The 5 Phases of Custom Risk Scoring

Why you Need a Client Reputation Risk Analysis Engine that Computes a Risk Score for Every IP Address

Akamai

Overview

Client Reputation is an optional module for Kona Site Defender. It computes and assigns customer-specific risk scores to malicious web clients, identified by their IP address, based on their propensities to engage in attacks. Attack types include:

- Application layer attacks
- Denial of service (DoS) attacks
- Vulnerability scanning
- Web-scraping activities

The high quality of the Client Reputation service is driven by the intelligence and threat insights provided by Akamai's Cloud Security Intelligence (CSI) platform. This platform processes billions of security events and legitimate traffic logs per hour, using the data to forecast the likelihood of a client to pose risk to specific customers.

CSI's analytical processes include:

- Sophisticated attacker behavioral profiling
- Detection of malicious payloads and zero-day attacks
- Analysis of common malicious traffic patterns
- Clustering of malicious activities performed by botnets

Many reputation services that are on the market today provide only a single client reputation score, which is the same for all customers. Client Reputation, however, uses a state-of-the-art, proprietary risk analysis engine that computes a risk score for every source IP address, customized for every customer. This custom risk-based scoring model is significantly more accurate than generic scoring, and it has shown that actions taken based on the risk score are less likely to negatively impact legitimate clients and users.

Client Reputation uses a state-of-the-art, proprietary risk analysis engine that computes a risk score for every source IP address, customized for every customer.

In recent years, the threat landscape's complexity and sophistication evolved dramatically. Malicious actors now leverage different attack tools and methods of operation. In addition, they are using compromised or low-cost resources, like IoT devices, compromised servers, and cloud infrastructure to mask their activity or orchestrate mass-scale attack campaigns. Given the abundance of such cheap attack resources, these resources may only be used for a specific attack campaign and likely do not pose any risk to other customers. In addition, many attack campaigns last for a short time period. After that, the resources used for the attack campaign might not pose further risk to customers.

As a response to these trends, Akamai developed its custom risk-based scoring model, which is capable of assessing the real risk each client poses to each Akamai customer at any given time.

The key for computing a more powerful scoring model is knowledge extracted from high-quality big data. Akamai leads the Content Delivery Network market as a central hub in the Internet ecosystem, serving 15-30% of all web traffic at any given moment.

Akamai leads the Content Delivery Network market as a central hub in the Internet ecosystem, serving 15-30% of all web traffic at any given moment.

Leveraging this unique position, Akamai sees both legitimate and malicious traffic traversing the Akamai platform. Akamai uses the Cloud Security Intelligence platform to track and classify malicious clients as belonging to at least one of these risk score categories:

- **Web Attackers –** Web clients or actors who perform generic web-oriented attacks such as SQL injection (SQLi), remote file inclusion (RFI), or cross-site scripting (XSS).
- **Denial of Service (DoS) Attackers –** Web clients or botnets that use automated tools to launch volumetric DoS attacks
- **Scanning Tools –** Tools used to scan web applications for vulnerabilities during the reconnaissance phase of an attack
- **Web Scrapers –** Automated tools used to harvest information such as pricing data from web pages in a systematic fashion

The Client Reputation module computes a risk score on a scale of 1-10 for each category. A risk score of 1 forecasts a low likelihood of future attacks by that client, while a risk score of 10 forecasts a high likelihood that the IP address may be used by a malicious actor.

Once these risk scores are assigned to a client for a specific customer, they are shared with and applied to the Edge servers on the Akamai Intelligent Platform™. Customers using the Client Reputation module can then choose how Akamai's Edge servers will handle clients with a specific risk score.

A common practice is to alert when the risk score of a client is equal to or higher than 5, and block when the risk score is equal to or higher than 9. These scores reflect the trade-off between the chances of a future attack and the possibility that the client will also generate future legitimate traffic.

In conjunction with the risk score, Akamai customers can further adjust the security measures by applying additional conditions, like:

- The source IP's Autonomous System Number (ASN)
- IP or GEO network lists
- IP address/CIDR
- Specific HTTP header names and/or values
- Specific HTTP cookie names and/or values
- Target hostname
- Target HTTP request path

The following two examples demonstrate how Akamai customers can benefit from applying additional conditions described above:

1. Although businesses thrive in a global economy, many customers conduct most of their business with partners and consumers in a limited number of geographic regions. Therefore, customers can easily take more severe actions against malicious IPs coming from specific geographies or source networks that are not part of their business.
2. In some cases, activities between business partners may seem malicious and will be flagged. However, interactions between business partners' IT systems are usually set up to occur from specific source networks and to send HTTP requests using specific headers and/or cookies. Hence, customers that wish to ignore traffic from these partners — so that it will not be denied by the reputation controls — can use the conditions to exclude and not block any traffic originating from specific networks, headers, and cookies.

