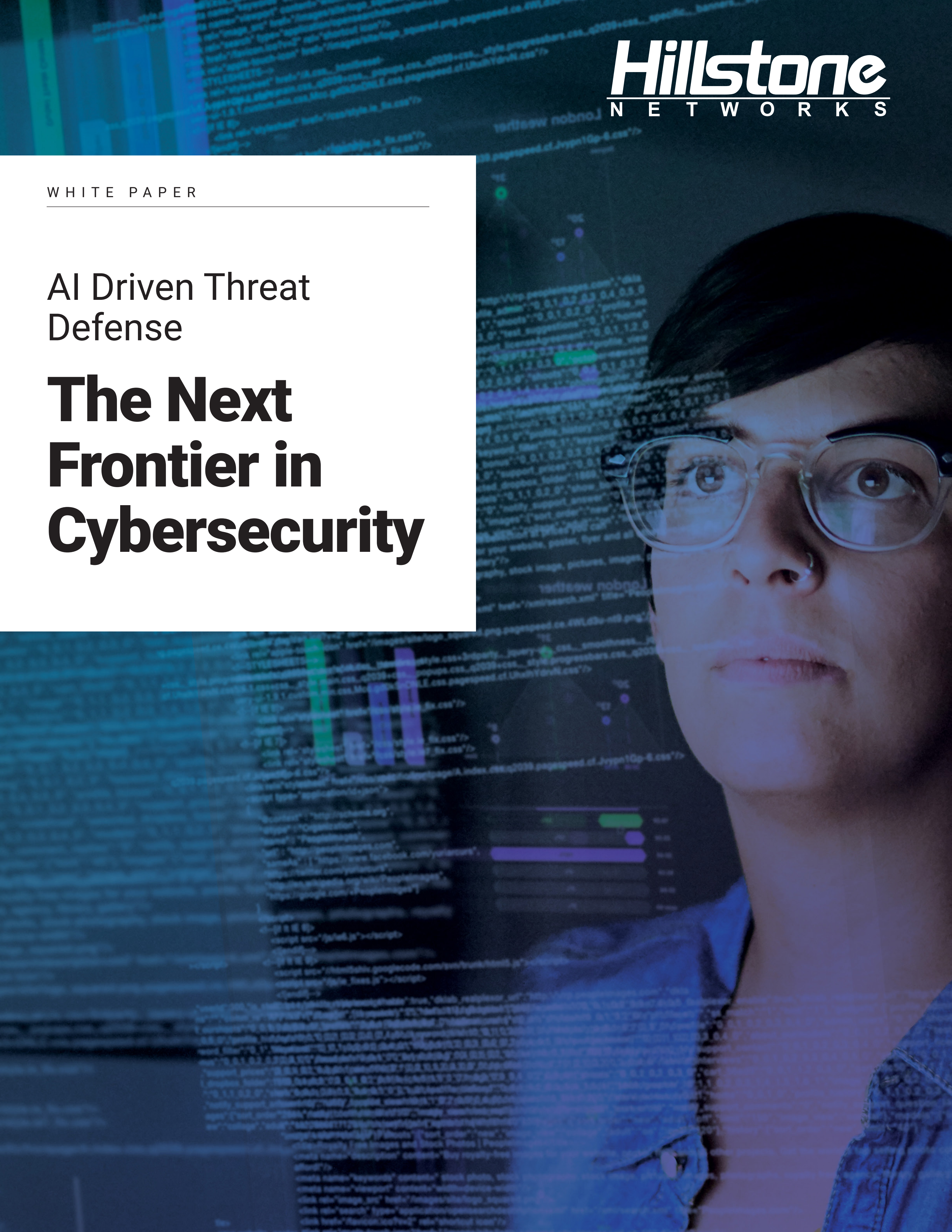


WHITE PAPER

AI Driven Threat Defense

The Next Frontier in Cybersecurity

Introduction

It’s undeniable that the landscape of modern cybersecurity has evolved dramatically—and at a rapid pace—just in the past few years alone.

