A10

DDoS Threat Intelligence: Leveraging AI to Meet Evolving Threats

Enhance the Depth, Accuracy, and Proactiveness of your DDoS Defense

DDoS, the number-one threat incident, drives the need for specialized defenses. Recognized by top researchers as a fast-growing sector, threat intelligence requires unique implementations, which can benefit from generative AI technologies. Traditional solutions, broad but shallow, are reactive. **A10 Defend Threat Control, powered by AI and human expertise, offers high-confidence, in-depth, and proactive DDoS defense.**

Use-case 1:

AI-enhanced Granular Insights

A large organization with general threat intelligence deployed requires a more accurate and concentrated list with depth on specific DDoS attacks. This is likely due to general threat intelligence lists that only cover a limited number of DDoS vectors, which are not representative of the breadth and complexity of how DDoS attacks are conducted today. Additionally, general threat intelligence is oftentimes crowd-sourced instead of undergoing an extensive AI-enhanced research methodology to ensure low false positives. Finally, most lists are reactionary because they are signature-based. Deploying Defend Threat Control will provide a proactive, in-depth, and accurate solution that can remedy the existing challenges.

Use-case 2:

High-confidence, Actionable Block Lists

A large organization with existing firewalls, IDS, or other security devices have limited DDoS protection because it is not the core functionality of these devices. A dedicated DDoS threat intelligence service with high efficacy can help bolster the overall security posture, because DDoS attacks can hinder the performance of any other defense systems, including a IDP solution, zero trust architecture, and others. A10 Defend Threat Control helps provide high-confidence actionable lists that can be ingested by top firewall providers. This is especially effective for those who do not possess a dedicated DDoS solution. Deploying Defend Threat Control can help check the health of security devices, and also generate highly actionable and confident block lists which can be integrated within the organization's IDS, firewall, or other security device.

| A10-GR-70361-EN-01

The A10 Defend Threat Control Advantage

- ✓ Stop more DDoS attacks with deeper coverage of DDoS protocols
- ✓ Advanced AI/ML-based intelligence network fuels improved dataset with low false positives, reducing impact of DDoS attacks
- ✓ Assess the external threat landscape beyond the network perimeter, but retain industry-specific and global state of DDoS attacks; stay ahead of upcoming threats

> “*Organizations continue to experience skill shortages and look for opportunities to automate resource-intensive cybersecurity tasks. Use cases for the application of generative AI include, synthesizing and analyzing threat intelligence.*
>
> **— Gartner 2023**”

Contact Us for a Solution Planning Session

408-325-8668

A10networks.com