IronNet

Edition #26: February 2022

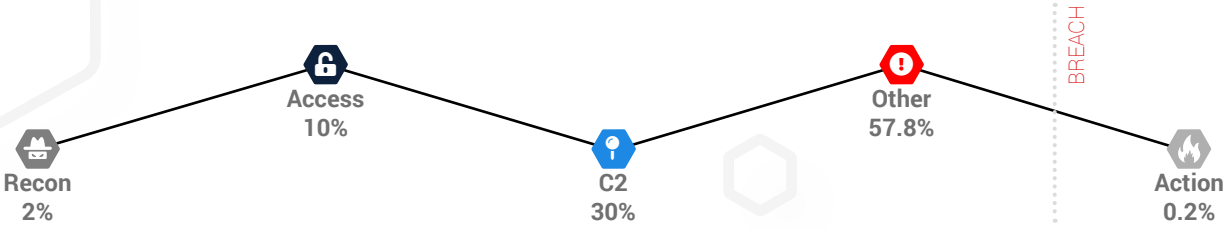
IronNet:
Threat Intelligence Brief

Top Observed Threats from IronNet Collective Defense Community
January 1 – January 31, 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 **165 IoCs**
- Action **1 IoC**
- Access **55 IoCs**
- Recon **11 IoCs**
- Other **320 IoCs**



Recent Indicators of Compromise

Domain/IP	Rating	Analyst Insight
best-lucky-man[.]xyz	MALICIOUS	This domain hosted process injection malware detected by ESET and was flagged as malicious by VirusTotal.
itchytidying[.]com	MALICIOUS	After investigating the domain and its related IPs, we determined it was malicious. In addition, multiple vendors have flagged it as malicious and/or suspicious.
tsmtracking[.]com	MALICIOUS	This domain is indicative of a successful phishing attempt from a phishing email impersonating a bank. Further triage revealed personal information left the network.
prodidygame[.]com	MALICIOUS	This is a typo-squatting domain impersonating prodigygame[.]com. We recommend blocking the domain.
prophetachybrief[.]com	MALICIOUS	This domain has been known to actively host malware/adware without the user's permission. If installed, the malware/adware could cause a variety of problems, including slowing down the browser and exposing the laptop user's personal information. We recommend cleaning the infected device and blocking the domain.
railcowboy[.]com	MALICIOUS	After investigating both IP (192.243.59.13) and domain, The IP has been determined as malicious and the domain suspicious. We recommend blocking both domain and IP.
81.171.33.201	MALICIOUS	The IP 81.171.33.201 is owned by Eweka Internet Services B.V. Web traffic to this IP presents a potentially high fraud risk. We recommend blocking this IP.
dominantpartition[.]com	MALICIOUS	Multiple vendors on Virustotal.com flagged this domain as malware. We recommend blocking the domain.
test1-smalleststores[.]com	MALICIOUS	This domain has been flagged as malware. We recommend blocking the domain.
itchytidying[.]com	SUSPICIOUS	This domain is associated with Terraclicks, a browser redirector known to redirect to malicious sites. We recommend blocking all traffic to this domain.

