A10 Networks DDoS Security Incident Response Team

While multi-vector DDoS attacks are increasing in frequency, severity and duration, the need for DDoS attack mitigation is paramount to secure the edge of cloud infrastructures.

The A10 Thunder TPS solution detects and mitigates DDoS attacks to help ensure your infrastructure is safe and your business remains operational.

Thunder TPS provides agile, efficient and network-wide protection against the full spectrum of DDoS attacks. This includes the challenging multi-vector attacks that use a combination of high-rate volumetric or network protocol attacks and more sophisticated application attacks.

To further enhance this proven protection, A10 delivers the 24-7 DDoS Security Incident Response Team (DSIRT) that lends aid when a DDoS attack is targeting your infrastructure and business continuity is in jeopardy.

What is DSIRT?

Highly specialized and CSX Cybersecurity-certified, DSIRT is available to support your organization in the event of a DDoS attack against your infrastructure.

- **Around-the-clock defense.** Protect your business with immediate, 24-7 emergency response to mitigate DDoS attacks and restore service to applications and your business.
- **Fully certified.** Trust A10's highly specialized, ISACA-certified team, which is trained to handle a variety of DDoS-based security events, including the latest 1 Tbps-plus attacks.
- **Shared intelligence.** Leverage the knowledge from external attack events, which is shared globally amongst DSIRT to help mitigate new attack types and protect all A10 customers.
- **Real-time threat data.** The service also includes the A10 Threat Intelligence Service so you are protected with real-time threat feeds and dynamic updates.

Technical Support for DDoS Attacks

Immediate Assistance with "Follow-the-Sun" Support	A10 offers 24-7-365 technical support teams in multiple locations around the world, including Amsterdam, Beijing, Tokyo, Cary, N.C., and our Silicon Valley headquarters in San Jose, Calif.
DDoS Mitigation Expertise	DSIRT is highly skilled in cybersecurity and delivers deep expertise in DDoS mitigation techniques and attack vectors.
CSX Cybersecurity Certification	To leverage in-depth knowledge of the cybersecurity landscape, A10 requires DSIRT members to be ISACA CSX Cybersecurity-certified. With more than 140,000 constituents in 200 countries, ISACA is the leading international professional association focused on IT governance.
Fast-path Escalation	With this service option, your issue will be escalated and managed faster. Gain an accelerated path to higher levels of support engineers and management teams.
Dedicated Phone Line	Access to a dedicated telephone line for faster access to DSIRT.
Security Case Queue	Bypass general support and gain direct access to the Security Case Queue. Receive closer attention and monitoring, resulting in quicker response times.

A10 Threat Intelligence Service

Proactive Defense Policy	The Threat Intelligence Service includes ongoing protection against attack vectors by automatically delivering live threat data to your network devices.
Block Command & Control Servers	Ensure your users can safely connect to the Internet. Prevent threat actors from using them as an attack vector to extort or exfiltrate your data, or turning your network into a botnet for criminal use.
Real-Time Indicator Threat Feeds	Threats are continuously discovered by our security researchers, tracked by 50-plus threat intelligence sources. We integrate these feeds and automatically share as policy updates to the A10 platform.
Granular Control of Outbound Traffic	Determine the action needed when an endpoint attempts to connect with a threat actor. Connections can be blocked with an error response, blocked with no response, allowed to pass, or dropped with no response.
Dynamic Threat Vector Updates	The policy is automatically updated to block new threats and no longer block access to locations that have been remediated.
Ease of Use	Setup is simple. It only takes a few minutes for subscribers to select one of our standard policies or create their own custom policy in our portal.

DSIRT Response Time

With A10 DSIRT, each customer case is closely monitored until resolution. Depending on the priority of the problem and the elapsed time, key management personnel are engaged to bring crucial resources to resolve the issue in the quickest possible time.

Our DSIRT Service Level Agreement (SLA) response times are as follows:

Priority	Response Time	Status Update	Management Escalation
1: Critical	Immediate	Every 2 Hours	Immediate
2: High	30 Minutes	Every 4 Hours	1 Hour
3: Medium	2 Hours	Every 3 Business Days	5 Business Days
4: Low	4 Hours	Every 7 Business Days	N/A

More Information

To inquire about the A10 Networks DSIRT service, please contact Sales@A10Networks.com.

About A10 Networks

A10 Networks (NYSE: ATEN) provides secure application services for on-premises, multi-cloud and edge-cloud environments at hyperscale. Our mission is to enable service providers and enterprises to deliver business-critical applications that are secure, available and efficient for multi-cloud transformation and 5G readiness. We deliver better business outcomes that support investment protection, new business models and help future-proof infrastructures, empowering our customers to provide the most secure and available digital experience. Based in San Jose, Calif., A10 Networks serves customers in 117 countries worldwide. For more information, visit: **www.a10networks.com** and follow us **@A10Networks** on Twitter.

Learn More

About A10 Networks

Contact Us
a10networks.com/contact

Part Number: A10-SCE70191-EN-02 APRIL 2020