deepwatch

ADVANCED DETECTION OF EVASIVE THREATS AT MACHINE SPEED

Deepwatch DetectML

Some threats and malicious behaviors aren't detectable with point-in-time rules and signatures. Today, businesses have more data than ever before that can be used to detect sophisticated threats, including ransomware, malware, and botnets. However, manually sifting through millions of logs is resource prohibitive, and many threats typically evade standard detection technology.

DetectML strengthens Deepwatch MDR service and Deepwatch Squad Expertise with threat detections by analyzing network data at machine speed. The DetectML proprietary software replicates the detection capabilities of multiple experts by analyzing large amounts of historical data and identifying threat patterns to reduce blind spots and maximize ROI.

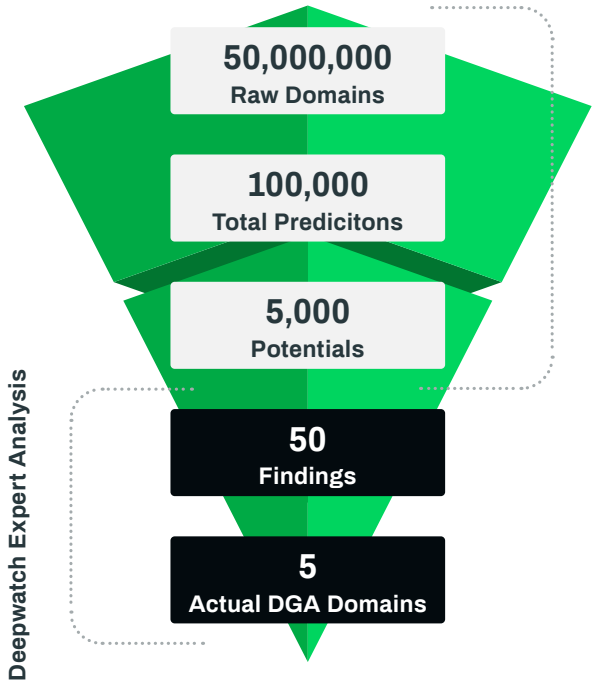
Today's Complex Attacks Require Advanced **Cyber Security Detections at Machine Speed & Scale**

Security leaders can dive deep into their data to identify malicious activity indicating compromise so they can respond before their business is disrupted or regulated data is lost. Deepwatch's proprietary software leverages cloud-based storage, sophisticated ML analytics, and Deepwatch's bench of security expertise to provide intuitive and actionable results.

Whether well-known malware variants or tailored attacks seen in APTs, sophisticated attack vectors often communicate in ways that are nearly indistinguishable from legitimate traffic on an organization's network. Critical threat information may be hidden in quiet signals in network flows, separate events, and/or disparate anomalies that require advanced analysis and customer-specific context to identify the threat.

Once these complex threats spread over long periods of time are identified, Deepwatch leverages its strong expertise in event correlation and ML platforms to yield high-fidelity results for further investigation.

PROCESSING TO DETECT MALWARE AND BOTNETS



Amplify threat detection capabilities of human security experts to find evasive threats by analyzing large volumes of data at machine speed and scale.

Advantages of Managed Detection and Response with **Machine Learning**

Get In-Depth Insights with Machine Learning and Data Analytics

- ✓ Identify malware and botnets at machine speed
- ✓ Detect attacker communications
- ✓ Identify unauthorized tools and communications

Augment the Deepwatch Squad to Detect Suspicious Activity

- ✓ Environment knowledge/contextualization across hundreds of customer environments
- ✓ Find the signal in the noise and apply expert human intelligence and judgment to take action

Stop Malicious Behavior and TTPs Early in the Attack Lifecycle

- ✓ Perform long-tailed historical analysis of large-scale security data sets based on DNS data
- ✓ Innovation rooted in attacker behavior & methods

Analysis at Machine Speed and Scale

- ✓ Replicate detection from hundreds of human experts at machine speed
- ✓ Seamlessly combine data sources to identify threats early

How **DetectML Works**

Deepwatch DetectML analyzes unaltered DNS log events from a secure S3 instance owned and managed by Deepwatch on behalf of the customer for activities pertaining to malicious domain communications. Potentially malicious domains are triaged, enriched, and sent to the squad for action with customer-specific context.

1 DNS Requests

Query sent from customer DNS client to a DNS server to ask for IP address associated with a domain name

2 Customer Data Landing Zone & Log Ingest (AWS)

Source type-specific setup:

- Umbrella - Customer or Cisco Managed S3
- Infoblox & MSID - Splunk data fork via Vector

3 Machine Learning Pipeline

The DetectML system runs, uncovering patterns, anomalies, and behaviors in data at scale

4 Prediction & Scoring

Deepwatch uses proprietary transformation and scoring logic to assign ranking and prioritization

5 Critical Domains Identified

TRIAGE: Highly critical domains are sent to the squad via XSOAR for expert investigation & analysis

6 XSOAR Enrichment

Suspicious domains are enriched in XSOAR with third-party intelligence & contextual information (Virus Total, WHOIS, etc.)

7 Deepwatch Squad

With environmental-specific insight, squads communicate customer risks and remediation steps

deepwatch

ABOUT DEEPWATCH

Deepwatch is the leader in managed security services, protecting organizations from ever-increasing cyber threats 24/7/365. Powered by Deepwatch's cloud-based security operations platform, Deepwatch provides the industry's most comprehensive detection and automated response to cyber threats together with tailored guidance from dedicated experts to mitigate risk and measurably improve security posture. Hundreds of organizations, from Fortune 100 to mid-sized enterprises, trust Deepwatch to protect their business.

CONTACT US

sales@deepwatch.com
4030 W Boy Scout Blvd, Suite 550
Tampa, FL 33607
855.303.3033
www.deepwatch.com