TAG CYBER

NEXT-GENERATION DIGITAL RISK PROTECTION AT ENTERPRISE SCALE: AN OVERVIEW OF CONSTELLA INTELLIGENCE

EDWARD AMOROSO, TAG CYBER

Constella INTELLIGENCE

TAG CYBER

NEXT-GENERATION DIGITAL RISK PROTECTION AT ENTERPRISE SCALE: AN OVERVIEW OF CONSTELLA INTELLIGENCE

EDWARD AMOROSO

Digital risk protection (DRP) solutions are used in the security community as mainstream means for addressing cyber threats to individuals. Tailored solutions work well for a small group of executives but extending DRP to larger communities require novel means for automated scaling. The Constella Intelligence platform is used to demonstrate such scaling for enterprise.

INTRODUCTION

Modern cybersecurity is usually associated with the protection of applications, systems, networks, and infrastructure under an organization's control. Vendors emerge on a daily basis, for example, with the goal of preventing or detecting attacks to endpoints, servers, devices, and information – and such attention is warranted: Ransomware, enterprise breaches, and other attacks have not waned in recent years, especially since the COVID-19 pandemic.

An area of emphasis that has not received enough attention from the cybersecurity community, however, involves the protection of employees and executives from digital threats based on data and activity on systems and platforms not under an organization's control. We all know how this problem has exploded in recent years with bad actors targeting identities, reputations, and personal data. The risk extends to business when such targeted individuals or groups are closely connected to the organization, perhaps in executive roles or those with access to critical systems and sensitive data.

A new discipline is described in this report called digital risk protection (DRP) and its application is becoming an essential aspect of modern cybersecurity. Combining the protection of individuals and groups with corporate brands and reputations, DRP solutions scan the entire threat landscape to create actionable intelligence at scale. The Constella Digital Risk Protection Platform is used to demonstrate how a commercial solution can be used for this type of protection.

SCALING ADVANCES IN DRP

The most typical solutions used to protect an executive from digital risks, whether preventive in advance of problems or reactive after issues have emerged, involve a great deal of tailored concierge services delivered manually. While this approach allows for deep investigative analysis and bespoke security action on behalf of the victim, it certainly does not scale for enterprise teams hoping to protect large numbers of employees, managers, or executives.

Enterprise scaling requires novel approaches to DRP, ones that can take full advantage of automation, while also not losing the advantages of tailoring responses to an individual's online presence and digital footprint. The primary architectural solution to the scaling problem involves a data ingestion architecture with intelligent processing that creates a pipeline for handling large numbers of individuals without reliance on manual methods.

