deepwatch™

WHITEPAPER

Deepwatch Threat Analytics:

The Practical Approach to Low Volume, High Fidelity Alerting to Build Cyber Resilience

www.deepwatch.com

TABLE OF CONTENTS

deepwatch™

Executive Summary

Organizations need continuous visibility into the complex threats within their networks and data.

A variety of security operations tools are available to help security teams understand, visualize, and communicate an organization's risk level. Unfortunately these tools create an avalanche of alerts, making it virtually impossible for teams to assess and respond to threats before they cause damage.

Modern security operations (SecOps) tech stacks consist of various security tools from endpoint protection and network firewalls to cloud security solutions. All of these tools generate alerts to inform IT and security teams of a potential event. An alert may be irregular and/or minor but does not seriously impact a business, or an alert could be highly disruptive and possibly cause a loss of revenue, making it an incident.

Accurate correlation and curation of alerts across different systems is needed to paint a complete picture of the potential threat activity in an environment. Deepwatch Threat Analytics uses our proprietary Dynamic Risk Score methodology to ensure customers see only actionable alerts with an extremely high fidelity rating, while reducing overall alert volume.

Deepwatch Threat Analytics

Introduction

As cyber threats become more pervasive and complex, security teams must not only consider how threats originate, they must know how they persist and evolve. Teams must continuously discover new indications of compromise and understand how they relate to others, or identify where multiple alerts point to the same threats.

Deepwatch Threat Analytics capabilities offer security teams expanded visibility into their environments through contextualization. Correlating risks across users and activity over time is critical. By correlating related threat activity for a single entity, Deepwatch Threat Analytics can reduce alert overload and reduce time spent on other analysis, improve detection and drive accurate, rapid response.

Threat Analytics, the use of data analytics to achieve security outcomes, is a core capability within the Deepwatch platform. Deepwatch Threat Analytics uses our proprietary Dynamic Risk Score methodology to ensure customers see only actionable alerts with an extremely high fidelity rating.

Security Team **Maturity**

Today a variety of security operations tools and vendors offer SecOps teams ways to understand, visualize, and communicate an organization's risk level.

SIEM and SOAR solutions are typically the first stops on their maturity journey, and teams spend much of the SecOps time understanding then fine-tuning these tools to meet security objectives. Because they represent significant investment, it is important to find ways to expand capabilities within SIEM and SOAR solutions, as opposed to replacing them.

Customization and fine-tuning, however, can lead to problems and visibility gaps. For example, compliance-driven organizations may only focus on high or critical alerts mapped to PCI or HIPAA, then fail to adjust for new ransomware techniques. Sophisticated data-centric approaches like workload protection must approach SOC operations based on capacity, but may not be optimized to identify new threats.

Risk-based approaches provide the most protection, but are difficult and expensive for most teams to implement. Risk based approaches triage risk-informed alerts based on severity levels specific to a single organization.

How do SOCs Address this Today

The Evolution of SOC Alerting Processes

Ad-Hoc Approach

- Opportunistically log in tools and look into things that matter most
- Typically direct work in product consoles
- **DOWNSIDE:** Highly inefficient and high likelihood of errors

Compliance Approach

- Address only high & critical alerts
- Manage "scope" - alerting on log sources in compliance tagged systems (PCI/PHI/NYDFS/etc...)
- **DOWNSIDE:** Attackers don't care about compliance scope

Workload Based Approach

- Triage based on capacity (X of Y% is reviewed in Z timeline per internal SLAs)
- More sophisticated as a data-centric approach
- **Downside:** Not optimized; probable to miss something in the gap

Risk Based Appraoch

- Triage alerts based on risk informed approach to build severity levels specific to your organization
- Continously improve models to maximize time spent and investments needed to implement
- **DOWNSIDE:** It's HARD!

Increased CMMI as Moving to the Right

Security Team **Maturity** (continued)

Alert Deduplication, Enrichment & Prioritization

Threat detection and threat analysis reaches beyond SIEM and SOAR capabilities, and offers teams greater insight into risks throughout their environment. Alerts can be processed further through deduplication, enrichment, and prioritization.

