IronNet™

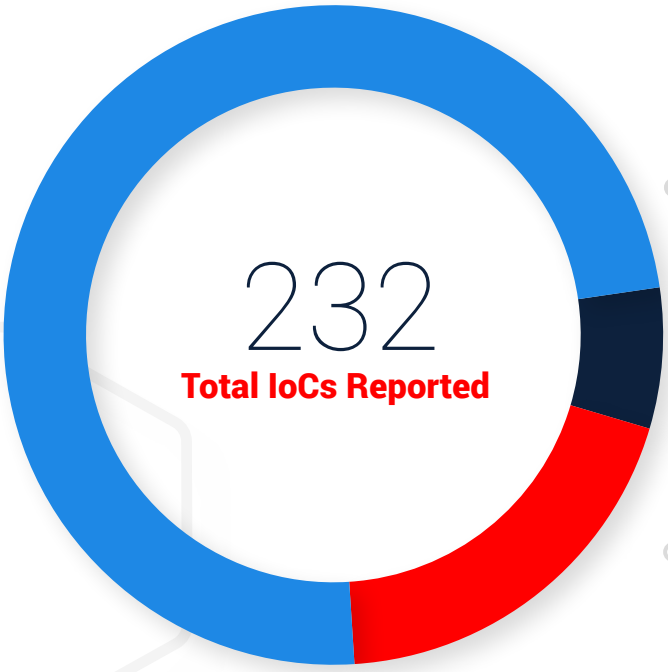
Edition #11: November 2020

IronNet:
Threat Intelligence Brief

Top Observed Threats from IronNet Collective Defense Community
October 1 – October 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:
171 IoCs

Access
16 IoCs

Other:
45 IoCs

Recent Indicators of Compromise

Domain/IP	Rating	Analyst Insight
accessbny[.]com	MALICIOUS	This is a phishing site imitating a Bank of New York login portal. The site appears to be targeting customers' user credentials.
developerstatss[.]ga	SUSPICIOUS	This domain has been used in WordPress infection exploits. Traffic to this site may indicate that a user visited a WordPress site that had been injected with this domain in a post or similar content. Investigate any redirections for malvertising.
declarebusinessgroup[.]ga	SUSPICIOUS	This domain was used with the WordPress File Manager exploit, a zero-day vulnerability that allows actors to hijack websites. Traffic to this site may indicate that a user visited an infected WordPress site. Investigate any redirections.
paypal-debit[.]com	SUSPICIOUS	This domain is related to credit card skimming activity. Investigate the traffic for loss of personally identifiable information (PII).
bestbuystoreapple[.]com	SUSPICIOUS	Although this site claims to sell Apple products, it has no association with Apple Inc. and is likely a scam website selling fake products. OSNT sources also associate this domain with suspicious activity.
lotaboutpay1[.]live	SUSPICIOUS	This is a phishing site with adult content themes. If seen in your network, investigate the traffic for any policy violations and block the domain.
shrimpsqueezed[.]com	SUSPICIOUS	This domain is related to TerraClicks. If seen in your network, investigate any redirections and block the domain.
jounin[.]net	SUSPICIOUS	The TFTP server executables tftpd32.jounin[.]net and http://tftpd64[.]com were downloaded, which may indicate policy violations by an end user. If this TIR creates an alert, we recommend verifying the end user's role.
dev-nano[.]com	SUSPICIOUS	This domain may indicate an undesired browser extension. Although the extension claims to be for ad blocking, OSINT suggests it may collect network information. The domain may indicate a user visited the site to look at the tool description. If seen in your network, investigate the traffic and consider blocking the domain.
my-account-amazon[.]com	SUSPICIOUS	This is a phishing page using the 16Shop phishing framework. At the time of triage, the page was down. Investigate POST activity for potential credential loss.