Threat Rules Developed

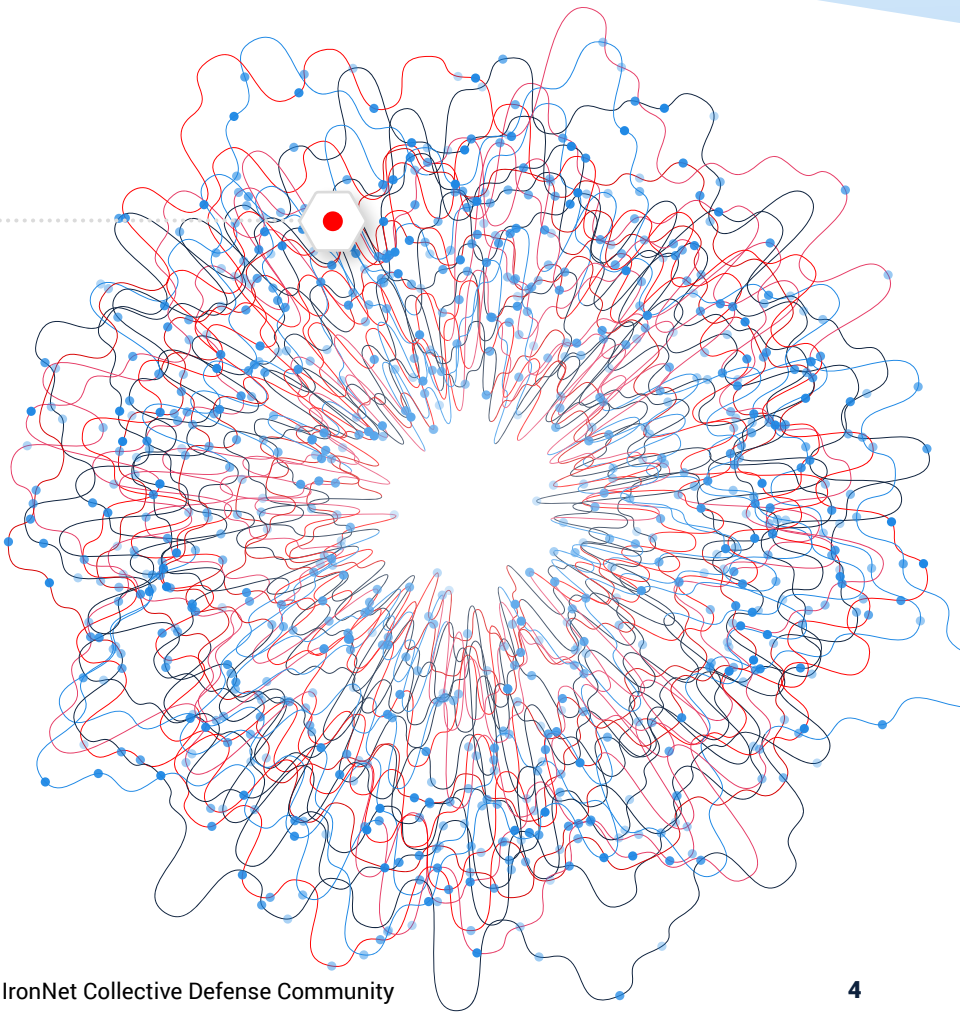
Every month, IronNet's expert threat analysts create threat intelligence rules (TIRs) based on significant community findings from IronDome, malware analysis, threat research, or other methods to ensure timely detection of malicious behavior targeting an enterprise or other IronDome community participants.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

3,521

Threat Intel Rules Developed This Month

293,909

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)
- IoCs related to new ZLoader campaign abusing Microsoft's digital signature verification
- Malware delivery domains for Gafgyt, Setag, Tsunami, Typosquat, ClipBanker, and Perseus malware
- IoCs related to BlueNoroff, a North Korean APT
- IoCs related to an Android malware called FluBot
- IoCs related to Log4Shell
- IoCs related Dark Herring SMS scam campaign