Attackers, whether individual hackers or state-sponsored organizations, are becoming more sophisticated, using new tactics and tools anchored by email, social media or deepfakes to infiltrate and bypass conventional threat detection. These attacks are aimed at accessing corporate critical assets or personal data, with the end goal of stealing valuable information and, at times, causing disruption to normal business operations.

In parallel, security vendors and research organizations are advancing technological innovation to deliver cutting-edge tools and integrated solutions for threat prediction, prevention, detection and mitigation with ever more improved efficiency and effectiveness. On the analyst front, Gartner recently proposed the CARTA (Continuous Adaptive Risk and Trust Assessment) framework to highlight integrated cybersecurity technologies and how they can be used at different stages in defending against cyberattacks.

Furthermore, 5G networks and cloud computing are changing the way and pace of how we communicate: The world is transforming to digital at an unprecedentedly fast pace; information and data are increasing at explosive rates; and vast amounts of data are now available and are being monitored, collected, stored, analyzed and presented using many different types of applications. This data comes from all sorts of different sources, endpoints, network devices, mobile devices, cloud, individual users and other entities, to name a few. How to analyze and use this data effectively and efficiently has become a critical task for organizations large and small.

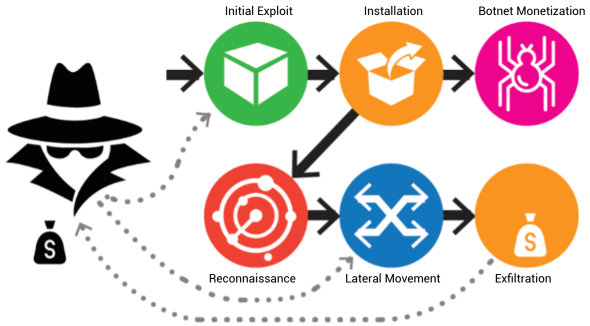
As a result, collecting, storing and analyzing this data can no longer be carried out with traditional threat detection and prevention techniques, whether manual or automated. Today, security automation—especially the automation propelled by Artificial Intelligence (AI) and Machine Learning (ML) in threat detection, threat analysis, threat hunting and threat response—has become one of the most active development areas in network security.

AI is used to apply advanced analysis and logic-based techniques, including ML, to interpret events, support and automate decision making and also to help admins take sound and effective action to respond to threats and attacks. AI technologies, such as ML deep learning, graph theory and neural networks, have actually been around since the early 80’s (or even earlier), but mostly in academia or research. With the emergence of high-speed internet and the availability of advanced applications and big data, AI technology has reached critical mass and has matured into a powerful suite of tools to help prevent and fend off known and unknown cyberattacks.

Contents

AI-driven
Threat Detection, Hunting and Response

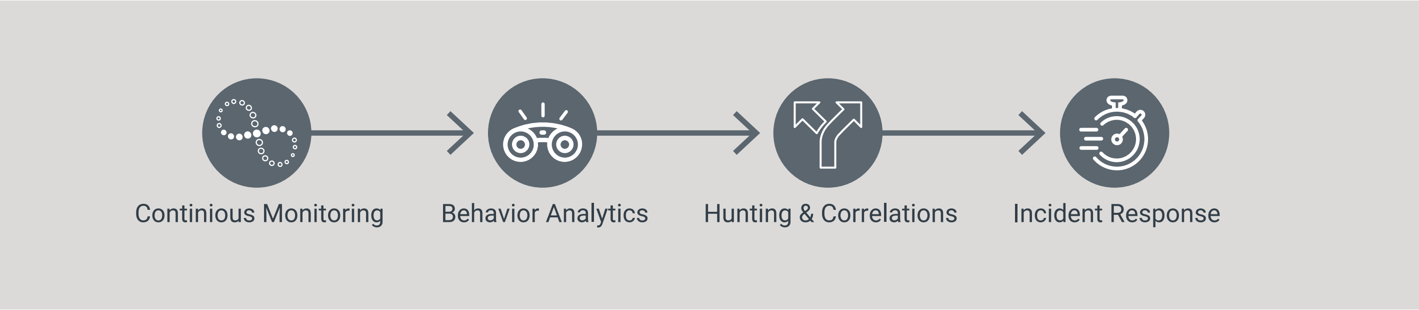
Today's Advanced Persistent Threat (APT) attacks usually involve a targeted, sophisticated and multi-stage process, commonly described as the cyberattack kill chain in the security industry.



