Cleafy

CLEAFY Threat Detection: a New Approach against Advanced Attacks

SOLUTION
WHITEPAPER

Table of Contents

TABLE OF FIGURES

Introduction

This whitepaper describes Cleafy new approach and threat detection capabilities against today advanced threats resulting from compromised endpoints.

Cleafy solution is based on unique, client-less, real-time integrity detection, pattern clustering and malicious code extraction technology. Cleafy seamlessly integrates with server-side infrastructure (at Application Delivery Controller level), does not require any application change and is completely transparent to end-users. Furthermore, Cleafy provides threat protection capabilities and can also be integrated with risk-based authentication systems and Security information and event management (SIEM) systems, thanks to its open architecture.

Cleafy can protect against a variety of advanced attacks from compromised web client and mobile devices, including Man-in-the-Browser (MITB), Man-in-the-Middle (MITM), RAT-in-the-Browser, VNC/BackConnect, OTP grabbing and Mobile Overlay. These are the types of attacks performed today by fraudsters against financial and e-commerce services and that are not detected by other solutions.

Cleafy protects both users and on-line services by ensuring the business continuity even in cases of compromised endpoints. Moreover, Cleafy unprecedented level of real-time visibility on endpoints – down to snippets of injected code – improves operational efficiency of Security Teams and their ability to manage zero-day attacks, to prevent advanced targeted attacks specifically designed to compromise their company applications, and to conduct all required forensic investigations and other cyber-security activities.

Cleafy has been adopted by companies belonging to a variety of market segments, including financial services, e-commerce [1], gaming and gambling and others. Cleafy technology has been validated by major corporate and retail banks with millions of users and billions of events a day.

The problem

Today cyber-attacks are becoming more and more sophisticated. Depending on the market segment, negative consequences may include financial losses due to frauds, operational disruption, brand and reputation damage, customer dissatisfaction, regulatory fines, loss of proprietary information, sensitive data or other strategic assets [2].

The estimated cost of malicious attacks has been estimated by a recent report to reach about $7.7M per company, with the annual cost to the global economy from cybercrime is more than $400 billion [3] [5]. About 76 percent of worldwide organizations are reported to have been compromised [5]. Financial Services companies have been specifically targeted all around the world, with the number of cyberattacks growing 3.6 times in the last 3 years [6] [7] [8] [9].

It is widely acknowledged when it comes to securing online transactions, endpoints represent the weakest link in the chain [10] [11]. As a matter of fact, most of the advanced attacks performed by fraudsters against online financial services leverage compromised endpoints.

As reported by recent research, as much as 30% of web clients [12] are compromised by malwares. While for mobile devices it is more difficult to provide equivalent figures, it is also recognized that mobile applications are also exposed [13] [14]. The exposure of mobile applications is expected to grow as they will be used, for example to perform banking transactions, as it is already the case in some geographies.

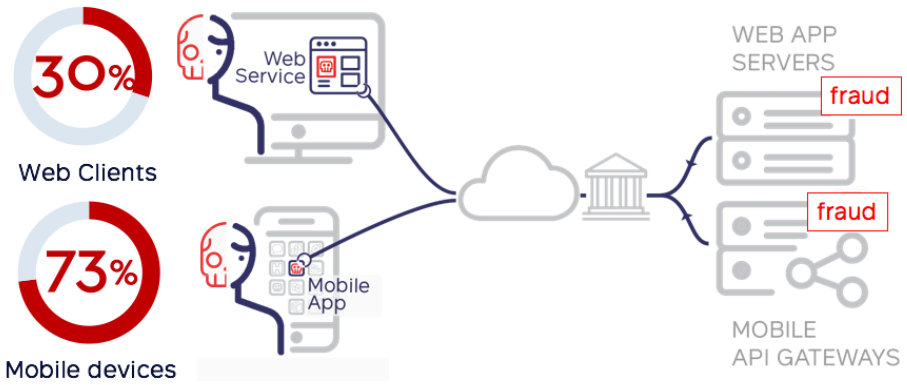

Figure 1. The scenario in today's on-line transactions

This scenario is getting worse as since previous year there has been a net increase in new malwares and variants (+36%) and zero-day vulnerabilities (+125%) [6] [7].

CLEAFY APPROACH

In the context described above, Cleafy has adopted an entirely different and innovative approach than any other solution available on the market.

Indeed, client-side solutions such as Enterprise Endpoint Protection Platform (EPP) [15] or Endpoint Detection and Response (EDR) [16] that aim at identifying (and removing) malwares are known not to be not very effective [15]. Moreover, today malwares are designed to by-pass these endpoint-based controls [H]. Finally, the cost for manage endpoints should not be underestimated, in particular when these endpoints are outside the company security perimeter.

Server-side solutions such as Web Application Firewalls (WAF) [17], that perform some syntactical analysis of the HTML code to recognize application anomalies at session level, or traditional On-Line Fraud Detection [18] solutions, that focus on identifying anomalous transactional or navigational patterns via behavioral analysis, fail to detect threats from today advanced attacks, which may involve multiple concurrent sessions, and can mimic normal user behavior (such as velocity and navigational patterns).

While all these solutions should be considered as components of a solid layered security infrastructure [19], a new approach is required today [20]. Cleafy innovative approach to threat detection is based on a (patent-pending) client-less, full integrity detection, pattern clustering and multi-entity correlation technology.

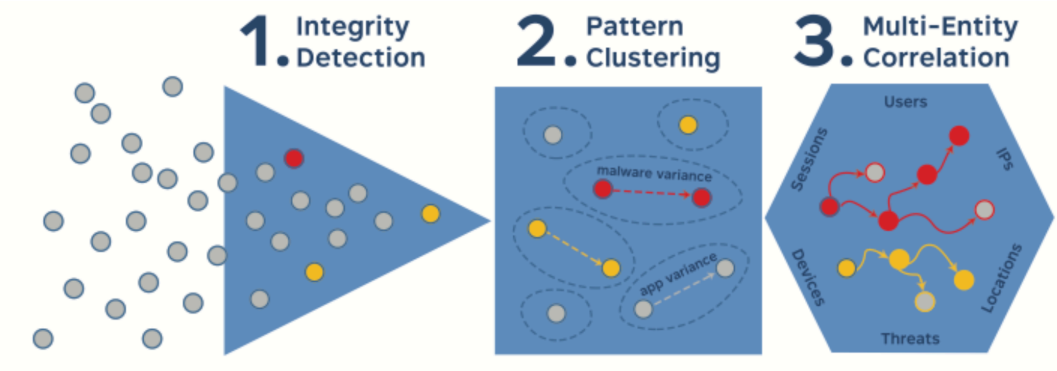

Figure 2. Cleafy in a nutshell

Cleafy Integrity Detection

Cleafy integrity detection provides the ability to verify in real-time whether the source code (and exchanged data) generated by the server side has been modified when executed on the client side. With respect to other solutions that use pattern matting and signature analysis, Cleafy performs a full code integrity check, not just simple pattern-matching analysis, at DOM (Document Object Model), XHR and API level calls. Therefore, Cleafy supports threat detection also for modern, dynamic applications.