This Month in the IronDome

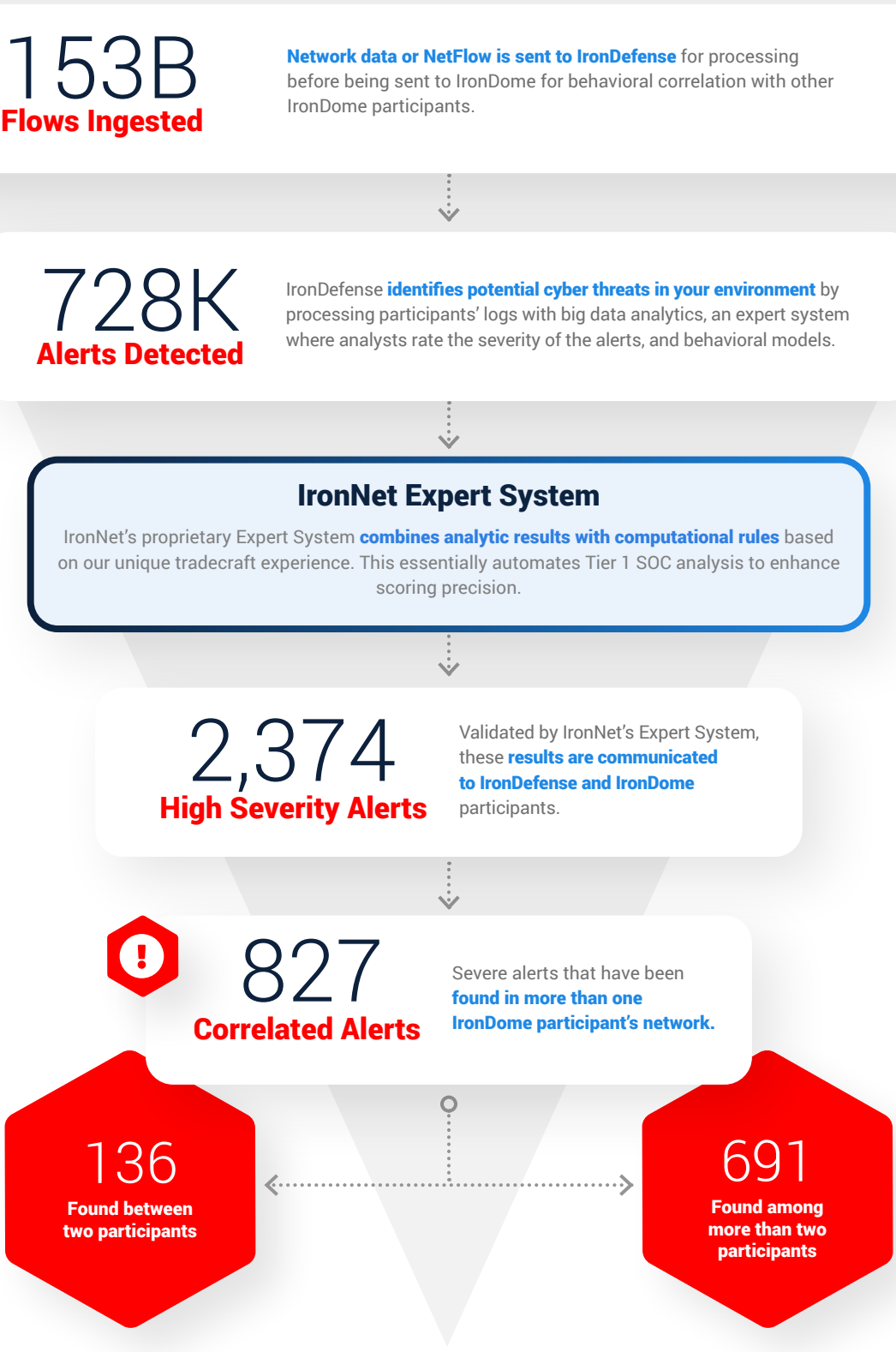
The IronDefense network detection and response solution detects behavior-based anomalies as follows:

- 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.

