WHITE PAPER

IMPORTANCE OF MONITORING ENDPOINTS IN SOC

WWW.AICYBERWATCH.COM

MONITORING THE FIREWALL ALONE DOES NOT HELP!

AiCyberWatch
Keeping you Ahead of Cyber Crime

Organizations have been continuously breached, despite deploying various security products. There are no means to detect abnormal or unknown "Threat". AiCyberwatch SOC Services boast of India's first AI and ML enabled XDR SOC offering that tightly integrate with security applications like Next -Gen SIEM, EUBA, EDR, VA, TI, NTA, NBAD, DDoS, AI and ML. The service provides a complete view of how users, devices and applications interact and behave, automatically correlating security events from many security tools. It uses machine learning combined with advanced self-learning threat models to detect abnormalities and real threats in real-time, while also providing the means to stop and contain the threats immediately upon detection. This helps organizations to visualize user activity, behavior, applications and flows.

AiCyberwatch offers Multi-Layer Effective Detection, i.e. detection of known as well as never before seen threats and Indicates all compromised sources and threat targets. It detects threats coming from compromised credentials and insider threats, and can detect Advanced Persistent Threats, all based on behavior, and done automatically. No workstation endpoint agents are required.

Traditionally organizations deploy many of the perimeter and endpoint devices to protect the corresponding segments of the infrastructure from known and signature-based threats. Such protection must be complemented to protect against the breaches in the network that sit in between perimeter and endpoint devices from the continuing evolution of threat vectors and surfaces that attackers employ. AiCyberwatch caters exactly to this problem by building a cohesive multi layered security posture to combat the modern known and unknown threats and ensure the security of critical information accessed by the network.

The service moves away from static rules-based threat detection and instead uses elastic compute power, dynamic threat models, behavioral analytics, advanced machine learning, AI with actionable intelligence with proprietary feature engineering and anomaly detection algorithms without a need to establish pre-defined or static rules. Applying rich analytics that correlate the flow, event, system and user data with the anomalous behavior allows organizations to more effectively identify their great risks and high value assets that are most exploitable. By identifying the attack surface and providing prioritized actionable risk intelligence, organizations can proactively protect themselves against these new breeds of threats.

Behavioral analytics can be used to develop comprehensive models. This will provide an organization with the ability to conduct risk assessment of users and systems to alert all entities that may pose a potential threat. It sifts through and correlates large amounts of data in order to identify non-conforming patterns. Some of these anomalies might represent compromised credentials, a rogue user on the network,

unwarranted escalation of user privileges, and transmission of sensitive corporate information across unsolicited channels.

Many customers tend to ask as to why we include endpoints in our SOC coverage? the answer is simple, we cover end points as part of the solution as today the attacks are very sophisticated and signature less. The Network firewall may not be able to detect these and allow them to traverse through the network. Hence it is important to not only monitor the firewall, but also monitor the logs from the AD (active directory), Virtual or Physical servers through sys logs, Netflows, and Antivirus deployed on the endpoints. The solution is agent less and the logs are captured via enabling the requisite ports.

The monitoring not only involves North /South (via the firewall) but also East/West or lateral/horizontal. Which implies that we will monitor and report on anomalies that come in via the firewall undetected and those that are created by the endpoint within the LAN.

A typical use case would be malware that uses the DNS protocol to evade detection. The Domain Name System (DNS) is the part of internet infrastructure that resolves easily remembered domain names that human's use into more obscure IP addresses that internet connected computers use. Malware authors are using DNS protocol to keep their communications covert and evade detection. DNS today is one of the major attack vectors used by malware author for DNS command and control (C&C) and DNS exfiltration because DNS is part of internet's infrastructure and also DNS traffic is not analyzed by the firewalls and IDS/IPS devices.

Cybersecurity technologies deployed in today's enterprise are built on a fundamental hypothesis - smart humans must use an array of advanced security tools from different vendors that were not built to communicate with each other seamlessly, analyze data and provide correlation from multiple sources, automatically identify a threat and then mitigate it. The biggest concern for enterprises is protection of data of all forms, 95 percent of attacks exfiltrate or corrupt data within a few hours of the breach hardly enough time for smart humans to react! AiCyberwatch enables organizations to detect both known signature-based and evolving not yet seen cyber threats quickly, and to stop them as they happen, preventing the infliction of extensive corporate damage.

To know more reach out to us at sales@aicyberwatch.com or call us a +91 129 2250400

About AiCyberwatch

AiCyberwatch, is the Cyber Security initiative of NGBPS LIMITED. Leading the next generation of Cyber Security, AiCyberwatch helps build and transform cyber security postures via its innovative approach to managed security services, enabling business continuity and mitigating risks.

We strive to strengthen security resilience by defending your organization against advanced threats, help to achieve regulatory compliance and prevent security breaches, enabling you to concentrate on growing your business.

NGBPS LIMITED, Level 6, 606, SSR Corporate Park, Mathura Road, Faridabad - 121003 , Haryana | +91 129 2250400 | www.aicyberwatch.com