THREAT VISIBILITY

Known, unknown, advanced persistent threats (APT) – today's networks face a diverse threat landscape while managing a growing diversity in devices. Mobile, cloud, virtualization, IoT all bring with them different threats. This increase in attack vectors makes threat visibility a critical component of IT strategy.

Iron Bow Technologies has the expertise to assess customer networks, provide security technology solutions that address security challenges and successfully deploy security solutions to provide protection against today's advanced attacks.

THREAT VISIBILITY THROUGH TRAFFIC VISIBILITY

Visibility into traffic traversing the network is vitally important to obtain a baseline of normal traffic flow, and from that baseline, be able to detect misconfigured devices and malicious attacks. Mature technologies, such as Netflow and Intrusion Prevention Systems, are critically important in providing insight on traffic within the corporate environment.

Today's organizations need to build on the data provided by these systems by integrating new security tools to:

- Mine raw data to provide an enhanced look at the security of a network including identifying command and control traffic and unexpected source traffic
- Pull a needle from a haystack by being alerted to even small variances in data type, traffic level and performance metrics
- Integrate with public security databases such as Virustotal and Spamhaus for the most up-to-date threat information
- Extend visibility to all endpoints to address the reality of a mobile workforce and enable the ability to block end-user traffic whether it is connected to the network or not

Threat visibility tools have a threefold impact on an organization

1. **Security** – increase the security posture of an organization including reducing risk from ransomware attacks and protection against competitors stealing valuable intellectual property
2. **Budget** – justify security budget by visually illustrating the continual threats the network faces
3. **Performance** – insight into bottlenecks and throughput/latency issues, allowing them to be remediated before they cause an outage or a loss of performance

IRON BOW IN ACTION

Threat visibility is part of a Continuous Diagnostics and Mitigation (CDM) approach to security. Being able to see what threats are hitting your network allows for more effective security and budget planning. In one case, an Iron Bow client began using a threat visibility tool and immediately saw probes from foreign countries and traffic from their network going to foreign countries. This visibility provided two critical functions. First, it was a graphical method of easily seeing when a breach has occurred. Second, it provided clear justification for the security budget. In this case, the attacks were unsuccessful, but the customer learned they were being attacked on a regular basis from places they never imagined. Examination over time brought to light a data exfilitration problem.

4800 Westfields Boulevard, Suite 300, Chantilly, VA 20151
703.279.3000 800.338.8866 | info@ironbow.com | www.ironbow.com

It was not malicious but instead was tied to a user that was trying to make sure the data they used was preserved by archiving records to their home storage device. The user did not realize the security ramifications if their home storage device was compromised, and through user education closed that vector. While that attack was really a non-issue, having the visibility into the threats coming at the network day in and day out, the IT team was able to better justify ongoing security investments.

Iron Bow has the expertise and experience to understand organization use cases, recommend the best solution, and ensure that the solution is successfully deployed in an operationally sustainable method.

STRONG. Our security specialists have in-depth knowledge on the latest attack methods and how to defend against them.

FLEXIBLE. By understanding threats, organizations can offer the diversity of access options that users demand and expect.

TARGETED. Our goal is to find the needle in the haystack by understanding what is normal traffic and immediately flagging any outliers in that flow.

4800 Westfields Boulevard, Suite 300, Chantilly, VA 20151
703.279.3000 800.338.8866 | info@ironbow.com | www.ironbow.com