In a typical APT attack, the initial stage involves exploitation using phishing, social media, deepfakes and other tools followed by actively weaponizing these exploits. After penetrating network borders such as firewalls, an APT usually lies inactive or hibernates for a long period of time (days, weeks or more), to avoid active detection tools deployed by corporate security. It then starts to conduct reconnaissance activities to search and locate critical assets—usually the database, file or email servers that host the data and files that are essential in carrying out day-to-day businesses operations. Subsequently, it will try to gain access to the servers using brute force, privilege escalations and other mechanisms. In the final stage, hackers exfiltrate and transfer stolen data and files to external Command and Control sites.

As we can see from the above, a typical attack surface involves multiple phases; each phase is quite different in terms of behavior and the attack tools used. In addition, attackers constantly modify attack tools and tactics to avoid static or signature-based detection. To add further insult to injury, these attack points and traces are buried under normal traffic, application and user data. Therefore, security analysts and admins are often overwhelmed with the volume of data presented to them as well as the pervasive threat alerts, making it harder to conduct analysis and take proper and timely action. Because of all these dynamics, security vendors and analysts are now heavily turning to AI and ML technologies to address threat defense battles that otherwise would be impossible by human or manual processes alone.

AI and ML technologies can be leveraged across the entire threat attack detection, analysis and response phases—we call this suite of technologies "AI-X." The following few paragraphs discuss these elements in greater detail:

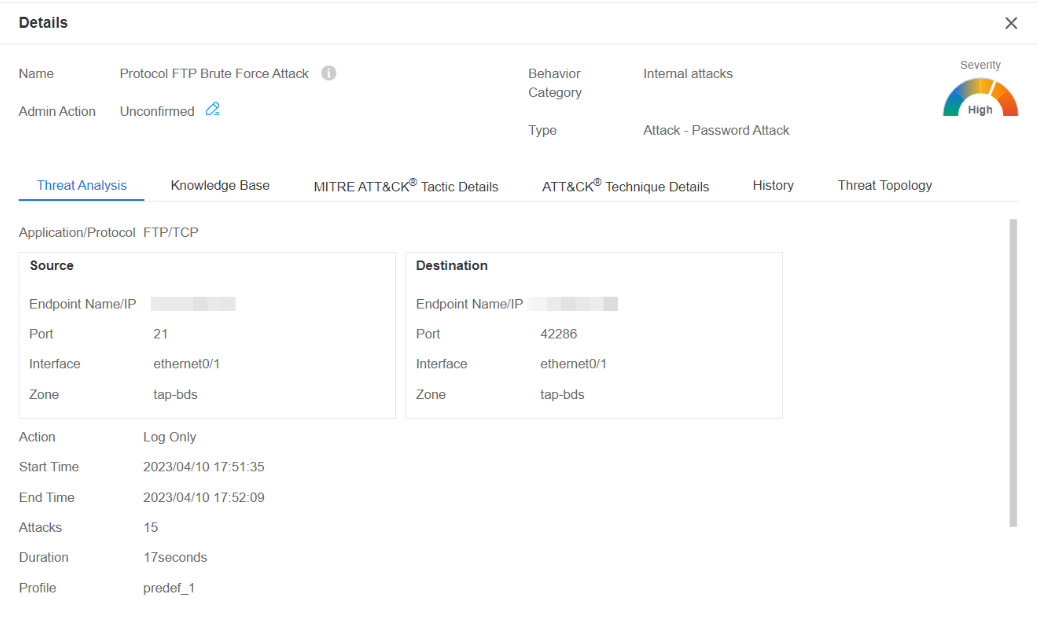


AI-driven
User Behavioral Analytics

Attackers frequently adjust and morph their behavior to avoid detection, making policy- and signature-based static detection mechanisms less effective because of the need to constantly update and patch signature databases. A more effective approach would be to monitor the behavior of attackers along the attack path, then use analytics to build models for standard profiles or baselines of behavior for users and other entities such as hosts, applications, network traffic etc. over spatial and temporal spectra. Activity that is anomalous to these standard baselines is flagged as suspicious, and security admins are alerted for further analysis. This is defined as User and Entity Behavioral Analytics (UEBA) solutions by Gartner. Two of the most common UEBA use cases desired by enterprises are detecting malicious insiders and external attackers infiltrating their organizations (compromised insiders).

AI-driven UEBA has proven to be an effective technique in these cases. There is great value in applying AI and ML to process vast amounts of data from disparate sources efficiently and effectively in order to provide a fusion point that glues the sources together—be it behavioral data from an endpoint, network, application or user. AI-enabled detection engines help monitor and establish normal behavior using mathematical models to help identify anomalies and conduct behavioral analysis to accurately alert admins with both confidence as well as supporting evidence.

The AI-based analytical engine monitors and learns normal user and application behavior during the so called “learning phase.” It renders all the information into mathematical models and outputs in order to establish normal behavioral baselines, taking into consideration exceptions such as holidays and scheduled IT operations. During the “detection phase,” corresponding user and application traffic is collected, decoded and checked against the normal baselines and anomalies are flagged if detection rules are violated. The AI engines also automatically ingest other forensic information from sources such as threat intelligence and threat reputation, in order to reduce noise and enhance accuracy.



Name Protocol FTP Brute Force Attack

Admin Action Unconfirmed

Behavior Category Internal attacks

Type Attack - Password Attack

Severity High

Application/Protocol FTP/TCP

Source		Destination	
Endpoint Name/IP	[redacted]	Endpoint Name/IP	[redacted]
Port	21	Port	42286
Interface	ethernet0/1	Interface	ethernet0/1
Zone	tap-bds	Zone	tap-bds

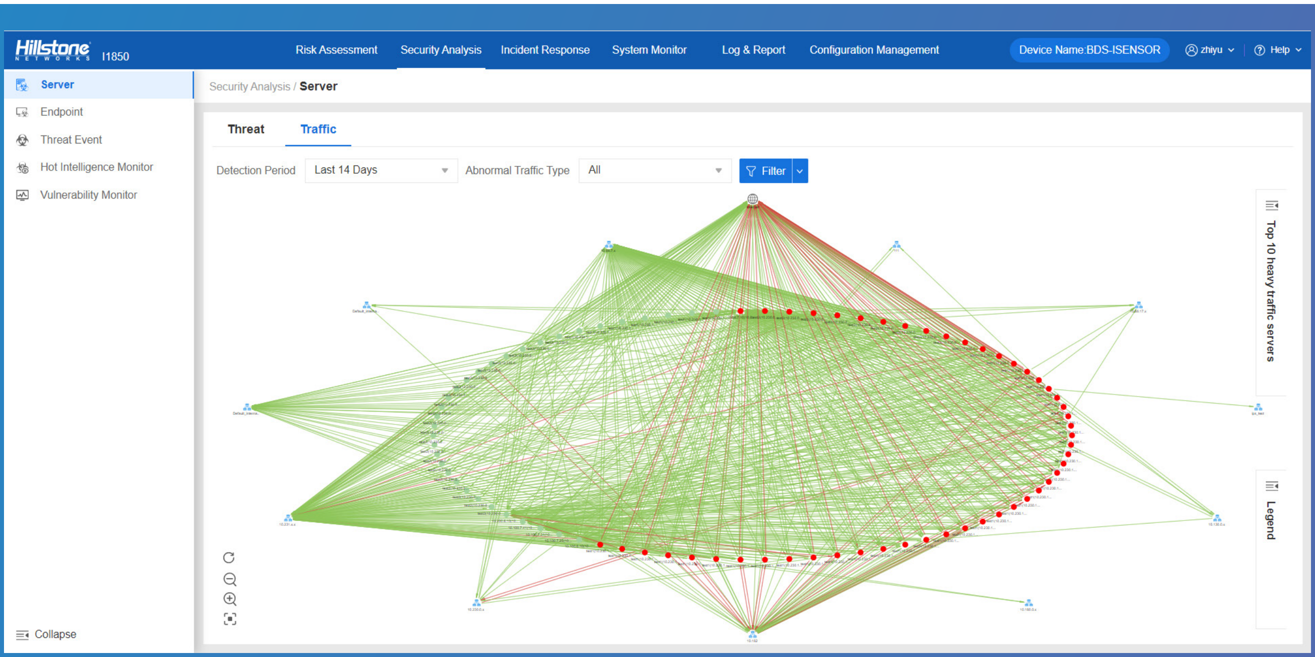
Action	Log Only
Start Time	2023/04/10 17:51:35
End Time	2023/04/10 17:52:09
Attacks	15
Duration	17seconds
Profile	predef_1