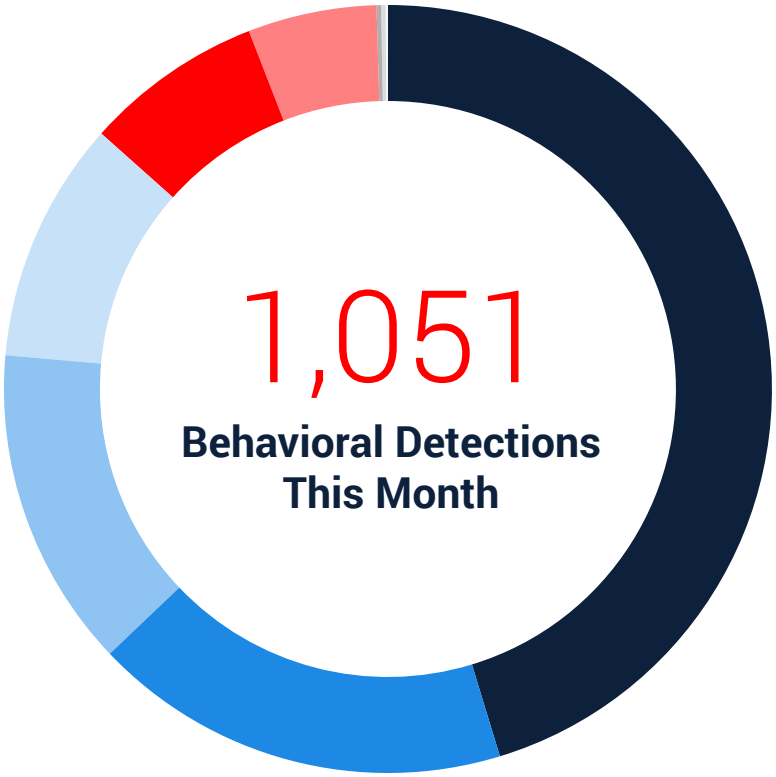
Monthly Alert Snapshot



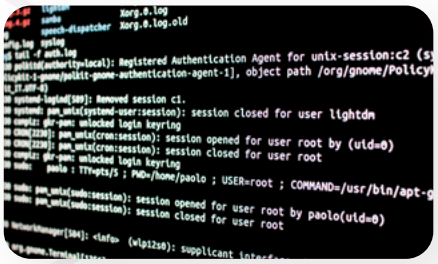
Top Most Frequent Behavioral Analytics

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

- External Scanning 45.3%
- C2 Rendevous (DGA) 17.6%
- New and Suspicious Domains 13.5%
- Credential Phishing 10.2%
- Beaconing 7.5%
- Encrypted Comms 5.4%
- DNS Tunneling 0.2%
- Suspicious File Downloads 0.2%
- Data Exfiltration 0.1%



Tracking Industry Threats



APT41's MoonBounce Bootkit

Kaspersky has recently discovered the third known case of a firmware bootkit in the wild: a new bootkit from APT41, dubbed MoonBounce. Moonbounce is a malicious implant that hides within Unified Extensible Firmware Interface (UEFI) firmware in the Serial Peripheral Interface (SPI) flash memory. UEFI is an essential part of a computer, as it is the interface between a device's firmware and its operating system, and its code is responsible for booting the system. This code is hosted in SPI flash, a non-volatile storage component external to the hard drive. If the firmware contains malicious code, then it will be launched before the operating system, which makes the malware deployed by the firmware bootkit particularly difficult to delete. Also, since the code is located outside of the hard drive, the bootkit slides by most security solutions undetected unless there is a specialized feature that scans this part of the device. The components of MoonBounce operate in memory only, meaning the infection chain does not leave any traces on the hard drive, which facilitates a fileless attack with a very small footprint.

MoonBounce first appeared in the spring of 2021. Since then, Kaspersky has linked the bootkit with high confidence to Chinese state-sponsored APT41, a.k.a. the Winnti Group. The UEFI bootkit was observed in a single incident so far against an organization in control of several enterprises handling transport technology, indicating a highly targeted nature of attack. Along with MoonBounce, Kaspersky observed other non-UEFI implants in the targeted network that communicated with the attackers' same infrastructure. These implants include several malicious loaders and post-exploitation malware, such as Sidewalk and Microcin. Commands leveraged by APT41 suggest the group was interested in lateral movement and data exfiltration, and given the use of a UEFI implant, it is likely the threat actors were interested in conducting ongoing espionage activity.

Microsoft Signature Verification Abused in ZLoader Campaign

Check Point Research has discovered a new campaign exploiting a vulnerability in Microsoft's digital signature verification to deliver ZLoader malware. ZLoader is a variant of the infamous Zeus banking trojan that's able to steal user credentials, cookies, and sensitive information, as well as act as a backdoor and loader for other malicious code. This specific campaign was first seen around early November 2021 and is believed to be currently active. As of January 2nd, 2170 unique victim IPs have been infected, with a majority of victims (over 850) residing in the U.S., followed by Canada and India.

The infection chain starts with the installation of Atera software, a legitimate remote management software (RMM). The exact distribution method for the file in this campaign has not been determined, but the malicious package containing Atera includes a downloadable file disguised as a Java installation, which installs an agent that connects the endpoint to an attacker's account. Once the agent is installed, the attacker has full access to the system and can upload/download files, run scripts, and more.

Two batch files are then uploaded to the victim's machine: the first is responsible for tampering with Windows Defender, and the second is used to load ZLoader. From there, the threat actors exploit Microsoft's digital signature verification method to inject the payload into a signed system Dynamic Link Library (DLL). The target DLL file is digitally signed by Microsoft, which is supposed to prove its authenticity; however, the attackers were able to inconspicuously append a malicious script to the signature section of the file without changing the validity of the signature itself.