Cleafy threat detection capabilities are based on the server-side injection of some JavaScript code (aka Cleafy Agent Script) that send signals back to the Cleafy Engine as described in the following flow (for web applications):

- [*server-side*] when the user asks for a resource (e.g. a webpage), Cleafy injects the Cleafy Agent Script in the generated page that is then sent to the client; Cleafy also stores a copy of the original resource (webpage) generated;
- [*client-side*] when the resource is executed on the end-point (e.g. the webpage is rendered in the browser), the Cleafy Agent Script is executed in the browser rendering space and it collects and sends back to Cleafy the rendered source code (along with a set of additional context information);
- [*server-side*] Cleafy compares the original and the rendered resource (e.g. webpage) thanks to Cleafy real-time integrity detection algorithms, and in case of integrity violations: i) categorizes identified threats; ii) recalculates risk score and iii) extracts snippets of malicious code;

Basically, Cleafy Agent script operates from the server-side as a virtual agent being executed on the client-side in the browser rendering space.

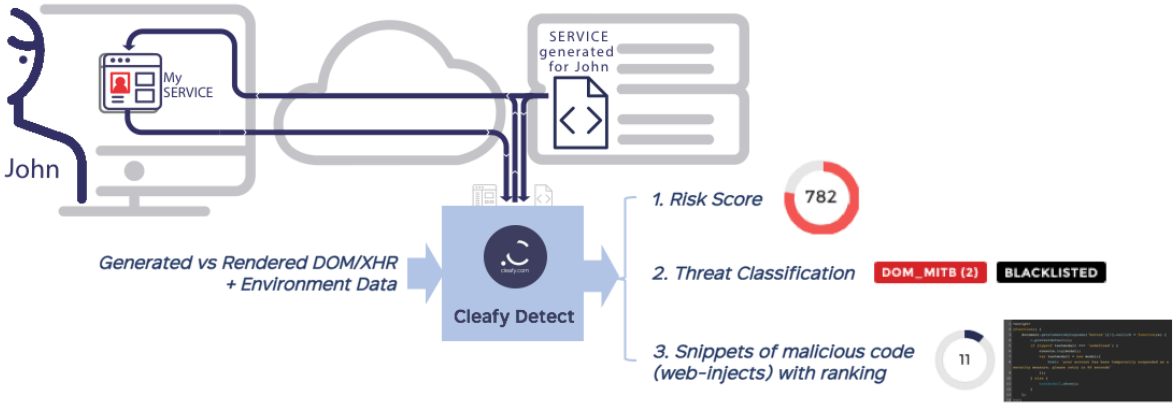

Figure 3. Cleafy Integrity Detection in action

Notice that since all data processing used for data integrity is executed server-side, Cleafy threat detection mechanism are better protected against malware operating on the endpoint. Moreover, Cleafy adopts specific mechanisms ("flag and probes") to detect any data tampering or interference from malwares, which can be detected and highlighted. Finally, Cleafy uses real-time obfuscation techniques based on unpredictable hopping technology to secure the communication between Cleafy Agent script and server side.

It is important to notice that Cleafy neither impacts the end-user experience nor requires any application change. Even in case of native mobile apps, Cleafy provides a passive SDK that can be incorporate without any change to the application. Since Cleafy works by detecting integrity violation and anomalies while analyzing in real-time the application traffic, it does not require knowing in advance the application flow or the structure of the webpages and can continue to automatically protect on-line services across application changes.

The Cleafy Agent script is quite small: its size depends on the specific data collection options that are activated, but is typically <2KB. Since data collection and processing mechanisms are asynchronous with respect to webpage rendering, the Cleafy Agent script does not have to complete for the user interaction to continue. Cleafy architecture can be sized to ensure than collection time (which also depends on the activated options and available endpoint browser/network resources) remains <200ms.

Cleafy categorizes threats leveraging both out-of-the-box tags (e.g. MITB, MITM, SCRAPER, BOT, USER_SPOOFING) and custom tags can also be defined based on a variety of factors such as user-agent (e.g. rendering browser and version), platform (e.g. OS version and language), device type, IP/geo-location and others. A risk weight is associated to each (either out-of-the-box or custom) tag. For each analyzed event (i.e. HTTP request/response), Cleafy calculates in real-time a (normalized) risk score (ranging from 0 to 1000), that is also propagated at session level, and possibly also across sessions as in the case when Multi-Entity Correlation analysis is performed (see below). Alarms can be fired to notify when the risk score associated to a session is higher than a configured a defined threshold (either defined globally or per-application).

Cleafy Pattern Clustering

In addition to identifying threats, Cleafy automatically extracts the snippets of malicious code that have been injected by the malware.

Cleafy extracted code snippets enable cyber-security analysis by making possible to distinguish between targeted and generic attacks and providing actionable info about attacker infrastructure (e.g. IPs of the Command & Control Center). They also provide user experience under attack (e.g. pop-up preventing users from logging-in), insights into attacker Tactics, Techniques & Procedures (TTPs) (e.g. credential stuffing) and support for improving security posture by adopting appropriate response and protection actions (e.g. deflection. Finally, code snippets represent real evidence of potential threats, thus providing additional support for better incident management and forensic investigation activities.

In order to be able to follow the evolution of attack campaigning despite potential malware variances (e.g. variation of query parameters in the URL), Cleafy uses proprietary clustering based on dynamic fingerprinting. This clustering also helps the purpose of avoiding false positives due to applications change without requiring Cleafy to be explicitly instructed on the application structure.