AI-Driven
Network Traffic Analysis

A specific area of focus in UEBA solutions is Network Detection and Response (NDR). Network traffic—whether raw traffic, metadata or flow record (e.g. NetFlow, sessions, logs)—possesses rich information both at the network and application levels, including normal or malicious patterns. Given that the volume of network traffic is massive and requires monitoring in real time, it is impossible to conduct traffic analysis by a human alone. AI or ML-based techniques are the best tools to assist security analysts or network admins to conduct real-time monitoring and analytics for today's network traffic flows. These techniques help establish normal traffic baselines—for example, normal business activities, file access and data transfers etc. It can also help provide comprehensive visibility, especially for east-west traffic within corporate intranets or among virtualized networks within datacenters. Abnormal behavior can be identified, analyzed and alerted.

The following figure shows the AI-driven NDR engine in operation. Network traffic, especially incoming and outgoing traffic from so-called critical assets (which are usually important corporate servers), are monitored, collected and decoded in real time. A set of important traffic metadata or PCAPs are sampled and saved periodically. The NDR engine conducts traffic classification and renders it through mathematical models to identify abnormal traffic patterns. After this, the AI-driven correlation engine can initiate behavioral correlation analysis, and ingest and fuse additional historical data, reputation information, threat intelligence feeds and network behavior. The objective is to reduce false positives and generate accurate threat alerts with rich forensic evidence.

The AI-driven user behavioral and traffic analysis tracks the attacker's network traffic behavior during the attack process and helps to identify suspicious or abnormal user, application or traffic behavior. It can also correlate additional threat hunting or forensic information over time and space spectra to generate accurate threat events and alerts.