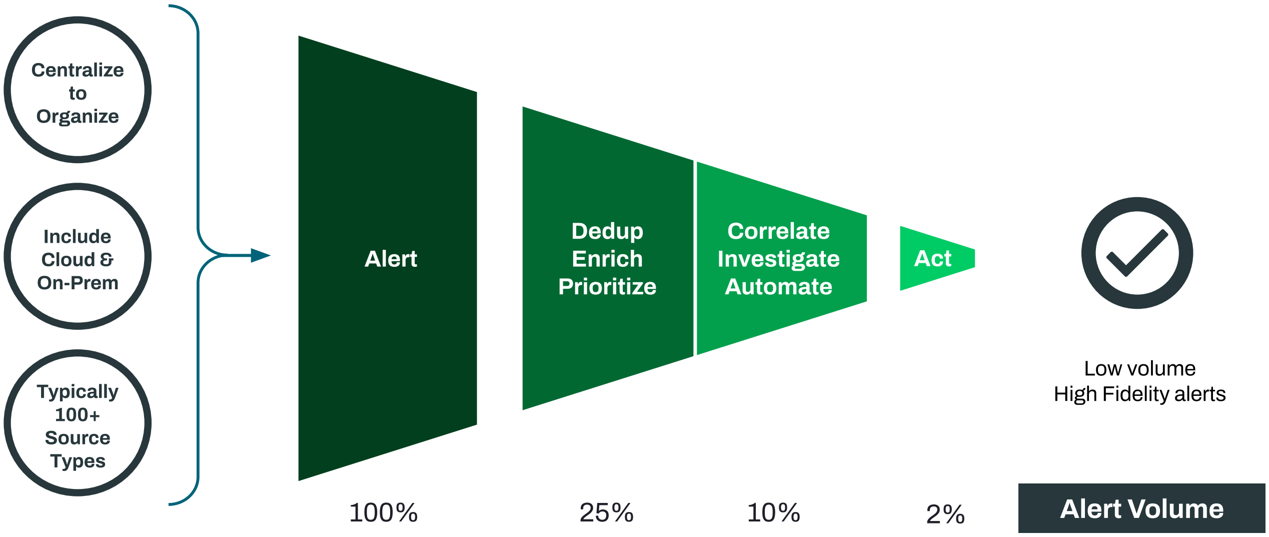
Alert deduplication is the process of reducing alert noise by organizing and grouping alerts. Alert enrichment removes false-positives and deduces actionable intelligence from alerts. SOCs can see a nearly 75% reduction in alerts through these processes.

SOCs can then use advanced correlation and investigation to further reduce actionable alerts. Together, advanced correlation and investigation can help reduce the actionable alerts by more than 90%. However, even after these refinements, the SOCs still have to process tens of thousands of alerts.

Core Principles:

- Use all data; don't drop things at process flow overloads
- Enrich across alert types; not simply within single vendor alerts
- Leverage SOAR whereveer possible

Preferred Principle of Alerting



Emerging and Complex **Threats**

Threat actors develop new tools, techniques, and procedures every day. To discover emerging threats and address their inherent complexity, security teams must be proactive and focus on correlation of alerts or events.

With more sophisticated adversaries and newer techniques, a human element is often required to review or confirm the work of automation platforms. While this is critical, it also slows the remediation process and proves to be difficult in many resource-strapped organizations. This problem results in effective blind spots and in missed events that can prove disastrous to the organization.

Threat Analytics

The Deepwatch Threat Analytics capability within our platform allows us to remain aware of those events that might otherwise fall below normal alert thresholds, trending and correlating them over a period of 30 days. This results in fewer alerts and more actionable data, allowing security teams to focus on other priorities while improving their overall security posture.

Deepwatch Threat Analytics is a dynamic alert correlation technology that normalizes all alerts from multiple technology types into a single Risk Object. Correlation across every transaction generates a Dynamic Risk Score. Under this customizable framework, low and medium severity alerts aren't discarded. Instead, additional context on suspicious but non-alertable activity is preserved e.g. increased auth/web activity.