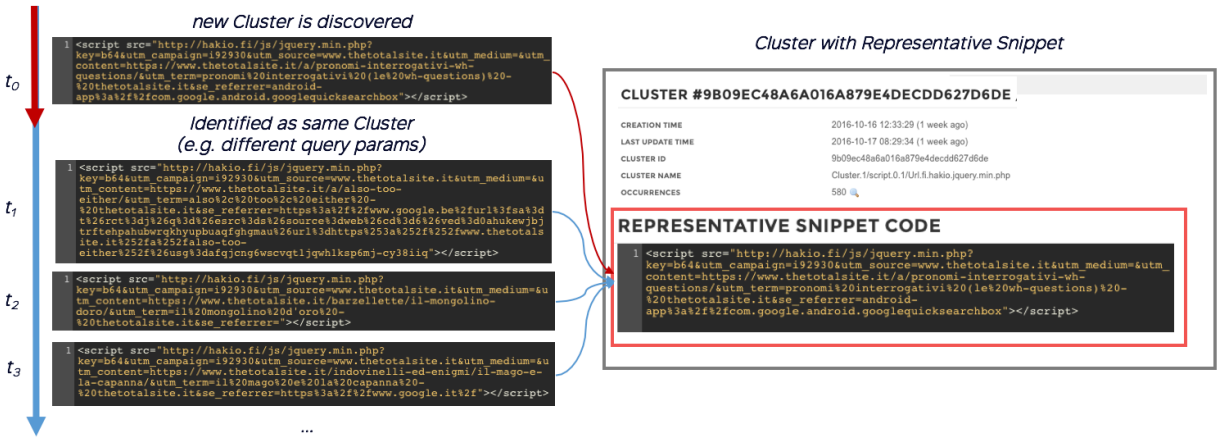

Figure 4. Cleafy Clustering in action

Cleafy Multi-Entity Correlation

Cleafy can correlate threats that have been identified on different entities (e.g. User, IP/Device) and across different sessions and channels, thus identifying attacks that would otherwise go undetected by just performing a session-level analysis and without multi-entity correlation.

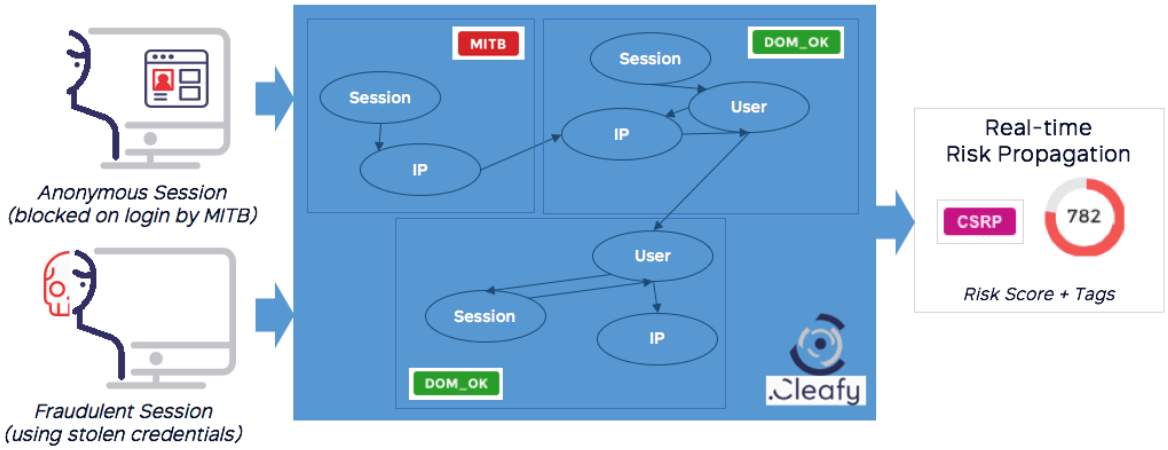

Figure 5. Cleafy Multi-Entity Correlation in action

The previous figure illustrates an example of an attack scenario where a legitimate user session is intercepted by a MITB that captures the user credentials while keeping the user on hold before the login phase is completed (therefore leaving the session as anonymous), while a concurrent session is issued by a fraudster to perform a fraudulent transaction. This is a scenario where Cleafy can identify the user(s) corresponding to the anonymous session, propagate the MITB threat identified on that anonymous session to the (otherwise clean) session performed by the fraudster, thus correctly identifying the risk associated to the overall scenario.

CLEAFY DEPLOYMENT ARCHITECTURE

Cleafy can be deployed either on premise or as a cloud-based service.

When deployed inside the server-side infrastructure, the Cleafy Engine is typically integrated at Application Delivery Controller (ADC) level (see following figure). Several technologies such as F5 BIG-IP, Citrix NetScaler or Array Networks APV are supported.

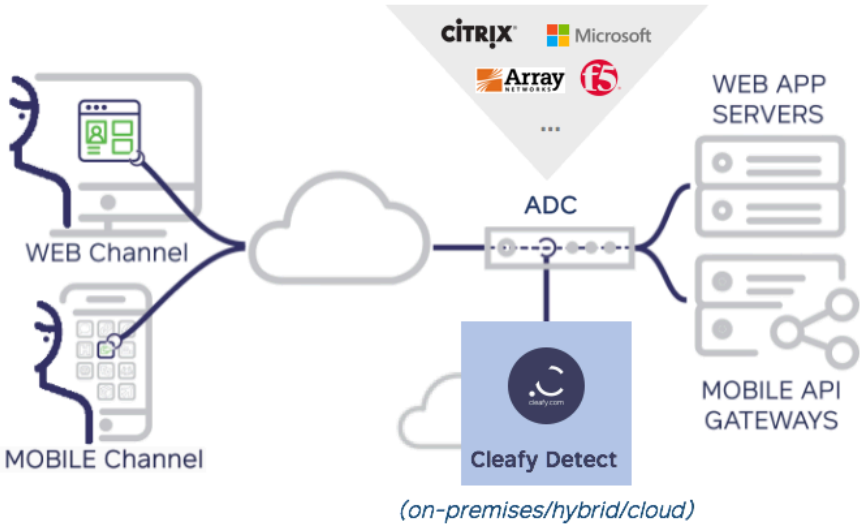

Figure 6. High-level architecture of Cleafy Detect deployment

In general, Cleafy needs to be integrated where SSL traffic is terminated to be able to analyze all pages and data exchanges, including those under SSL certificates. Moreover, the integration at ADC level also provides the mechanism for injecting the Cleafy Agent Script that send all signals back to the Cleafy Engine for supporting integrity detection capabilities.

