IP Address Audit Checklist: A 10 Step Guide

Quickly securing your Internet Edge is an urgent business imperative, and must start with a baseline audit of the IP addresses that are relevant to you, not only those directly registered to you, but also those IP addresses that host digital assets your organization exposes to the public Internet.

10 Step Checklist

- [ ] **Identify the IP ranges that are directly registered to your business through a Regional Internet Registry (RIR), or through advertisement by Autonomous System Numbers (ASNs)**
  - Are these IP addresses responsive to the Internet?
  - Are all IP addresses advertised by your ASNs registered to you?
- [ ] **Identify IP space hosting your services at third party providers**
  - Cloud providers, MSSPs, and shared office buildings (such as building controls), host your business-critical services but are often not well tracked.
- [ ] **Map IP address ranges to business impact (subsidiary, joint venture, business unit, etc.)**
  - Identify which IP address ranges belong to your core business, your subsidiaries, or your joint ventures.
  - Know which business unit is allocated to which IP address range.
- [ ] **Identify “Shadow IP addresses”**
  - Do you have active services on the Internet hosted in IP address space unregistered to you or to a third party with which you have no formal relationship?
- [ ] **Validate each IP address range**
  - What services are present on these IP address ranges?
  - Was this IP address range being tracked on any existing list at your business?
  - Make sure newly discovered IP address ranges are appropriately configured, and update your existing infrastructure to reflect deprecated ranges (e.g., update firewall whitelists).

- [ ] **Ensure registration information is uniform and authorized**
  - Correct any misspellings, and ensure each point-of-contact (POC) listed is still employed at your company.
  - Consider implementing a specific format for how IP address ranges should be registered.

- [ ] **Ensure POCs are associated with each IP address range, and that information is up to date**
  - Make sure each IP address range has a point of contact associated with it.
  - If multiple teams are responsible for an IP address range, consider assigning a POC for each team to that range.

- [ ] **File tickets with RIRs for deprecated ranges**
  - Are there any address ranges attributable to your business due to outdated registration information?
  - Deprecated registration information can affect your security rating scores if they host critical services left open to the Internet. File a ticket with the RIR hosting that registration to get the information up to date.

- [ ] **Share this information across all your relevant teams**
  - Information is useless if not shared. Empower cross-functional collaboration across your IT Operations, Security Operations Center, Vulnerability Management, and any other relevant teams by ensuring they all have the same information.

- [ ] **Be diligent about re-auditing your IP address space over time**
  - Even statically-allocated IP address space is dynamic. Expanse routinely observes significant IP address changes on the Internet Edge of large organizations due to mergers, divestitures, errors, and other reasons. Re-audit your IP addresses on a continuous basis to ensure your Internet Edge conforms to your company's policies.

Learn More

Expanse, formerly Qadium, a San Francisco-based SaaS company, provides IT and security teams with complete visibility of the assets and risks on their global Internet Edge. This enables our customers, Fortune 1000 companies and major government agencies, to quickly and efficiently eliminate these risks. Through technology and service expertise, we surface and help remediate Internet Edge risks to prevent large breaches and successful attacks.

Contact sales@expanseinc.com for further information about how Expanse can help your organization evaluate acquisition targets, and assess Internet Edge hygiene and risks.