IronNet Attack Assessment

Overview

Bringing together some of the best minds in cybersecurity and an unmatched team of experts from industry, government, and academia, IronNet was born to more effectively defend enterprises, sectors, and nations against highly organized cyber adversaries and increasingly sophisticated attacks. IronNet is continually creating solutions to address the exponentially advancing cybersecurity threats on a more holistic, global level. Today, our revolutionary Collective Defense approach is enabling nations and enterprises to defend against emerging threats in real-time as a unified front.

Network Detection and Response (NDR) technology is critical in combating today's sophisticated cyber criminals providing the ability to determine if attackers are in your network,what they are doing and if they have caused harm. Purpose-built for this mission, IronNet has thecapability to detect attackers who are continually looking to exploit vulnerabilities across your enterprise's expanding attack surface. With limited resources and people, cybersecurity teams are stretched thin with limited time to actively look for threats. IronNet was designed to increase visibility, dynamically detect threats, and dramatically reduce the overall dwell time of the attacker.

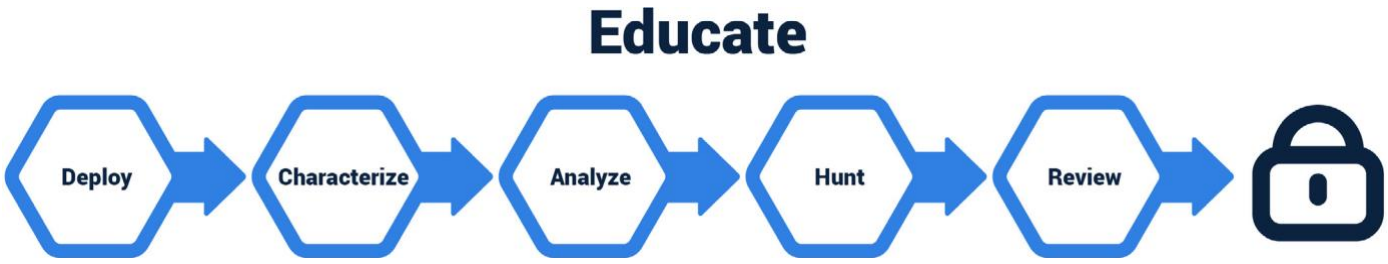
The IronNet Attack Assessment combines human expertise in digital forensics with attack intelligence supported by the company's industry-leading behavioral analytics that power IronNet'sNDR technology. This assessment focuses on education, identifying potential risks, reviewing active attacks, analyzing potential threat actor activity, and executing a Red Team simulation to determine your attack readiness.

Scope

IronNet IronDefense	Up to 5 Gbs of traffic analysis
IronDome	Attack Intelligence and correlation
Duration	30 Days
Number of appliance	1
Timeline/Process	Week 1: Characterize
Timeline/Process	Week 2: Understand
Timeline/Process	Week 3: Hunt
Timeline/Process	Week 4: Analyze
Time Commitment	3 hours per week

Methodology

After deployment, IronNet's highly skilled cyber solution engineers characterize your network and the protocols that are running on it to look for potential attack vectors into the environment. Once these have been reviewed, we take a comprehensive look at the network, using IronNet's industry- leading analytics to determine if threat actors are currently present in the network. After this analysis is completed, we conduct a formal after-action review, in which we answer questions anddetermine next steps.



Week 1: Characterize

The key to any effective cyber security strategy is understanding what you need to defend before you can successfully defend it. Week 1 of the Attack Assessment focuses on the characterization of your environment by operationalizing the IronDefense platform and conducting threat surface assessment. Leveraging IronNet's cutting-edge technology, IronNet will conduct an analysis of your network security posture. Our passive detection technologiesminimize our deployment footprint to stay hidden from attackers. Understanding your attack surface is critical to measure your cyber risk.

GOALS:

1. Successfully deploy and validate analytics
2. Training on the use of NDR tools in your network
3. Initiate threat surface analysis

Week 2: Understand

Once a bad actor penetrates the outer defenses of your network, it is up to you to stop them. One highly effective method is ensuring vulnerable systems and legacy protocols are eliminated or strictly controlled. By limiting the attack surfaces your network provides to bad actors, you will significantly inhibit or prohibit lateral movement. IronNet will conduct a comprehensive assessment of known security issues that may be negatively affecting your organization security posture today.

In conjunction with this review, IronNet's cyber solution engineers will directly engage with your staff to show them how to triage alerts and interact with the IronNet CyOC (cyberoperations center). As part of this ongoing education, you will learn how to use the tool to help detect both known as well as unknown attacks. More importantly, you will learn how to engage with IronNet when you need guidance. We will conclude the week with a Red Team simulation that shows the detection capabilities of the platform and provides real-world test cases to facilitate the triage ofsimulated threats.

GOALS:

1. Review IronDefense alerts and conduct baselining
2. Learn how to triage top indicators of attack
3. Conduct Red Team simulation

Week 3: Hunt

When was the last time you were asked, "Are we impacted?" when a headline announced a new ransomware or cyber-attack? Week 3 of IronNet's Attack Assessment revolves around a deep dive of the activity IronNet is ingesting and the associated alerts generated by the analytics. This deep dive is led by some of the top cyber threat hunters in the industry. They will teach your team tactics, techniques, and procedures (TTP) cyber attackers use and how to spot those activities with the IronDefense platform. More importantly, by the end of Week 3, you will be able to confidently say you do not have bad actors or advanced persistent threats in your network.

GOALS:

1. Answer the question, "Are we in the middle of an undiscovered cyber-attack?"
2. Minimize dwell time of potential attackers via early detection
3. Get a global picture of what is happening in your community of interest
4. Review all threat actor activity and remediation techniques

Week 4: Analyze

In Week 4, we review the findings of the assessment. We will review the vulnerabilities found in your threat attack surface and detections found by IronNet analytics. From this after-action review, we will determine nextsteps to help keep your network secure. In addition to a better understanding of your network you will have peace of mind attackers are not actively hiding in your network. Join with IronNet on our mission to help secure your network and confidence that your system has been analyzed for vulnerabilities by IronNet's team of expert hunters and solution engineers.