Notice that Cleafy does not represent a single point of failure and that the main impact on the infrastructure is only represented by additional internal traffic. In any case, Cleafy can be configured to only analyze specific applications and a specific perimeter (i.e. specific URLs) for those application of interest (e.g. login and disposition pages in case of a banking application). It is also worth noticing that different policies can be set in Cleafy to manage different applications.

Cleafy architecture can scale both vertically and horizontally, while only requiring a relatively small infrastructure. For example, for a small environment (e.g. up to 150/200 pages/sec) one single server (e.g. 4 CPU core, 16GB RAM “appliance”) can be adequate.

In general, Cleafy has been carefully designed and implemented to operate in large, high-volume production environments. A good example is provided by device fingerprinting, which when enabled is the only data processing performed by the Cleafy Agent on the client-side. Indeed, several options are available on how device fingerprinting is calculated (e.g. resolution, color depth, fonts or CPU information), to minimize the impact on endpoint. Moreover, fingerprinting execution is broken down in multiple steps across multiple pages to minimize the impact on endpoint performance.

Cleafy Integration Scenarios

Cleafy has been designed and implemented as an open and scalable architecture, by leveraging Big Data components and providing a comprehensive set of APIs.

Cleafy APIs provide access to both collected data (e.g., events, performance stats, HTML error codes) and generated threat information (e.g. risk scores, alarms and snippets) that can be consumed by external systems, such as Case/Incident Management or SIEM solutions.

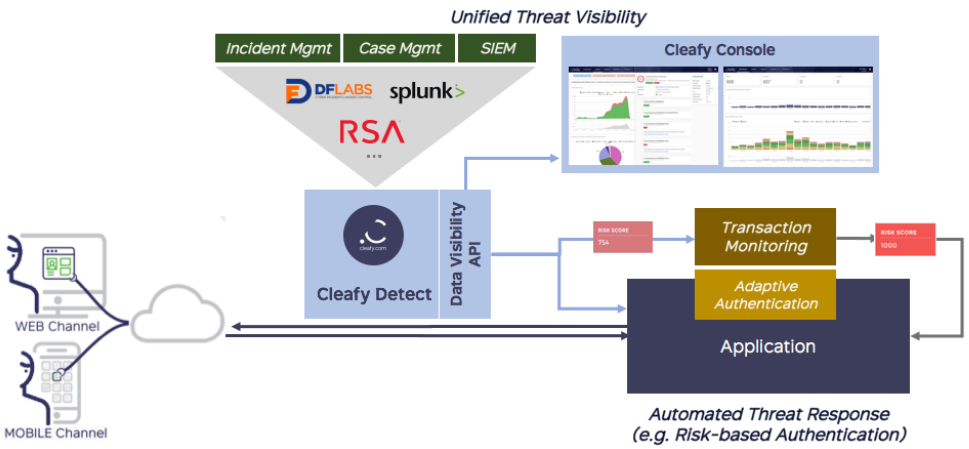

Figure 7. Cleafy integration architecture

Cleafy has also been integrated with Transaction Monitors and Adaptive Authentication solutions (such as RSA AAOP) to enhance risk scoring and friction-less adaptive authentication or to deploy more sophisticated counter-measures, such as deflection (e.g. redirection or dynamic modification of requested resources).

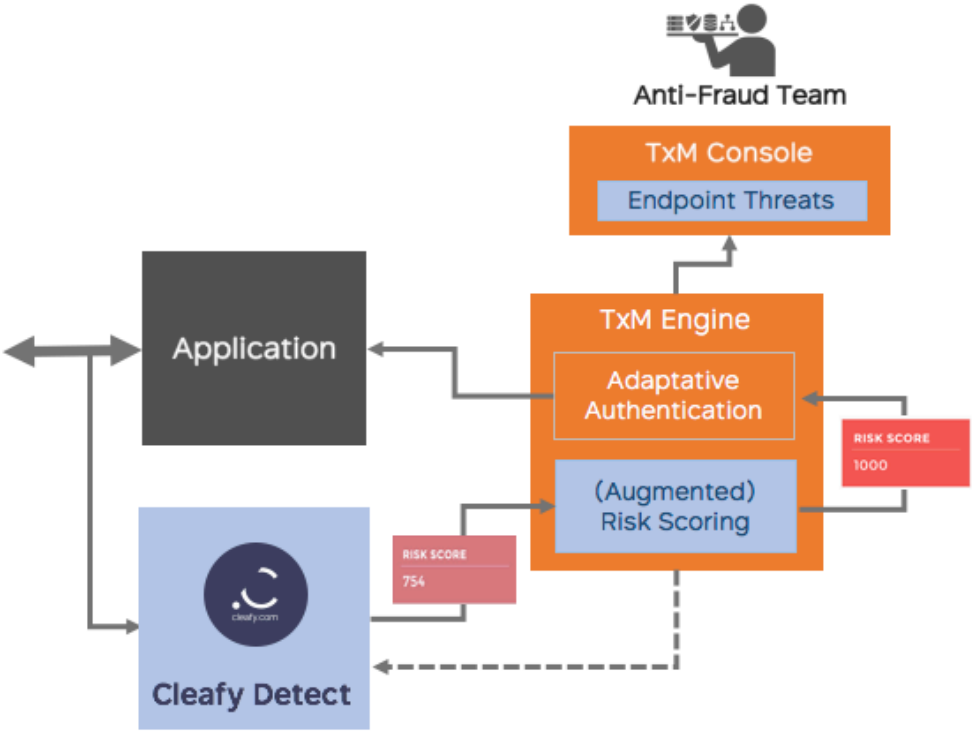

Figure 8. Cleafy as part of a layered approach to security

CLEAFY USER INTERFACE

Cleafy provides a web user interface (Cleafy Console) that has been designed to effectively support threat analysis and cybersecurity activities. The Cleafy Console is multi-tenant and RBAC compliant that allows granular control in terms of visibility and actions that users can perform.