How Custom Risk Scores Are Computed

Client Reputation's risk analysis engine executes five separate analysis phases. At the end of all phases, a custom risk score is computed for the malicious actor and propagated to the entire Akamai Intelligent Platform™ on an hourly basis.

Phase #1: Malicious Activity Identification and Classification

Client Reputation identifies malicious actors through a variety of techniques, including behavioral analysis, statistical models, and attack signatures. During this phase, Client Reputation leverages client fingerprinting and behavioral clustering techniques to detect botnets. This is very powerful, because when analyzed in isolation, clients may appear harmless; it is often overlooked that they collectively cause greater harm as part of a much larger botnet.

Phase #2: Custom Risk-score Calculation

A custom risk score is calculated per category and per customer by factoring in the following measures:

- **Attack magnitude –** the amount of generated malicious traffic
- **Attack distribution –** the number of attacked targets
- **Attack persistency –** the frequency of malicious traffic over time
- **Attack severity –** the potential damage that the attack can cause
- **Target severity –** the potential damage that the attack can cause
- **Target industry –** the industry vertical that the malicious actor tends to target
- **Target Akamai customers –** the specific customers that the malicious actor tends to target

In addition to the factors noted above, the risk analysis engine classifies malicious clients based on type and previous behavioral patterns. This helps Client Reputation to better understand the nature of the attacker — whether a compromised device is being used consistently, or whether the IP was used only for a single event and is not expected to participate in future attacks. These factors affect score calculation and provide intelligent context-aware decay.

Phase #3: Error Correction Heuristics and Auto-tuning

In some situations, legitimate clients demonstrate behavior that might seem invalid or suspicious. For example, clients may send large volumes of traffic in a short period of time, or HTTP messages containing potentially hazardous payloads (SQL queries, PHP code, and others).

In order to avoid assigning risk scores to legitimate clients, the risk analysis engine contains multiple layers of error-correcting heuristics and auto-tuning mechanisms that not only cluster and analyze events as a whole, but also apply mitigation controls.

Phase #4: Shared IP Detection

Some IPs on the Internet are shared by many end users, including corporate security gateways, NAT gateways, mobile gateways, and proxies. In order to ensure that the system does not penalize legitimate users that share their IP address with potentially malicious actors, Client Reputation automatically applies multiple layers of shared IP detection such as behavioral analysis, fingerprinting, and IP address classification. IPs that are detected as shared are whitelisted or treated appropriately — for example, malicious proxies or anonymizing VPNs that only generate malicious traffic might still be assigned a risk score.

Phase #5: Reputation Risk-score Recovery (Decay)

In cases where an IP no longer poses risk, its score will reduce over time. The rate at which score decays depends on features such as:

- Type of malicious activity
- Persistence of the malicious activity
- Frequency of previous malicious events
- Magnitude and distribution of relevant previous activities

Akamai Threat Operations

System health monitoring is continuously performed by Akamai's Threat Operations team. The team is staffed by industry-leading application security researchers and data scientists using a variety of statistical analysis and machine learning tools. The team is responsible for guaranteeing the integrity and accuracy of the system and its data, as well as identifying and researching large-scale events and patterns that require special human attention.

Summary

Client Reputation adds a sophisticated intelligence-based protection layer to web application delivery. Client Reputation leverages the threat insights of Akamai's unique Cloud Security Intelligence platform, which continuously analyzes as much as 30% of all web traffic from thousands of web applications spanning the globe and industries.

At the heart of Client Reputation lies a state-of-the-art, proprietary risk analysis engine. This engine computes a custom risk score for every IP, per customer, depending on the actual risk an attacker poses to that customer. The custom risk score is recalculated regularly and takes into account malicious activity classification, error correction heuristics, shared IP detection, and risk decay over time. Using an accurate, customized, risk-based scoring model to customize application delivery to each client significantly enhances application security while reducing the chances of business loss as a result of denying potential legitimate clients.

Operational and technical benefits of Kona Client Reputation include:

- An additional intelligence-based layer of defense against malicious activities such as web application layer attacks, denial of service attacks, vulnerability scanning, and web scraping
- Improved security decisions based on previous activities of malicious actors
- Ability to stop malicious actors before an attack takes place
- An additional source of intelligence for back-end security systems

Client Reputation Scoring

- Visibility into 15 to 30% of all web traffic
- Accurate in-house data analyzed within context
- Tailored to each customer's business
- Calculated from malicious and legitimate client behavior