Threat Rules Developed

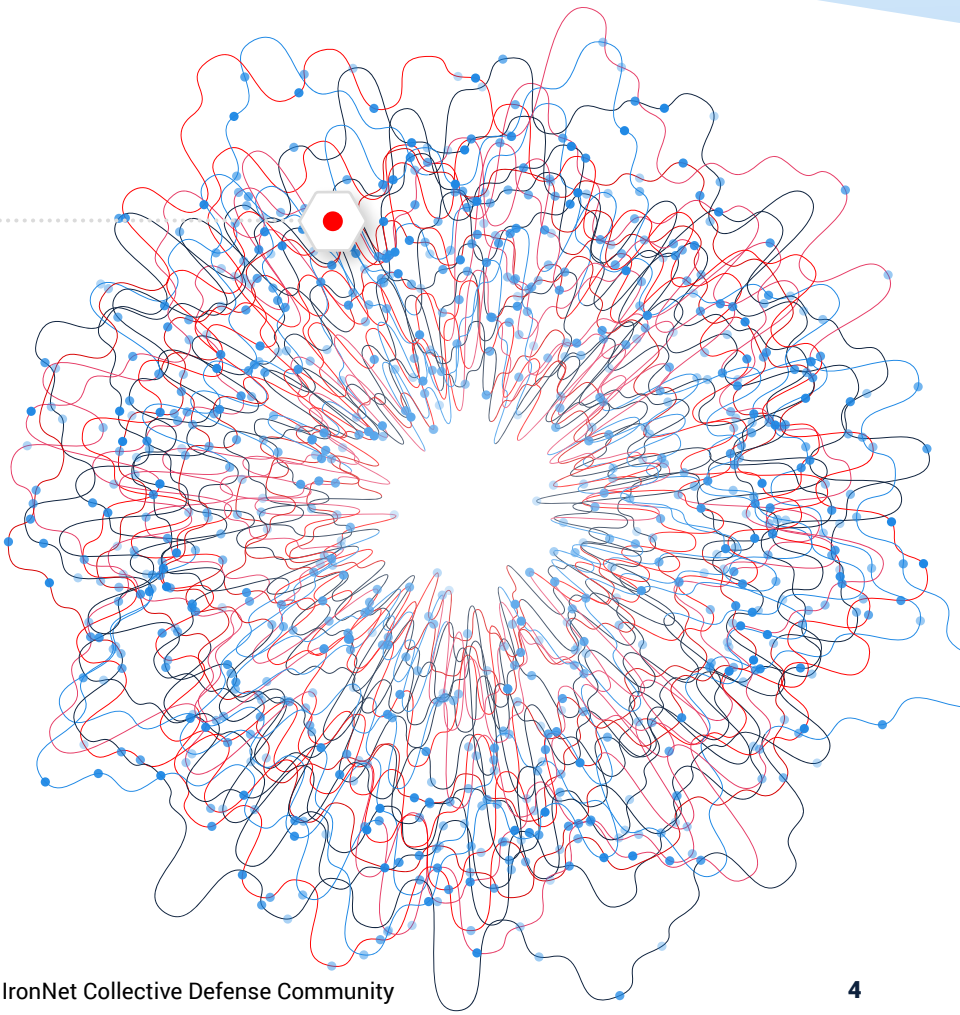
Every month, IronNet's expert threat analysts create threat intelligence rules (TIRs) based on significant community findings from IronDome, malware analysis, threat research, or other methods to ensure timely detection of malicious behavior targeting an enterprise or other IronDome community participants.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

7,750

Threat Intel Rules Developed This Month

159,879

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, Domain Analysis TLS, Periodic Beaconing HTTP, Phishing HTTPS, Suspicious File Download, and TLS Invalid Certificate Chain. 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:

- Indicators associated with the Ryuk ransomware infection chain tied to recent malspam campaigns
- Analysis of the Russian language malware MontysThree, which has been leveraged for industrial espionage operations
- AZORult information-stealing Trojan targeting supply chain-related organizations in the Middle Eastern Oil and Gas sector
- Multiple phishing sites used by the Iran-linked threat actor Silent Librarian to actively target universities in multiple countries
- Indicators associated with new Mirai botnet variants targeting recent Internet of Things (IoT) vulnerabilities
- Analysis indicating increased activity from the Lemon Duck cryptocurrency-mining botnet
- Recent GravityRAT campaign targeting users in India across Windows, Android, and MacOS platforms
- Research examining updates to the Purple Fox exploit kit that incorporate exploitation of two recent Common Vulnerabilities and Exposures (CVE) and add methods to better evade detection tools
- Analysis examining a fake antivirus installer observed infecting systems in Eastern and Central Eurasia
- Recent upticks in voter registration and U.S. election-themed phishing emails
- Indicators associated with Ryuk ransomware identified by multiple government and private sector cybersecurity entities
- Recent activity by the Iran-linked Phosphorus group targeting individuals attending upcoming high-profile international conferences
- New malicious backdoors associated with the Operation Earth Kitsune cyber espionage campaign

This Month in the IronDome

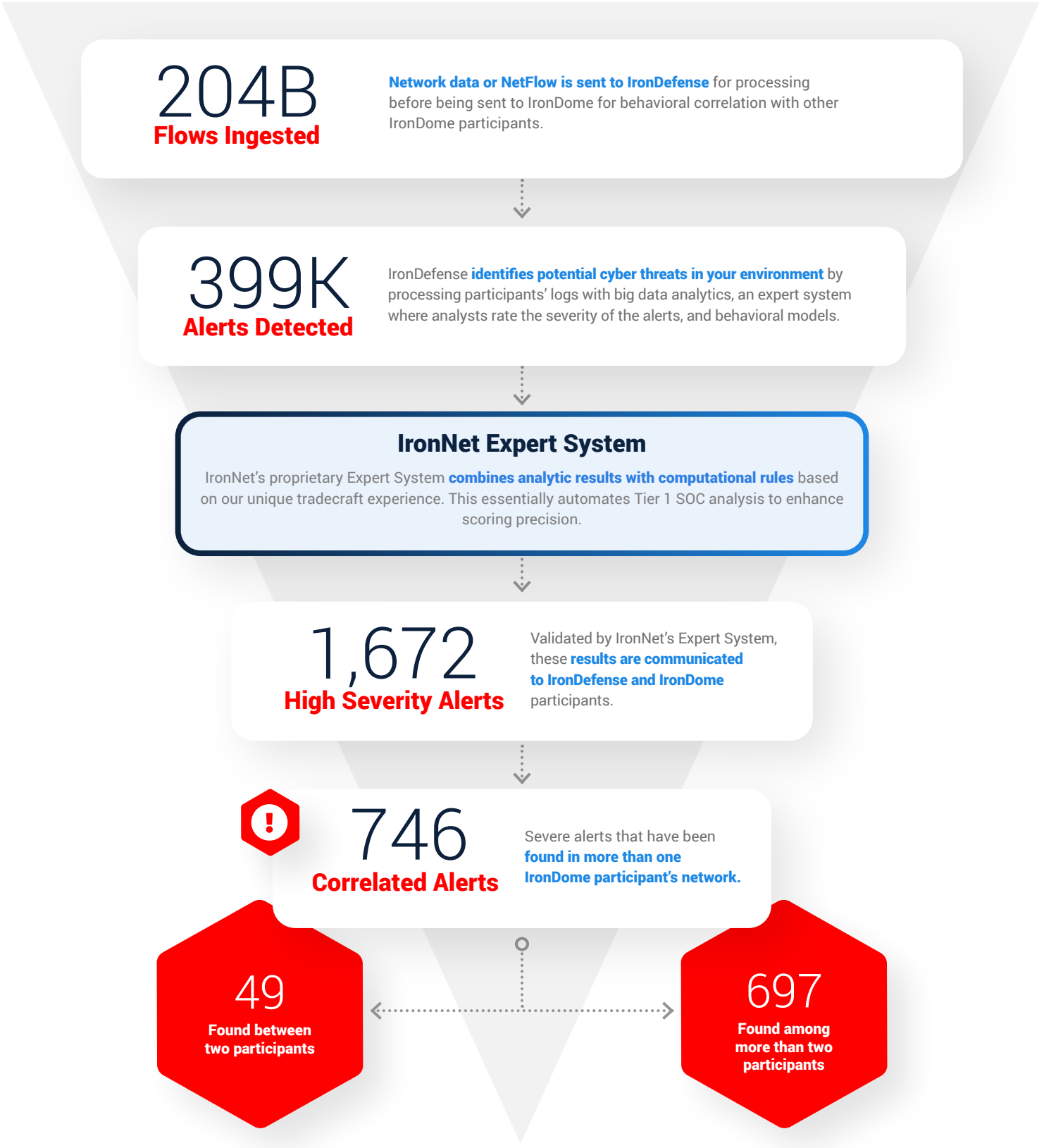
The IronDefense network detection and response solution detects behavior-based anomalies as follows:

- 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



Tracking **Industry Threats**

Efforts to Disrupt TrickBot Emerge

A group of international cybersecurity firms has announced a coordinated effort to disrupt the widespread TrickBot botnet. Microsoft obtained a court order and coordinated with telecommunications providers to cut off a large number of TrickBot's command and control (C2) servers.

This comes on the heels of reports earlier in October that the U.S. Cyber Command was responsible for disrupting TrickBot by distributing bogus configuration files to infected Windows systems. These configuration files changed the designated C2 server to "localhost" in an attempt to disconnect the Windows systems from the botnet.

TrickBot has been one of the most active and pervasive malware families since its emergence in 2016. The modular nature of the malware and its decentralized and resilient C2 infrastructure make it especially difficult to consistently detect and disrupt. Such threats require dynamic and collaborative security solutions to rapidly identify new communication channels and functionality.

Iranian "MuddyWater" Group Linked to Recent Attacks

Cybersecurity researchers have identified a recent campaign targeting multiple Israeli organizations. The campaign has been attributed to MuddyWater, a threat actor that has been previously tied to the Iranian Islamic Revolutionary Guard Corps. The group attempted to install a malicious downloader known as PowGoop during this most recent campaign. PowGoop was likely used during another recent intrusion into a Middle Eastern state-run organization in which an unidentified group of threat actors also deployed the Thanos ransomware. This activity suggests the presence of PowGoop may serve as a precursor to ransomware deployment.

Since MuddyWater has not been previously observed conducting such ransomware attacks, researchers speculate that the actual goal of this attack may have been to serve as a de facto destructive attack, similar to destructive attacks carried out by other Iranian threat actors in the past.

Publicly available network indicators related to PowGoop have been deployed as threat intelligence rules in IronDefense. IronNet Hunters have also conducted focused queries to identify any recent network activity potentially related to such activity.

Ransomware Gang Increasingly Targeting Hospitals

In recent weeks, the cybersecurity community has witnessed an uptick in ransomware attacks targeting hospitals and healthcare facilities. Last week, several U.S. federal agencies released a joint advisory highlighting the "imminent threat" from these ransomware operators. The advisory also provided recommendations for detecting and mitigating such threats. Since the advisory's release, news has surfaced that healthcare systems in Oregon, New York, and Vermont have been affected by ransomware. Private sector reporting has attributed these campaigns to the Ryuk ransomware gang, sometimes known as UNC1878 or Wizard Spider, a criminal group likely operating out of Russia.

The infection vectors commonly preceding the deployment of Ryuk are not particularly new or novel. Email phishing using malicious attachments and embedded hyperlinks have been cited as typical ways in which attackers first gain access to victim networks. A defense-in-depth strategy leveraging a combination of email inspection, network detection and response (NDR), endpoint detection solutions, and comprehensive backup and recovery systems represents the best path to combating such ransomware infections.

U.S. Government Names and Shames Multiple Russian Hacking Groups

In October, the U.S. government took action against multiple Russian state-sponsored hacking groups. The Justice Department announced the indictment of six Russian men who are members of a group known as the Sandworm Team. The indictment lists numerous intrusion campaigns executed by these actors, including the infamous NotPetya attacks, targeting of French politicians and government entities during the 2017 elections, and efforts to interfere in media and government networks in Georgia in 2018 and 2019. These charges also included the first official acknowledgement by the U.S. government that Sandworm was responsible for the Olympic Destroyer malware used to disrupt the 2018 Winter Olympic Games in PyeongChang, South Korea.