Cleafy comes with three user roles: Admin, Power and Standard User. Basically, Power users can configure Cleafy key functionalities (e.g. enabling integrity check or device fingerprinting, changing weight to tags, searching audit logs, adding a new application) while Admins can also create/delete/modify users. Standard users can be authorized to have visibility on specific applications.

Cleafy supports both internal and LDAP defined users. Integration with LDAP authentication services can be configured at global level. Timeouts on active sessions can also be configured globally: users are notified when their sessions are about to expire so that they have the option to stay connected or close the session.

CLEAFY DASHBOARD

The following figures show examples of Cleafy dashboards. Cleafy provides a number of out-of-the-box dashboards and also the ability to create custom dashboards by simply saving any customer-created search.

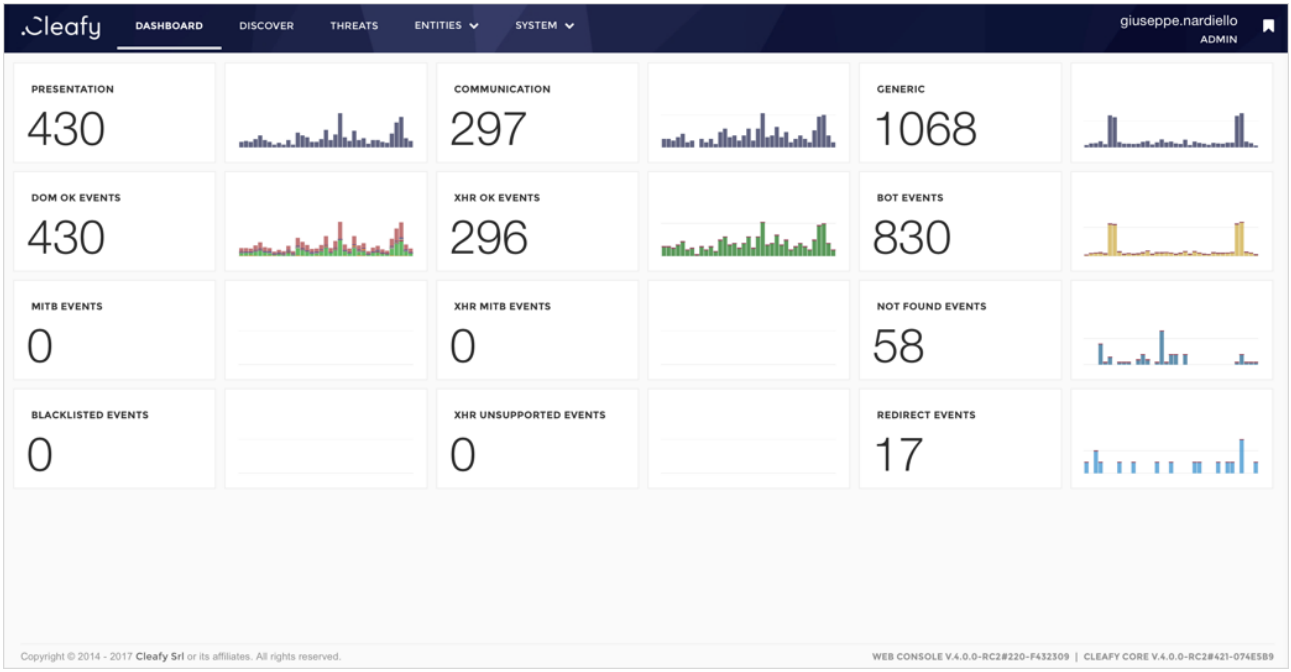

Figure 9. Cleafy “dashboard” showing some KPIs

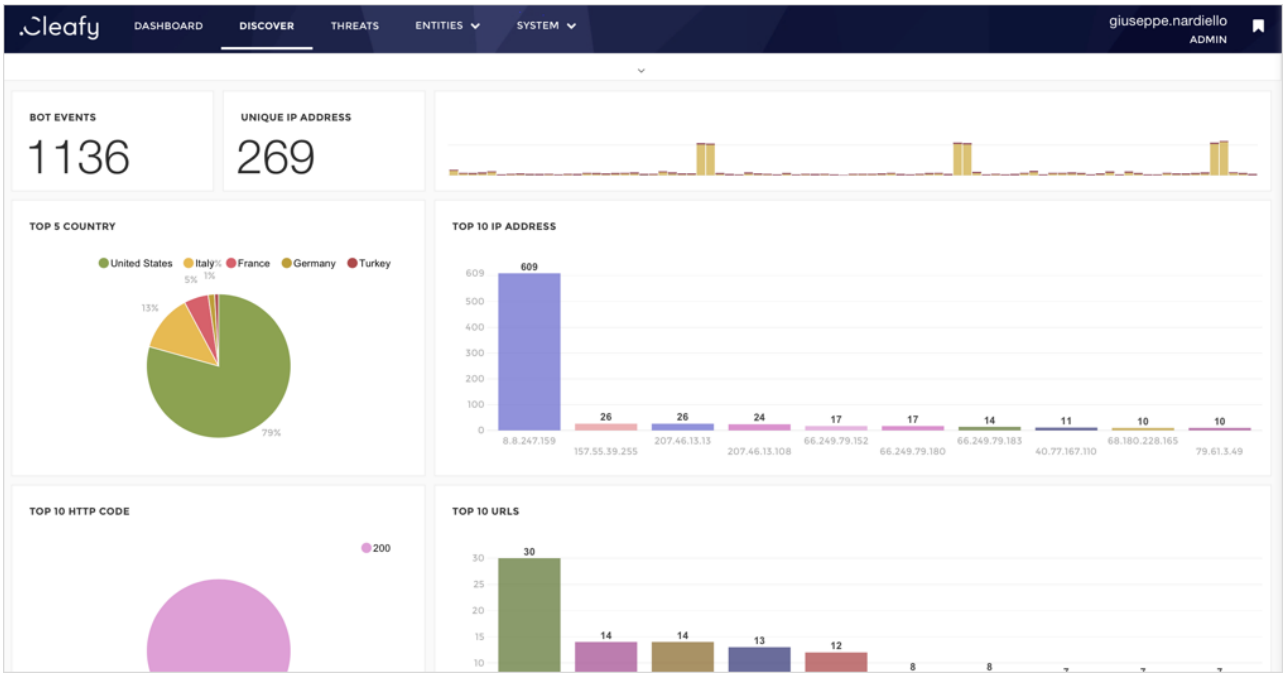

Figure 10. Cleafy dashboard focused on BOT detection

All charts are dynamic and interactive so they can be used to filter specific values (e.g. specific tags or HTML error codes) and to visualize displayed values.

