deepwatch™

HOLISTIC MODERN SECURITY OPERATIONS

OVERVIEW:

Holistic Modern Security Operations is designed to be easy, effective and efficient to transform traditional security operations through the active detection, prevention and response to today's most dangerous threats. To accomplish this, Deepwatch partners with best-of-breed data and security technologies and platforms to enable the cyber resilience enterprises need against today's threats.

Understanding that bad days will happen, whether from external threats or internal issues, our mission is to help enterprises understand their risks, execute appropriate responses, and continuously improve their security posture.

HOW IS THIS DONE?

Holistic Security is built on the following tenets:

- Expanded understanding, visibility and search capability of cyber security, and cyber relevant data without <explosively> increasing ingestion and correlation costs
- Allow for the contextualized, precision response across detection technology and types to enable true XDR capabilities
- Ability to combine the engineering, operationalization, advanced detections, and Deepwatch Expert based guidance to enable cyber outcomes that create understanding and resilience within an enterprise

Let's walk through the different modules and how they work together, and in what order, to provide cyber resilient security operations.

STEP 1

NEXT GEN
Managed Detection & Response:
CrowdStrike NG-SIEM (NG- MDR)

PRODUCT OVERVIEW:

Next Gen Managed Detection and Response is the foundation of a holistic modern security operations center, enhancing cybersecurity and ensuring robust protection and operational efficiency.

Key Features

- **Continuous Global Operations:** Deepwatch Experts provide 24x7x365 analysis and response
- **Security & Detection Engineering:** Advanced monitoring of data flow and availability notifications
- **Data Visibility & Selection:** Integration of 1st and 3rd party data selection and ingestion.
- **Migration & Operationalization:** Seamless migration from legacy SIEMs to modern solutions
- **Expansive Automation & Enrichment:** Extensive automation and data enrichment techniques

Benefits

- **Faster Detection and Response:** Quick identification and mitigation of threats
- **Reduced Ingestion Costs:** Efficient data management reduces costs
- **Increased Visibility:** Improved data visibility improves situational awareness and threat detection.
- **Improved Security Posture:** Integration of modern technologies enhances security posture and protection

STEP 2

NEXT GEN
Cyber Data Management
Cribl Edge & Stream (NG-CDM)

PRODUCT OVERVIEW:

Next Gen Cyber Data Management dynamically amplifies the value of cyber data by managing ingestion from various sources and ensuring real-time data flow monitoring and availability.

Key Features

- **Data Ingestion Management:** Handle data from any source to multiple destinations.
- **Real-Time Monitoring:** Monitor data flow and receive availability notifications.
- **Normalized Data Routing:** Simplify complex filtering or transformation needs.
- **Sensor Fleet Management:** Manage sensor fleets and nodes effortlessly at scale.
- **Distributed Search:** Conduct searches across multiple data repositories.

Benefits

- **Scalability:** Easily scales to handle growing data volumes.
- **Real-Time Insights:** Provides immediate insights through real-time data monitoring.
- **Operational Efficiency:** Simplifies the management of diverse data sources and destinations

STEP 3

NEXT GEN
Managed Endpoint Detection & Response
(NG-MEDR)

PRODUCT OVERVIEW:

NG-MEDR offers real-time identity threat detection, leveraging a single-agent platform to enhance cyber resilience by detecting, preventing, and remediating identity-based attacks.

Key Features

- **Enhanced Endpoint Insights:** Provides deep insights through log sources.
- **Higher Fidelity Signals:** Uses high-fidelity EDR signals for precise threat detection.
- **Augmented Data Telemetry:** Enhances EDR data with log telemetry from various sources.
- **Contextual Enrichment:** Enriches detections with log data, reducing triage time, false positives, and accelerating MTTR.

Benefits

- **Threat Prevention and Analysis:** Systematically mitigate threats.
- **Rapid Response Times:** Quick responses to critical alerts minimize downtime and damage.
- **Integrated Platform:** Integrated into the Deepwatch Platform, enhancing enrichment, correlation, intelligence, and automation
- **Continuous Optimization:** Regular health and tuning recommendations ensure ongoing endpoint protection effectiveness.

STEP 4

NEXT GEN
Identity Detection & Response (NG-IDR)

PRODUCT OVERVIEW:

NNG-IDR offers real-time identity threat detection, leveraging a single-agent platform to enhance cyber resilience by detecting, preventing, and remediating identity-based attacks.

Key Features

24/7 Monitoring: Continuous surveillance of user activities and identity assets.

Advanced Threat Detection: Utilizes AI and machine learning to identify suspicious behaviors.

Rapid Incident Response: Provides immediate action to contain and neutralize threats.