The U.S. Department of the Treasury imposed sanctions on the Russian Central Scientific Research Institute of Chemistry and Mechanics, effectively cutting off any U.S. business or engagement with the research institute and proposing sanctions against third-party nations that continue to do business with them. The sanctions represent the first public acknowledgement by the U.S. government of the institute's connection to the Triton malware designed to target industrial safety systems, which had been previously alleged by private sector cybersecurity researchers.

Additionally, the U.S. Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) released a joint advisory detailing active targeting of U.S. state and local governments and aviation networks by Berserk Bear actors. While the advisory stated that these intrusions did not appear to have disrupted any operations within the targeted networks, the group did successfully exfiltrate data from at least two victims and appeared to be hunting for information such as network configurations, passwords, and vendor purchasing data.

The pace and volume of these government initiatives highlights the significance of the threat posed by Russian cyber actors to a variety of sectors and underscores the value of collective intelligence sharing and rigorous defense-in-depth strategies.

Why **Collective Defense?**

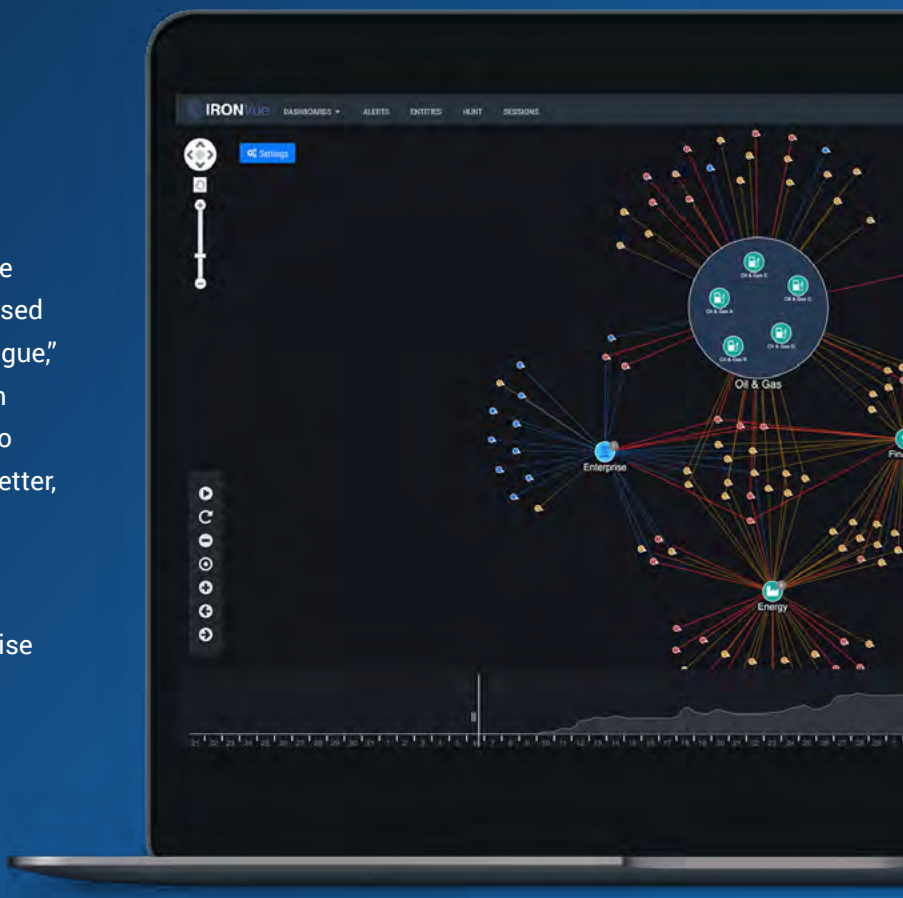
> **IronDome enables us to proactively defend against emerging cyber threats by uniquely delivering machine speed anomaly detection and event analysis across industry peers and other relevant sectors."**
>
> **— CISO, Industry-Leading North American Energy Company**

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 ecosytem 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