Where one event might not matter, two are potentially more problematic. Using Deepwatch Threat Analytics, organizations are able to provide continuous awareness based upon monitoring activities affecting identified risk objects. Bringing those events to the surface greatly increases our ability to protect our customers.

Deepwatch Threat Analytics ensures we deliver data-enriched, actionable alerts to customers while reducing the overall volume of alerts. This asset criticality identification process allows users to set an increasingly sensitive alert target on those applications, systems, identities, and services that matter the most.

Not only does this ensure that what matters the most to our clients is escalated, but it also allows Deepwatch to help improve our clients' reporting capabilities, presenting the opportunity to overlay a virtual segmentation schema where none previously existed. In organizations with older, less structured architectures, this is a game changing ability.

Deepwatch works with our customers to identify critical assets and configure our alerting platform to appropriately scale notifications to ensure that the most critical systems, applications, services, and identities receive the critical care that they deserve. This is one of the foundations of our services and capabilities, and Deepwatch works diligently to ensure that all information and supporting system configurations remain current at all times.

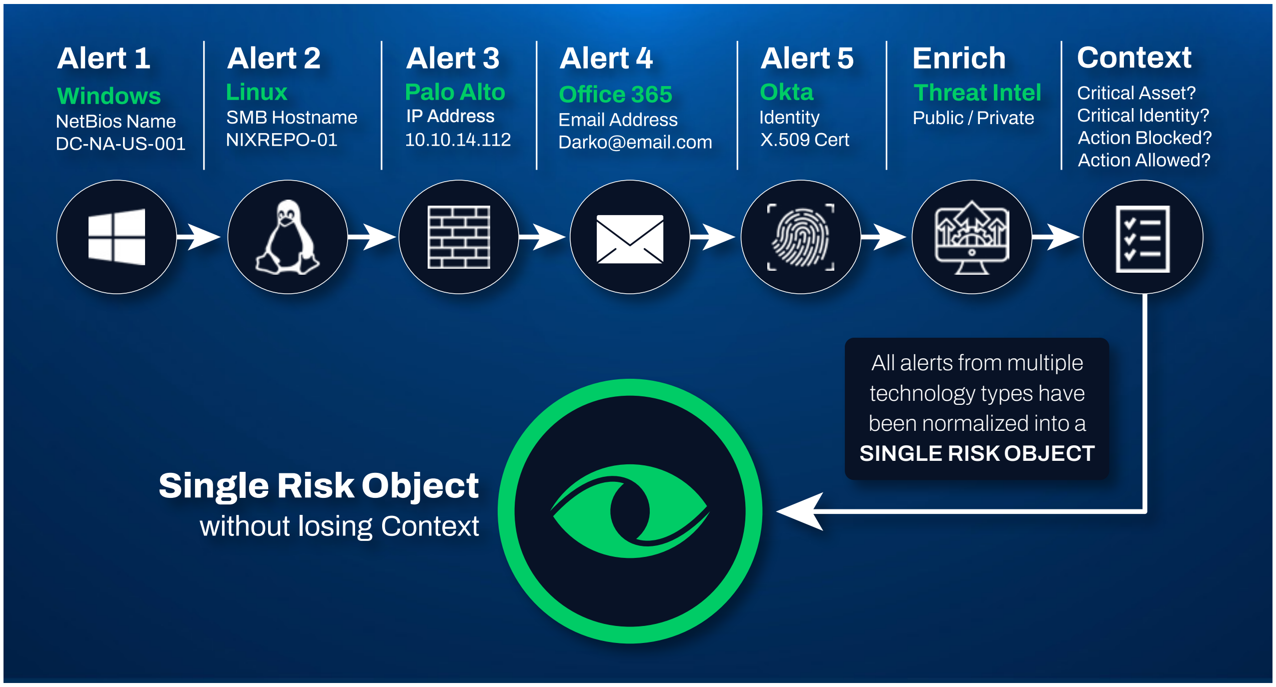
In addition, Deepwatch rolls this risk-based triggering methodology into our common analysis and alerting practices through our Dynamic Risk Score calculations. On a client-by-client basis, we work to understand the thresholds that constitute an alertable event.