To do this, they exploited a known vulnerability in the signature validation of crafted Portable Executable (PE) files, mentioned in CVE-2020-1599, CVE-2013-3900, and CVE-2012-0151. Microsoft released a fix for this issue in 2013, but the patch tended to alert on false positives where legitimate files were flagged as potentially malicious. As a result, the patch is disabled by default and many Windows devices do not have it enabled.

Check Point Research believes that a cybercriminal group known as MalSmoke is behind the latest campaign, and the tactics used in these attacks indicates MalSmoke puts great effort into defense evasion and is updating its methods on a weekly basis.

The recommended mitigation is to apply Microsoft's update for strict Authenticode verification. IronNet has integrated the domain and IP indicators of compromise associated with this campaign as threat intelligence rules and will be closely monitoring this campaign for additional information.

Attacks Targeting the Ukrainian Government

WEBSITE DEFACEMENT

During the night between January 13th and 14th, multiple Ukrainian government websites were wiped and defaced with a statement in Ukrainian, Russian, and Polish warning personal data had been leaked. The Ukrainian State Service of Communication denied any data being leaked, but government agencies whose websites were defaced include the Ukrainian Ministry of Foreign Affairs, Ministry of Education and Science, Ministry of Defense, the State Emergency Service, the website for the Cabinet of Ministers, and others.

The Secret Service of Ukraine (SSU) stated that the defacements were the result of a supply chain attack, which allowed the threat actors to gain access to the infrastructure of a company called Kitsoft, which manages websites for the Ukrainian government and thus has administrative access to websites impacted by the attack. It is reported the threat actors attempted to compromise 70 sites but only managed to modify 10.

The SSU suggested the attack was conducted by "hacker groups associated with Russian secret services," but it did not formally attribute the attacks to a specific threat actor or nation-state. On January 15th, Serhiy Demedyuk, stated that the Ukrainian government believes preliminarily that the group UNC1151 (aka, Ghostwriter) may be involved in the attack. UNC1151 has been linked to the Russian government – and more recently to the Belarusian government – and is known for its cyber intrusions and disinformation campaigns intended to undermine NATO's presence in and security cooperation with Poland, Lithuania, and Latvia.

WIPER MALWARE

On January 13th, Microsoft observed destructive malware being used in intrusion attacks against numerous Ukrainian government agencies and associated organizations. Microsoft determined that the malware is designed to look like ransomware, but it lacks a ransom recovery mechanism, which indicates its purpose is to render systems inoperable rather than to obtain a ransom. Organizations targeted with this malware include executive and emergency response government agencies and an IT firm that manages websites for public and private customers, including Ukrainian government agencies whose websites were defaced. Microsoft has identified the malware on dozens of compromised systems but states the identified victims are unlikely the only ones who have been targeted in these attacks.

In the attacks, the two-stage malware overwrites the Master Boot Records (MBR) on target systems with a ransom note containing a Bitcoin wallet and Tox ID (a unique account identifier used in the Tox encrypted messaging protocol). Although it distributes a ransomware note, the attacks are inconsistent with cybercriminal ransomware activity. These inconsistencies include the absence of a recovery mechanism, the lack of a custom ID, and the specification of only a single communication method (Tox ID). The second-stage malware executes when the compromised device is powered down, and it can best be described as a malicious file corrupter that locates files in certain directories and overwrites the contents of the file.

Microsoft tracks this activity as DEV-0586 and notes it has not found any notable association between DEV-0586 and other known threat actor groups. Additionally, given the timing of the wiper malware deployment and the fact the messages on the website said data had been stolen and deleted, there is some speculation that the website defacements and wiper malware attacks were intended to have been better coordinated. It should be noted that these attacks occurred against the backdrop of ongoing tensions between Russia and Ukraine regarding Russian troop build-up near the Ukrainian border.

Linux Pkexec Vulnerability: PwnKit

Qualys recently discovered a vulnerability in Polkit's pkexec component, which affects all major Linux distributions. Successful exploitation of this vulnerability, dubbed PwnKit, allows any unprivileged user to gain root (i.e., admin) privileges on the vulnerable host. PwnKit (CVE-2021-4034) has been hiding in plain sight for more than 12 years since 2009 when pkexec was created, which means all versions are affected.