Users can drill-down directly to specific pages providing detailed information about the entities represented by these indicators. For example, the following figures represent the list of events and sessions (ranked by risk score) respectively.

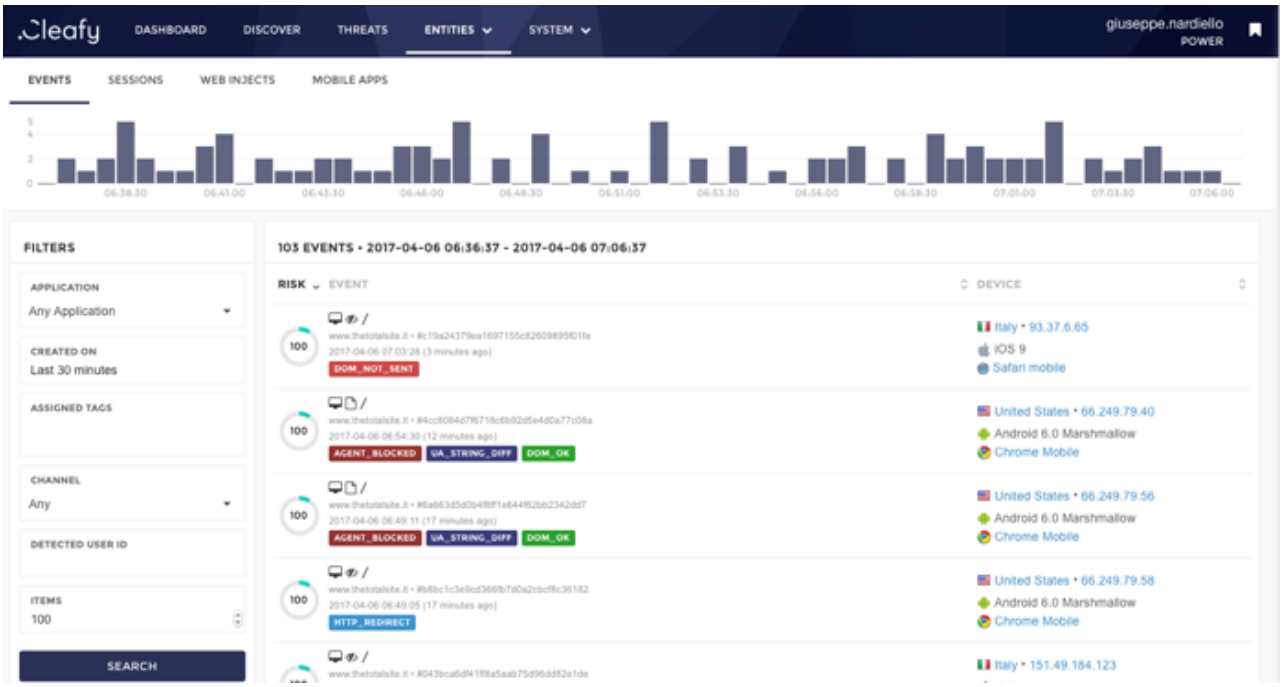

Figure 11. Cleafy Console displaying events (ranked by risk score)

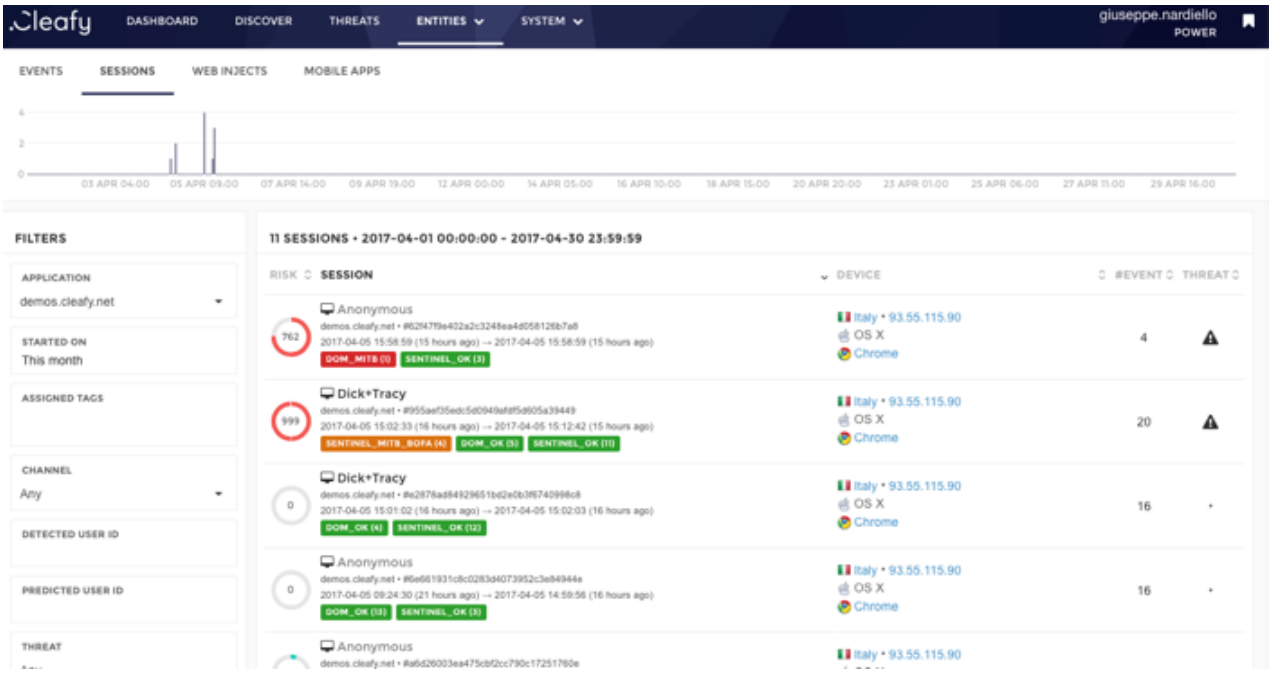

Figure 12. Cleafy Console displaying sessions (ranked by risk score)

The following figure shows a specific session with the currently calculated value of risk score. This page also displays all the events received at that point in time as they are processed in real time, with their associated tags (i.e. categorized threats).