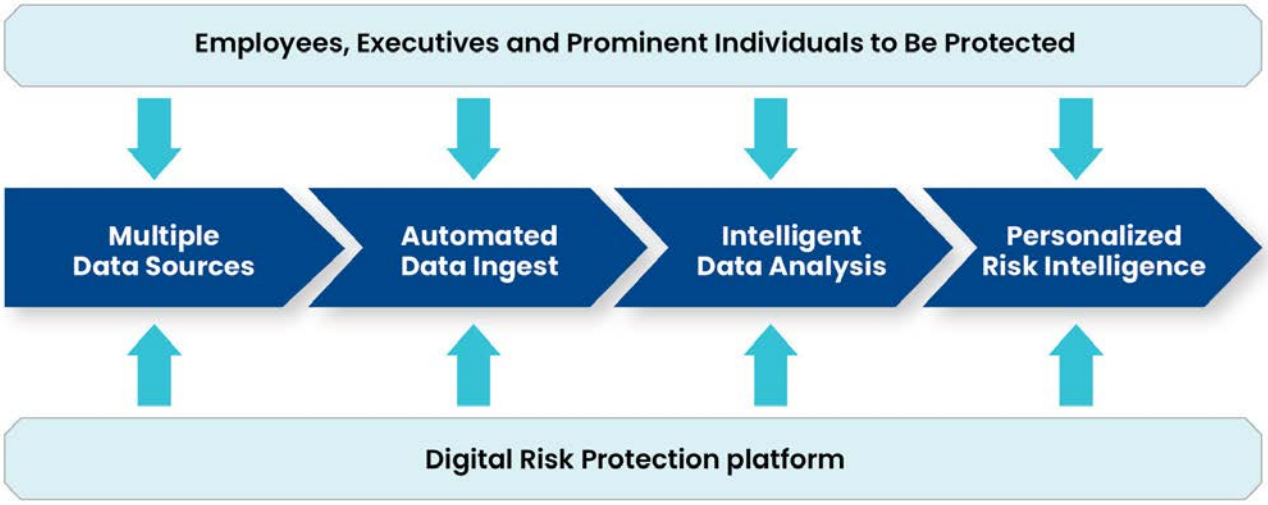

Figure 1. Automated Pipeline Approach to DRP

The most important aspect of the pipeline approach to DRP is automation because manual techniques simply do not scale. Although the security industry does include many commercial options for high-profile individuals that provide excellent concierge services from a small team of attendants – these offerings cannot scale without the support of a continuous monitoring services based on a platform.

OVERVIEW OF THE CONSTELLA DOME PLATFORM

The Constella Dome solution is a commercially available implementation of next-generation DRP services that includes strong support for enterprise scaling. Designed to protect the people, data, and brands of companies, the platform works continuously to map and monitor the posture and footprint an organization using data ingested from its many different online platforms, accounts, and services.

The platform specifically offers employee protection through automated continuous monitoring of three primary sources: (1) The Constella Data Lake is a collection of identities culled from the curated records of literally tens of billions of records spanning decades across 50+ languages and 125+ countries,, (2) commercial data brokers are used to provide additional information in the form of individual attributes that help with identify verification, and (3) public websites also provide information about individuals that complements other sources.

Executives and high-profile individuals are also protected using the sources listed above, but they represent a higher level of digital risk, given their prominence. As such, extended ongoing review is performed from three additional sources: (1) The deep web involves sites not indexed but that can include private data, (2) the dark web is rich with stolen credentials and other identifying information as well as conversations in forums that could evolve into personal threats against an executive and their family, and (3) social media is also an important source of identifying data.

The services that Constella offers an organization are arranged into logical components that provide specific benefits:

Employee and Executive Protection—The objective here is to reduce the risks associated with employees with credentials for systems and applications containing sensitive or critical data. These vectors of access make them particularly valuable targets for external cyber threats. Executives and VIPs are also major targets for enterprise theft and by activists or other actors who might take issue with some aspect of an organization's mission or activities.

Brand Protection—The reputational damage that can come with fraud and misuse of the online digital presence of an organization is hard to underestimate. Unlike some types of attacks that can be mitigated or recovered, the impact of public sentiment influenced by malicious entities is difficult to reverse. With the rise of disinformation-as-a-service, companies must address informational threats that pose a new axis of risk to their brands and bottom lines. Constella provides activity tracking to monitor hostile activity and persons of interest for targeted threats on the surface, deep, and dark web, and social media for brand impersonation, disinformation campaigns, domain squatting, and other targeted threats to a brand.

Geopolitical Protection—The platform also collects and interprets intelligence from across the surface, deep, and dark web, and social media, to anticipate global geopolitical or socially relevant trends that may present relevant signals of risk to organizations—including specific executives or operations. The corporate and security-related risks associated with sociopolitical unrest and shifting global dynamics can have distributed effects ranging from supply chain disruption to increased cyber threat actor activity. Anticipating these risks through intelligence monitoring enables globally operating organizations to stay one step ahead.

Identity Monitoring—The risk of identity theft and fraud has increased considerably in recent years. The Constella solution monitors individuals and domains for exposed data than can be used for identity-based attacks. Through application programming interfaces (APIs), the platform can alert consumers and organizations of new exposures before they can be used for identity theft and fraud. Processing is based on a massive historical database of compromised credentials from billions of curated records.

Threat Intelligence Services—Constella also delivers customized intelligence via its Insights team of intelligence analysts. We integrate proprietary technology with our team of expert intelligence analysts to monitor social media and the surface, deep and dark web, to deliver real-time alerts and report on threats targeting your executives and their circle of trust, your brands, and your digital assets. The Constella team also provides international coverage that helps considerably with data collection and interpretation. With offices in the US, Brazil, Spain, and India and its presence in other geographies around the world, the company provides strong support for different languages. This is critically important when correlating information found about an individual that could require proper contextual interpretation by a local native speaker.

An additional benefit the Constella team provides is an international coverage that helps considerably with data collection and interpretation. With offices in the US, Brazil, Spain, and India, in addition to presence in other geographies around the world, the company provides strong support for different languages. This is critically important when correlating information found about an individual that could require proper contextual interpretation by a local native speaker.

ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.