Detection Period: Last 14 Days

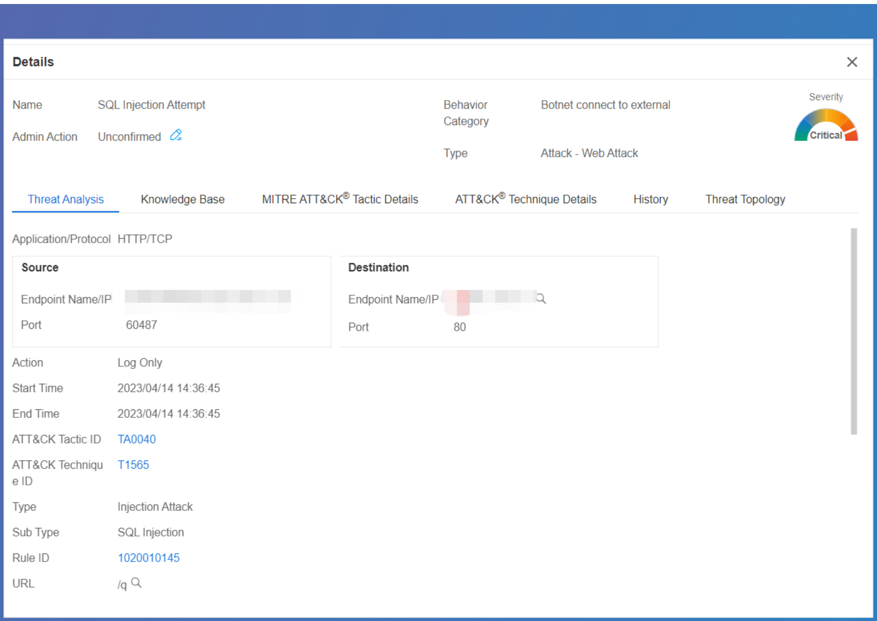
Abnormal Traffic Type: All

AI-driven
Threat Detection Using Data Science

Every day, up to billions of malware samples and data are collected by security vendors and other research organizations. To analyze this ocean of data has long been the art of data scientists and up to now has been a very complex and involved task, if even fully possible. Fortunately, using techniques powered by AI and ML, researchers and analysts can automate this process to produce their desired outcomes. This is also called Big Data analysis. According to industry surveys, the majority of CISOs and security analysts find that AI-enabled solutions are maturing and can be used in the areas of malware detection and advanced threat detection.

AI or ML techniques in data modeling-based malware detection usually involve data mining, model training and predictions. During data mining, large amounts of raw data are cleansed, normalized and classified into data sets, and the characteristics of malware families are abstracted into sets of features. Data sets are trained into models either supervised or unsupervised; in the case of ML, this process is supervised, but it can be done automatically in deep learning techniques. Live traffic is monitored and parsed according to defined rules and policies; suspicious packet captures are fed to previously established detection models for prediction. The output can then be fed into other AI-based correlation engines, which includes more forensic evidence and relevant threat intelligence to generate accurate true positives.

The following diagram shows a web threat alert from an ML detection engine from Hillstone Networks. Behind the scenes, Hillstone's ML-powered threat detection engine continually extracts the characteristics of millions of known malware families, harnessing unsupervised ML algorithms and mathematical modeling to identify common features of known malware families and train these data sets. The model is installed on physical and virtual security appliances and detects both known malware families as well as those with mutations. Once the suspicious packets are captured, they are parsed and dissected according to the ML model feature rules and subsequently fed into the model for predictions. The output is typically presented to the admins, with enriched forensic information.



Name SQL Injection Attempt

Admin Action Unconfirmed

Behavior Category Botnet connect to external

Type Attack - Web Attack

Application/Protocol HTTP/TCP

Source

Endpoint Name/IP [redacted]

Port 60487

Destination

Endpoint Name/IP [redacted]

Port 80

Action Log Only

Start Time 2023/04/14 14:36:45

End Time 2023/04/14 14:36:45

ATT&CK Tactic ID TA0040

ATT&CK Technique ID T1565

Type Injection Attack

Sub Type SQL Injection

Rule ID 1020010145

URL /q

AI-driven

Automation in Security Operations and Incident Response

Another important aspect of applying AI in cybersecurity is to empower Security Orchestration, Automation and Response (SOAR) in the Security Operation Platform (SOP).

According to Gartner, SOAR refers to a suite of technologies that enable organizations to collect input monitored by the security operations team. For example, alerts from the SIEM system and other security technologies—where incident analysis and triage can be performed by leveraging a combination of human and machine power—help define, prioritize and drive standardized incident response activities. SOAR tools allow an organization to define incident analysis and response procedures in a digital workflow format.