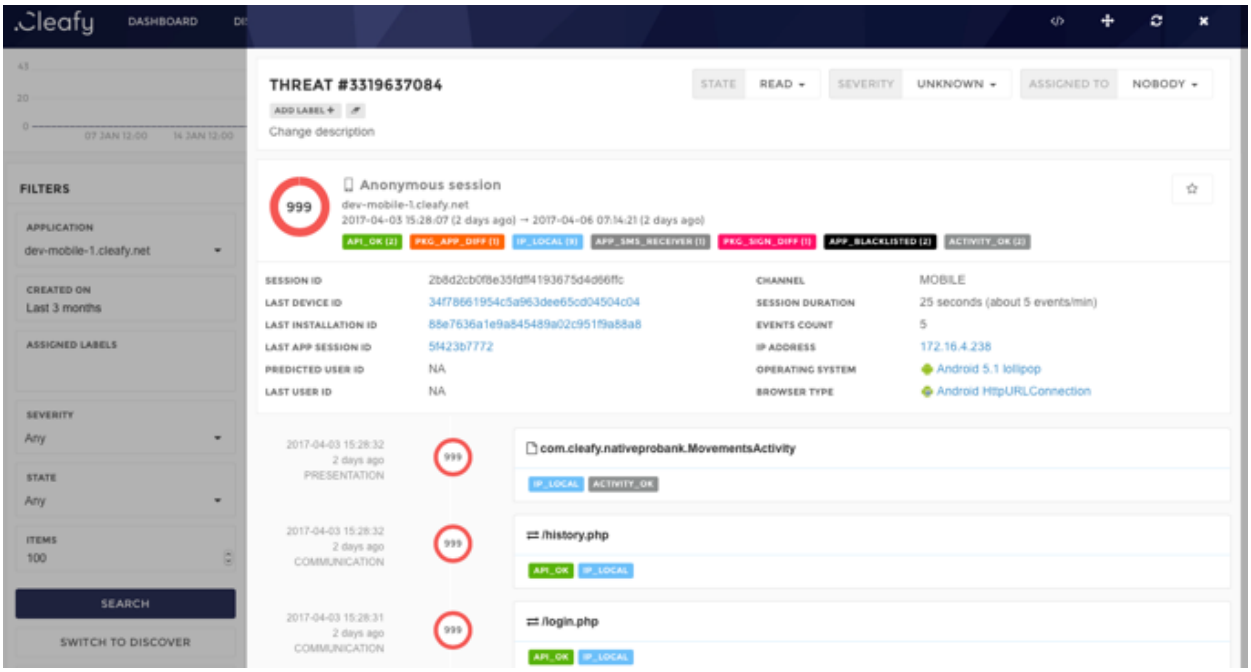

Figure 13. Session page displaying the risk score and all received events

Cleafy also provides a powerful, yet intuitive, Search & Visualization Query Language allows analysis spanning both historical and real-time data to be performed to quickly investigate pending threats and cases and to support cybersecurity activities.

Cleafy Search and Visualization Query Language can be used to display graphical charts (i.e. bar, area, histogram, line, pie, table) related to all fields of all entities (e.g. sessions, threats) and objects (e.g. alarms, events, snippets) available in Cleafy. Composing a query is made easy as fields and values are automatically prompted (see the following figure) as the user types the query string and any edited string is validated.

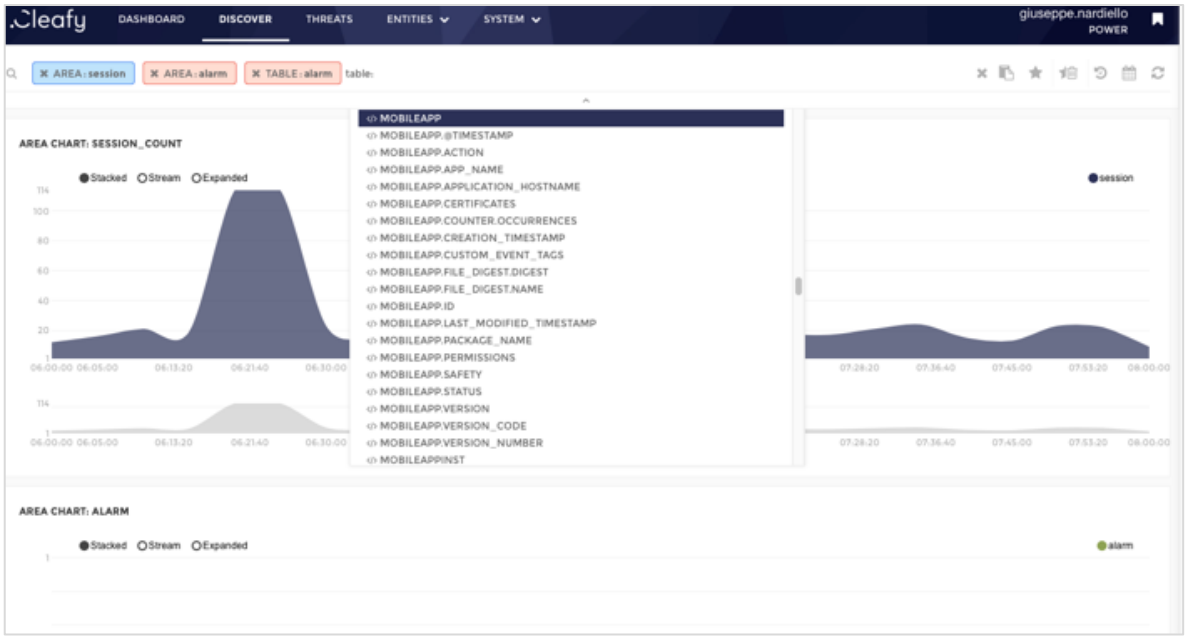

Figure 14. How users are aided in creating queries by menu showing available options

Queries can also be bookmarked and saved as dashboards (see next figure).