User Behavior Analytics: Analyzes user behavior for deviations from normal activity.

Customizable Alerts: Delivers tailored notifications based on organizational needs.

Benefits

- **Enhanced Security:** Provides robust protection against identity-based threats.
- **Reduced False Positives:** Improves detection accuracy, reducing false positive rates.
- **Faster Response:** Enhances response times with expert support and advanced analytics.

STEP 5

NEXT GEN
Cloud Detection & Response (NG-CDR)

PRODUCT OVERVIEW:

The Next Gen Cloud Detection & Response module extends detection and response capabilities to cloud-native workloads, providing enhanced visibility and protection against cloud-based threats.

Key Features

- **Cloud-Based Threat Detection:** Active response for cloud threats, integrating CWP and CSPM.
- **SOC & Falcon Console Integration:** Unified management within the Deepwatch Platform.
- **Multi-Cloud Monitoring:** Comprehensive monitoring of AWS, Azure, and GCP environments.
- **Auto Remediation:** Automates responses based on risk tolerance.
- **IOA Monitoring:** Monitors and responds to suspicious cloud activities.

Benefits

- **Improved Visibility:** Enhances visibility across multi-cloud environments.
- **Automated Response:** Reduces response times with automated remediation.
- **Holistic Management:** Provides a centralized management solution for cloud security.

STEP 6

CHOOSE YOUR NEXT STEPS

Program Options

Enterprises that have addressed their 24/7 Security Operations, matured their EDR program to enable active response at machine speed, and engaged additional protection and response for Identity and Cloud now have to select the area of their next address real needs.

What does the organization need first?

- **Data Needs:** To store additional logs in a security specific location, and for how long?
- **Prioritization and Patch**: How valuable is prioritized alerting, correlation, and response based on vulnerability data for exposed systems?
- **Compliance or Long Term Storage:** To meet data retention requirements for compliance or audit?
- **Threat Hunting:** The ability to go farther back in the security record to review prior actions and connections enable more comprehensive hunting?

Selection Criteria

Both Cyber Data Lake and Vulnerability & Exposure Management are valuable add-on modules for a Holistic Modern Security organization. Vulnerability & Exposure Management helps prioritize analysis, detection, and response for large organizations with complex operations. A security-specific data lake assists with long-term log storage for enterprises needing searchable data beyond standard retention terms.

STEP 7 a

NEXT GEN
Cyber Data Lake
(NG-CDL)

PRODUCT OVERVIEW:

The Next Gen Cyber Data Lake offers flexible data storage, retention, and retrieval by managing data ingestion from various sources, allowing configurable data replay and rehydration for forensic analysis or training.

Key Features

- **Manage Data Ingestion:** Seamlessly ingest data from multiple sources into the cyber data lake.
- **Configurable Data Replay:** Rehydrate data for forensic lookback or training.
- **Turn-Key Access:** Set up an isolated cyber data lake within hours.
- **Compliance Solutions:** Meet specific compliance and retention requirements.
- **Unified Search:** Perform retrospective hunts across multi-year data storage.

Benefits

- **Cost Efficiency:** Reduces costs associated with increasing log sources and complex storage engineering.
- **Enhanced Analysis:** Provides insights from data swamps and supports detailed forensic investigations.
- **Compliance:** Helps meet stringent compliance and retention requirements.
- **Real-Time Insights:** Provides immediate insights through real-time data monitoring.
- **Operational Efficiency:** Simplifies the management of diverse data sources and destinations.

STEP 7 b

NEXT GEN
Vulnerability & Exposure (NG-VEM)

PRODUCT OVERVIEW:

Next Gen Vulnerability and Exposure offers real-time assessment, management, and prioritization of vulnerabilities, simplifying patch management, compliance, and reporting for strong cyber outcomes.

Key Features

- **Real-Time Vulnerability Assessment:** Instantly assess vulnerabilities without lengthy scans.
- **Behavioral Classification and Passive Discovery:** Monitor and classify assets based on behavior.
- **Compliance Verification:** Automatically check device configurations against standards.
- **Guided Remediation and Mitigation Strategies:** Receive tailored guidance on addressing vulnerabilities.
- **Exposure Identification:** Quickly identify internet-exposed infrastructure for faster risk mitigation.

Benefits

- **Improved Efficiency:** Faster identification and remediation processes.
- **Enhanced Security Posture:** Proactive management reduces breach risks.
- **Compliance Assurance:** Ongoing verification of compliance with standards.
- **Reduced Operational Burden:** Automation and expert guidance ease security team workload.
- **Accelerated Response Times:** Immediate insights enable quicker responses.