeted intrusions.

Why **Collective Defense?**

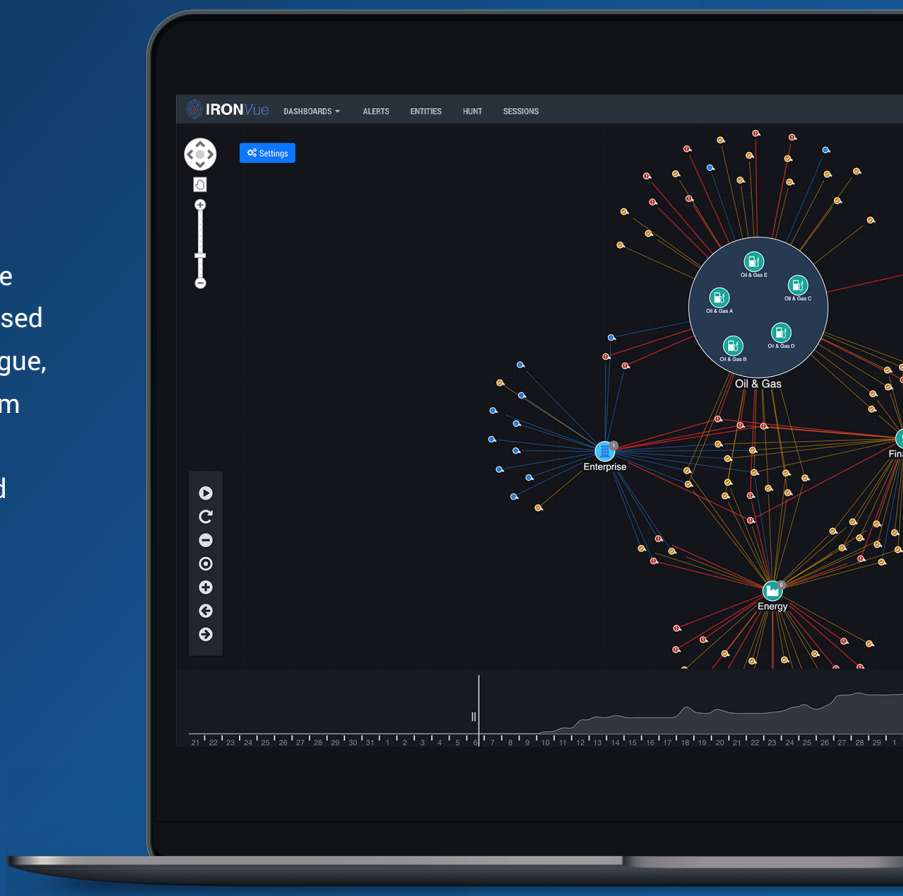
> **IronDome enables us to proactively defend against emerging cyber threats by uniquely delivering machine speed anomaly detection and event analysis across industry peers and other relevant sectors."**
>
> **— CISO, Industry-Leading North American Energy Company**

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