Polkit, formerly known as PolicyKit, is a SUID-root program installed by default on every major Linux distribution, and it's used for allowing non-privileged processes to communicate with privileged processes. Polkit's pkexec command is used to run commands with elevated privileges.

The vulnerability lies in how pkexec processes command line arguments and environment variables. A carefully crafted command forces pkexec to execute a non-SUID program specified by unprivileged environment variables as root, thus granting the attacker a local privilege escalation. It is trivial to exploit, but it does not allow for initial access, so an attacker first needs to gain a foothold through another attack vector. Once they have a foothold, they can then use this exploit to elevate their privileges; however, there is no way to exploit PwnKit remotely at the moment.

In terms of response, PoCs have been published by Qualys and others, and virtually all major Linux distributions have published patches. However, if no patches are available for your operating system or if for some other reason you can't patch your system immediately, a temporary mitigation is to remove the SetUID-bit from pkexec using the command: chmod 0755 /usr/bin/pkexec, which will prevent it from running as root when executed by an unprivileged user.

PwnKit is likely already being exploited in the wild by threat actors, but the fact that an existing foothold is needed does make it slightly less of a threat. However, since it is simple to exploit, basically 100% effective, present on a default install of a multitude of Linux distributions, and can leave no trace on the target system, PwnKit can be very malicious and many systems are vulnerable.

Why **Collective Defense?**

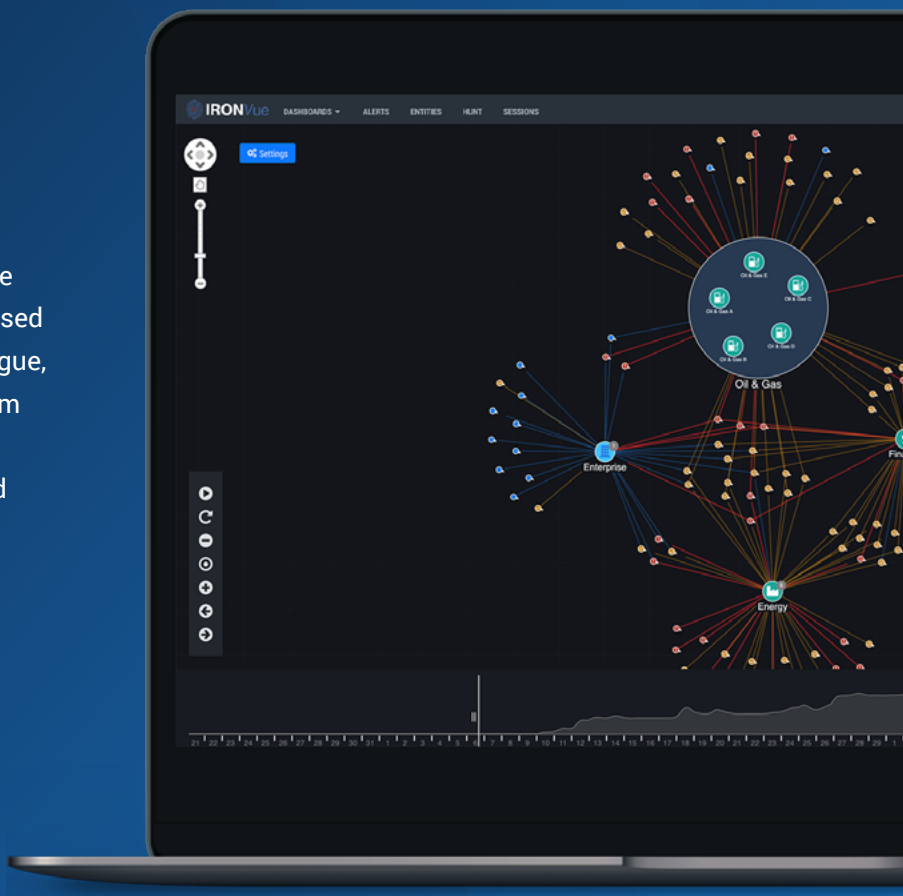
> **IronDome enables us to proactively defend against emerging cyber threats by uniquely delivering machine speed anomaly detection and event analysis across industry peers and other relevant sectors."**
>
> **— CISO, Industry-Leading North American Energy Company**

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