CyberProof

January 6, 2019

Using AI and Automation to Protect Your Critical Assets

A Whitepaper

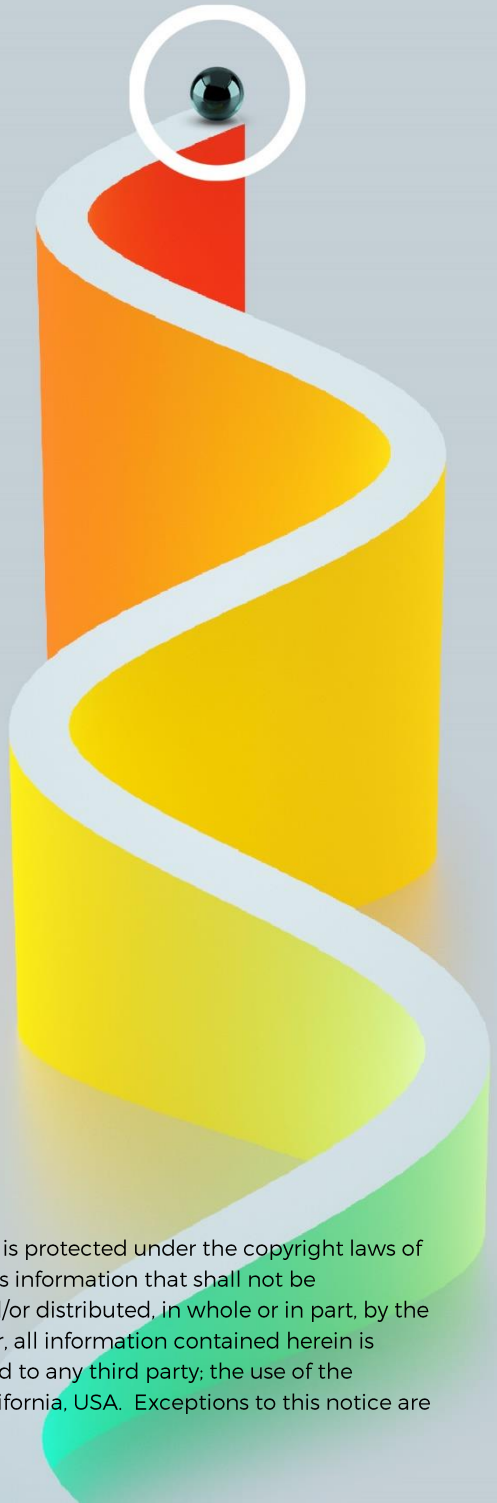

Table of Contents

Key Takeaways

- The CyberProof Defense Center (CDC) is the **fulcrum of your cyber defense infrastructure**, providing the means to detect and remediate attacks by containing and negating damage vectors aimed at critical assets, business processes, and sensitive repositories.
- The CDC is a SOAR (Security Operations Analytics & Reporting) enhanced SOC, riding on top of a vast information collection network that includes internal and external data.
- The huge volume of raw data from internal and external sources defeats the SOC team's ability to process and detect all potential IoCs. The bad signal-to-noise ratio of cyber intelligence led CyberProof to develop an automated and autonomous model of AI agents to supplement and augment the human SOC attendants and support TI teams. This family of AI agents is called SeeMo.
- SeeMo's open architecture facilitates rapid deployment of an array of mixed-functionality agents in multiple places in the architecture, with strong support for distributed and federated analytic models.
- The autonomous AI and ML SeeMo agents deploy the analytics in the right places across the many-layered global architecture, ensuring that analysis can be executed where it best fits the inflow of information and the design constraints.
- The CDC architecture in general, and the hybrid model in particular, ensures protection of business data and privacy-related information. The SeeMo agent model operates within these constraints yet provides significant capabilities of analytics across the entire system.

CyberProof Defense Center – Attack Detection & Remediation

CyberProof created a SOAR (Security Orchestration Automation and Response) orchestration platform that is a keystone of its cyber resiliency paradigm – the CDC.

The CDC is the fulcrum of the cyber defense infrastructure, providing the framework to detect and remediate attacks by containing and negating damage vectors aimed at critical assets, business processes, and sensitive repositories.

The CDC relies on broad access to data and intelligence. Internally, it connects to a SIEM or directly to security sensors and IT infrastructure. Externally, it pulls information regarding threat landscapes, threat actors, vulnerabilities, exploits, campaign alerts and indications of breach related to its customer base.

Automated Analytics Detect Indications of Compromise

The CDC processes, correlates, analyzes and matches the vast flow of information to detect Indications of Compromise (IoCs), match them to probable threat vectors (using the Mitre Att&ck Framework), and trigger alerts for invocation of the proper Incident Response (IR) playbooks.

The nature of the CDC mandates heavy reliance on automated analytics to process and disseminate the inflow of data.