For example, one client may not be concerned about PowerShell alerts when few people have Windows admin privileges and they are performing cert signing tasks. Another client may have hundreds or thousands of people with PowerShell access, creating additional risk.

Emerging and Complex **Threats** (continued)

How Does it **Work?**

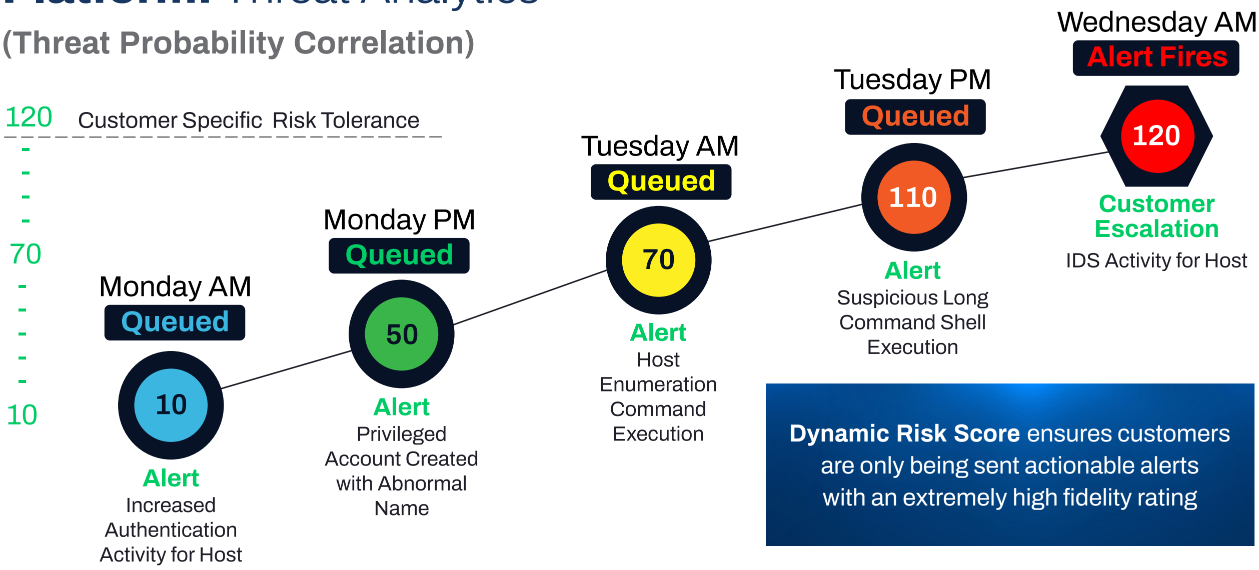
Consider this case in context:
a compromised windows machine with NetBios Name DC-NA-US-001 that becomes infected through email Drako@gmail.com and a compromised identity communicating with a rogue IP address may generate different alerts for host, email and FW. In this instance, SOC analysts are left to make sense of all these different alerts to get a complete picture of the threat. **Deepwatch Threat Analytics is able to correlate these alerts to a single risk object without losing the context.**



All alerts from multiple technology types have been normalized into a SINGLE RISK OBJECT

Platform: Threat Analytics

(Threat Probability Correlation)



Dynamic Risk Score ensures customers are only being sent actionable alerts with an extremely high fidelity rating

Benefits of Threat Analytics

Deepwatch Threat Analytics provides customized action points, combined with the ability to overlay the customer environment with a robust web of asset-specific criticality weightings, **ensuring that alerts delivered truly matter.**

Deepwatch Threat Analytics capabilities provide detection and analysis across on-prem, cloud, and SaaS applications. This solution provides visibility into privileged access from users, machines, and workloads, and can discover complex attacks early, before they have a chance to move laterally through a network. Utilizing Deepwatch Threat Analytics capabilities can help security teams create a stronger, more proactive security posture.

Enterprise customers benefit from Threat Analytics capabilities as a core component of the Deepwatch MDR platform. Along with our unique Dynamic Risk Score scoring methodology, Deepwatch Threat Analytics help us deliver higher fidelity, lower volume alerts and the best detection in the industry.