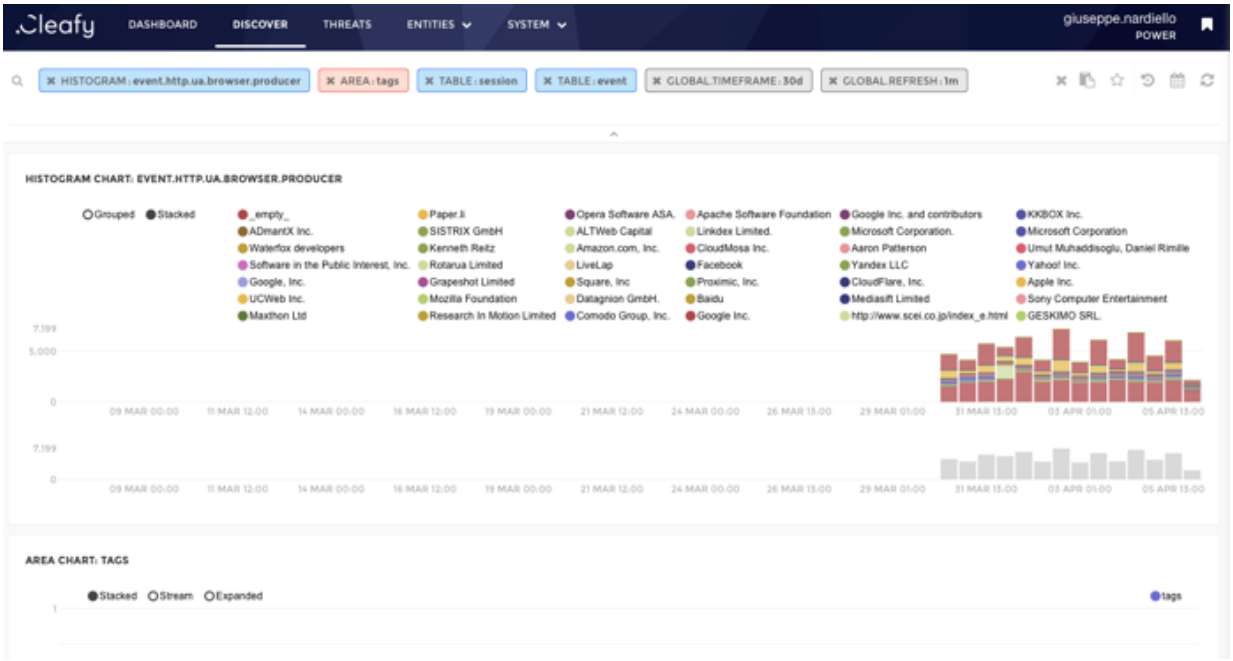

Figure 15. A custom query to be saved as a dashboard

CLEAFY AUDITING

All actions performed by users through the Cleafy Console or executed via APIs are audited (and logged separately) at different logging levels: INFO (general information), CREATE (create entities, users, applications, etc), READ (read-only access on single or multiple entities), UPDATE (update of an existing entity), DELETE (deletion of existing entities), SEARCH (performed search query) and WARNING (general warnings, blocked access, etc). The AUDIT LOG section of the SYSTEM menu provides access to all audit logs.

REFERENCES

[1] “Securing Web Commerce Using PCI DSS” (G00298555), Gartner (2016)

[2] “Beneath the Surface of a Cyberattack”, Deloittle (2016)

[3] “2016 Cost of Data Breach Study: Global Analysis”, IBM and Ponemon Institute (2016)

[4] “Cost of Cyber Crime Study”, Ponemon (2016)

[5] “Defence Report”, CyberEdge (2016)

[6] “Internet Threat Security Report”, Symantec (2015)

[7] “Net Losses: Estimating the Global Cost of Cybercrime”, McAfee (2014)

[8] “Automating Online Banking Fraud”, Trend Micro (2012)

[9] “2015 Data Breach Investigations Report”, Verizon (2015)

[10] “It's Losses Time to Isolate Your Users from the Internet Cesspool with Remote Browsing” (G00315285), Gartner (2016)

[11] “Online Banking Fraud 1: Know the Enemy”, NSS Labs (2013)

[12] “Panda Labs Quarterly Report Q3 2013”, Panda Labs (2013)

[13] “FireEye SSL Vulnerabilities”, FireEye (2014)

[14] “Man-In-The-Middle Attacks against Mobile Banking Apps”, Cleafy (2016)

[15] “Magic Quadrant for Endpoint Protection Platforms” (G00273851), Gartner (2016)

[16] “Market Guide for Endpoint Detection and Response Solutions” (G00274158), Gartner (2015)

[17] “Magic Quadrant for Web Application Firewalls” (G00290000), Gartner (2016)

[18] “Market Guide for Online Fraud Detection” (G00310495), Gartner (2016)

[19] “Keeping the bad guys out using five layers of fraud prevention”, Gartner Security and Risk Management Summit (2014)

[20] “Best Practices for Detecting and Mitigating Advanced Threats, 2016 Update” (G00296530), Gartner (2016)

About Us

Cleafy provides threat detection and prediction solutions that protect companies and their customers from advanced targeted attacks. Our vision is that in a context where you can safely assume that web/mobile endpoints are infected and that user identities are compromised, only direct, real-time evidences of threats can provide effective support for on-line fraud prevention.

Cleafy threat detection and prediction solution is based on unique, client-less, real-time integrity detection, pattern clustering and multi-entity correlation technology. Cleafy does not require any application change and is completely transparent to end-users. Cleafy can be easily deployed and seamlessly integrated with server-side infrastructure.

Cleafy solution reduces the risk of on-line frauds while reducing customer friction, provides predictive visibility on potential threats from targeted advanced attacks, improves security posture and the operational efficiency of your security team.

Cleafy has been adopted by major corporate and retail banks to protect millions of users and successfully prevent on-line frauds.

info@cleafy.com

EMEA

Via Simone Schiaffino 11/A

20158 Milan, Italy

+39 02 87031661

USA

283 Franklin St

Boston, MA 02110

+1 (617) 936-0212