DAVID GROUP Managed Detection and Response (MDR)

What is DAVID GROUP Managed Detection and Response (MDR)?

DAVID GROUP Managed Detection and Response (MDR) is specifically designed to actively counteract online gambling advertisement insertion attacks, which have become a national issue, especially on government domains.

DAVID GROUP MDR is optimized to neutralize malware that conducts data espionage and steals sensitive information significantly on active servers.

- Special inspection service for more efficient processing.
- AI-based system optimized to detect evolving threats.
- Next-generation firewalls, endpoint security measures, and detection algorithms.
- Machine-learning program to create behavior profiles and quickly halt new threats.

Highlights

- 24/7 Monitoring
- Cyber Patrols
- Incident Response
- Advanced Analytics

davidgroup.co.id

DAVID GROUP Managed Detection and Response (MDR) aims to promote domestic innovation that is internationally standardized and supports efforts to increase the use of domestic products (P3DN) and technology development.

DAVID GROUP Managed Detection and Response (MDR) Key Notes

1. Offers Single Monitoring for More Efficient Usage

Functions and Capabilities

a. Provides a full-cycle dashboard that covers every threat vector and access point.
b. Offers integrated software that includes ITOps, SecOps, and NetOps.
c. Accesses and manages data, analytics, and automation from a centralized location.

2. Enhancing Productivity and Strengthening Cybersecurity

Functions and Capabilities

a. Automated threat hunting on endpoints, including threats with low prevalence.
b. Enables administrators to create and scan Custom Indicators of Compromise (IoCs).
c. Predictive network threat remediation driven by behavioral analysis.
d. Prioritizes threat remediation on a regular basis.

3. Providing Actionable Priorities, Wherever You Need Them

Functions and Capabilities

a. Collecting and correlating every detected cybersecurity vulnerability.
b. Continuous monitoring and patrolling.
c. Advanced analysis that produces contextual priority alerts when unknown malware and other silent attacks are detected.
d. Real-time continuous threat monitoring and prioritizing recovery/remediation.

4. Integrated Detection, Regardless of Vector or Vendor

Functions and Capabilities of DAVID GROUP Scan Engine

a. Detects and stops abnormal endpoint program behavior in operation, including exploit-based memory injection attacks.
b. Determines Indicators of Compromise (IoCs) with international mapping.
c. Monitors file reputation to detect and isolate threats at the entry point.
d. Identifies OS vulnerabilities in your environment, allowing administrators to prioritize recovery based on risk and reduce attack surface.
e. Uses advanced analysis to quickly detect unknown malware, insider threats such as data theft and policy violations, as well as other silent attacks.

5. Rapid and Accurate Threat Response

Functions and Capabilities

a. Rapid response to endpoint threats following a compromise.
b. Identifying and isolating the root cause of a problem or incident quickly.
c. Quickly stopping malicious malware through confirmed analysis.
d. Remediation using DAVID GROUP Cyber Security Compliance Standards.

davidgroup.co.id

https://e-katalog.lkpp.go.id/katalog/produk/detail/75407527

DAVID GROUP Cybersecurity Compliance Standards is aimed at promoting internationally standardized domestic innovations and supporting efforts to boost the use of domestic products (P3DN) and technological advancement.