CyberProof uses ML (machine learning) and AI (deep artificial intelligence) to detect and elevate indications of a threat whether known or unknown. Embedded logic is crucial to the CDC's teams to handle emerging threats fast enough to contain the damaged vectors and ensure the resiliency of a customer's systems.

Collecting and Storing Data

The CDC is a SOAR-enhanced SOC platform, which rides on top of a vast information collection network and includes:

- Internal data, usually collected by a SIEM engine that pulls in system event logs, logs from security boxes, and logs of transactional applications.
- External data, usually pushed from 3rd party partner platforms that perform multiple services, including Web harvesting, social media monitoring, vulnerability feeding, and Darknet data scavenging.

For internal data, the CDC utilizes a multi-tenant model to ensure each customer's privacy. In hybrid configurations, the SIEM data resides on premises and never gets loaded to the cloud, while in pure form virtual SIEM machines manage the data in

the cloud. For external data, the external intelligence repository is global – though local copies are maintained at each regional SOC.

The CDC has multiple cloud installations to support regional SOCs and franchise SOCs. Overall, the internal data archives are handled as multiple distinct and separate repositories, and any ML or AI components must execute in multiple local instances.

The CDC's Automation Mechanisms for Logic Components

The CDC employs these automation mechanisms:

- Rule engines for multiple discrete decision tables
- Statistical modeling function libraries
- Link analysis repositories
- SeeMo analysis agents
- Heavy duty back-end analytic libraries

These are configured to generate notification, elevation, and alerts on analysis runs. Their primary goal is to enrich and service the CDC dashboard and IR handling environments. They also support in-depth intelligence analysis performed by the back-office threat intelligence teams.

The SeeMo Family of Autonomous and Automated Agents

The huge volume of raw data from internal and external sources defeats the SOC team's ability to process and detect all potential IoCs. The bad signal-to-noise ratio of cyber intelligence led us to develop an automated and autonomous model of AI agents to supplement and augment the human SOC attendants and support TI teams. We call this family of AI agents SeeMo.

SeeMo's design pattern is of autonomous agents executing specific tasks, under a general framework of connectivity, to facilitate data source access and result dissemination. An agent normally takes one of these forms:

- Distributed decision table set – Used mostly on the local instances of customers, to facilitate external data sources and globally calculated values for IoC tagging from the CDC back-end logic subsystem.
- Distributed statistical modeling – Execute continuously on SIEM subsystems; execute statistical models too resource-hungry to include in the inline processing elements.
- Federated ML components – Process at the entrance or on top of the SIEM, and send anonymized results upstream – so the CDC can perform near real-time ML analytics in a multi-tenant architecture.

- Autonomous AI agents – Run independent of any other component, aside from a back-end training environment for supervised algorithms. They match incoming data flows to pre-calculated value tables and infer the potential existence of hidden patterns, which are elevated for scrutiny by the CDC shift or directly to back-end analyst teams.

Each SeeMo agent is configured to include its support data, though some that rely on continuously updating tables perform rime-based refresh from external sources such as vulnerability feeds, calculated thresholds for IoC tagging, etc.

SeeMo Quickly Creates and Deploys Analysis Agents

SeeMo's main benefits are the fast creation and deployment of analysis agents – without complex integration or versioning of the software. Many agents can even be hardcoded onto appliance boxes.

SeeMo's open-ended architecture allows CyberProof fast deployment of an array of mixed-functionality agents in various places in the architecture, with strong support for distributed and federated analytic models.

Agents can be configured to dynamically enrich IoC indicators from global external repositories or directly from online sources, enriching the detection process in separate instances. SeeMo also executes in the hybrid model, running on top of the local MongoDB repository that drives the CDC and on the local SIEM platform as an ad-on application.

Leveraging Analytics in the Right Place within the CDC Architecture

CyberProof's design provides for inline and autonomous processing of data and repositories at various levels and subsystems of the CDC platform, supporting constraints of multi-tenancy and hybrid configurations while providing robust analytical capacity for a range of deployment scenarios.

The autonomous AI and ML SeeMo agents deploy analytics in the right place across the many-layered global architecture, ensuring that analysis can be executed where it best fits the inflow of information and the design constraints.

CyberProof's model can expand with the customer base and with advances in AI and ML functionality without impacting the CDC architecture or our commitment to ensuring data privacy and control per customer preferences.

About CyberProof

CyberProof, a fully owned subsidiary of UST Global, is a platform-enabled company, whose mission is to reduce cyber risk with flexible service models. At CyberProof, we approach risk modelling using a top-down model where we define the magnitude of attack and focus on the top attack scenarios. We then facilitate a business-oriented prioritization of a customer's investment in defense and response.

CyberProof was recently ranked Leader in the Forrester Wave™ Report: Emerging MSSPs Q3 2018, validating our disruptive approach to cyber security services.

For more details, visit our website at www.cyberproof.com.