Although overlapping with some of the SIEM functionalities, compared to the traditional SIEM platform, the scale, complexity and workloads in an SOP is much larger. An SOP intakes more variety in data than just logs, and conducts much more sophisticated analysis. Nowadays, because of the ever-increasing data volumes and ever-increasing complexity in analytics, security staff are constantly too overwhelmed with the amount of data and workload to keep up with time- and resource-consuming SOC operations and workflows, let alone analyze or respond to all threat attacks.

Because of these dynamics, AI and ML technologies have emerged as the new paradigm in improving security automation. Specifically, many routine and repetitive jobs are intelligently designed and built into playbooks. Playbooks are set of rules for workflows that can be initiated when an event or data access is triggered. Similar to software programs, playbooks allow users to build complex structures and process logic depending on requirements and desired outcomes. AI- or ML-based micro-engines can also be loaded dynamically during different workflow phases to assist threat hunting, enrich forensic evidence, improve detection accuracy, reduce false positives, automate response ticketing and streamline incident response workflows. This will relieve SOC staff, data scientists and admins from tedious and routine tasks and, instead, allow them to focus on threat resolution and other business-critical activities.

Stay Ahead of The Curve

AI-driven Security Solutions by Hillstone Networks

In the field of cybersecurity, no technology can work effectively solo or in silos. Instead, disparate detection and response techniques need to work together to form a closed-loop ecosystem. In this case, AI and AI-enabled detection technologies have become the new frontier in battling cyberattacks. AI, ML and their many different types of analytics and automation tools act as needles and threads that suture the gaps to form a safety net that helps identify and capture attacks and the criminals behind them.

Over the last several years, Hillstone Networks has been investing and harnessing its advanced AI-driven technologies at all fronts—the network perimeter, inside the corporate intranet, as well as within the cloud. Hillstone's solutions work together to block attacks at the network border, and detect, track and mitigate cybersecurity breaches in progress inside the corporate network and in the cloud.

These efforts at Hillstone Networks have received awards and gained accolades both domestically and internationally. For example, Hillstone's AI-powered NDR product, the Server Breach Detection System (BDS), has been listed as a representative solution in the Market Guide for Network Detection and Response by Gartner. BDS adopts multiple threat detection technologies that include traditional signature-based or rule-based technology and large-scale threat intelligence data modeling, as well as machine learning-based user behavior analysis. The system provides an ideal solution for detecting advanced threats, including ransomware and crypto-mining malware, and protecting high-value critical servers and sensitive data from being leaked or stolen. Together with deep threat hunting analytical capabilities and visibility, BDS provides security admins the effective means to detect IOCs (Indicators of Compromise) events, locate risky hosts and servers, and restore the attack chain. Moreover, it conducts threat and attack mitigation with the conjunction of NGFW, as well as with the integration of Hillstone's XDR solution iSource. BDS brings an effective and comprehensive solution to detect and respond to different breeds of network attacks and threats in an enterprise's assets.

Looking forward, Hillstone Networks will continue to focus on AI and ML research and development and also to integrate AI and ML technologies across its solution portfolio. Our mission is to provide threat prevention, detection and mitigation to our customers so that they can have a best-in-breed weapon in their arsenal against cyberattacks.

About Hillstone Networks

Hillstone Networks' Integrative Cyber Security approach delivers coverage, control, and consolidation to secure digital transformation for more than 26,000 enterprises worldwide. Hillstone Networks is a trusted leader in cyber security, protecting enterprise critical assets and infrastructure, from edge to cloud, regardless of where the workload resides. Recognized as a Visionary in Gartner's Magic Quadrant for Network firewalls, Hillstone Networks' entire suite of cyber security solutions is relied upon in many of the world's most challenging technology environments.

Hillstone NETWORKS

Visit **www.hillstonenet.com** to learn more
or contact Hillstone at **inquiry@hillstonenet.com**