Reduce False Positives and Resource Drain

The growing volume and complexity of attacks makes it difficult for security teams with limited resources to keep up. An expanding array of technology solutions provides an avalanche of log data and alerts, but many security teams consist of less than five full-time employees. Those teams must reduce the number of fires they feel compelled to put out, and they have limited security expertise.

Deepwatch Threat Analytics capability within our platform works with best-in-class SIEM and SOAR technologies. Customers can leverage their existing investments in security tools. The Deepwatch platform is transparent and allows access to a customer's SIEM.

The Deepwatch platform enables customers to add response capabilities at their pace and customize the workflow based on their needs.

- All alerts from multiple technology types are normalized into a single Risk Object
- Additional context on suspicious but non-alertable activity e.g. increased auth/ web activity
- Dynamically upgrade & downgrade the severity of an alert based on custom conditions

Benefits of Threat Analytics (continued)

Security teams **benefit from Deepwatch Threat Analytics** in six key areas:

- **Improved coverage** based on MITRE framework
- **Enriched correlated alerts** for investigations and remediation
- **Improved risk value** based on activity within the customer environment
- **Significant reduction in time** to triage alerts
- **Improved higher fidelity of alerts** through enrichment, correlation and risk tolerance
- **Reduced volume of alerts** elevated to customer for review and action

Case Study: Threat Analysis Stops PowerShell Attack

In one example, Dynamic Risk Score correlation helped thwart a download of data-harvesting tool Sharphound from an unknown user. Unique use cases fired for Malware Activity, Unknown Powershell, Unknown Sys Info Discover, unknown Trusted Developer Utilities Proxy Execution, and unknown Process Hollowing. Without Threat Analytics, each of these events will result in individual alerts. With Threat Analytics, the SOC analysts can see that all these activities were tied together and is an attempt by someone to execute PowerShell.

Deepwatch observed a Powershell request to download Sharphound as a .ps1, potentially attempting to evade using an executable by instead using a Powershell script. However this was also blocked. This was potentially blocked by the execution policy, as the following command was a request to bypass -ep, which was also blocked. Two hours later, at 17:09 EST we observed a different set of tactics. The same user attempted to use in house building applications (MSbuild) to likely bypass the security policy. All observed attempts were also blocked.

Active directory logs show that this user had the title of "security engineer" and belonged to several elevated permission groups, including domain administrators. This activity was observed in multiple prior tickets from this user. Furthermore, we observed Crowdstrike SAML login activity to the Crowdstrike console five times between 7AM and 2PM that same day, which could indicate preparation for an internal pen test. The Dynamic Risk Score for a specific workstation increased from 0 to 120 in a period of 48 hours. The customer was alerted only after Dynamic Risk Score increased beyond the configured risk tolerance.

In another example, a higher-ed institution was able to dramatically reduce the number of alerts by applying Deepwatch Threat Analytics. Prior to its application, the college faced over 5,000 individual alerts per week with approximately one percent resulting in a true positive. Deepwatch Threat Analytics were able to reduce alerts while providing more actionable data.

Threat Analytics: Customer Benefits

Activity would have normally come through as a series of individual alerts. Deepwatch Threat Analytics was able to successfully capture, correlate and elevate for analyst review.

High-ed institution realized a **higher fidelity in alerts** once they adopted Deepwatch

5,000 ALERTS
PER WEEK PRIOR TO DEEPWATCH

150 ALERTS
PER WEEK POST DEEPWATCH

1% TRUE POSTIVE
PRIOR TO DEEPWATCH

53% TRUE POSTIVE
POST DEEPWATCH

deepwatch™

Deepwatch® is the leading managed security platform for the cyber resilient enterprise. Our platform combines patented, innovative technology with Deepwatch expert security practitioners to deliver unmatched threat detection and response capabilities. By operating as an extension of your cybersecurity team, we provide comprehensive security management, 24x7x365 monitoring, and precise automated threat responses. Deepwatch enhances visibility across your attack surface, improves security effectiveness and value through security technology and human security expertise. Join the growing community of leading brands who rely on Deepwatch for peace of mind and cyber resiliency.

THANK YOU

CONTACT US

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

www.deepwatch.com