CYBERSECURITY RISK HUNTING

The Foundation of Exposure Management

PREDICT AND BREAK ATTACK PATHS

REVEALD

Endpoints are the primary vehicle for infiltrators, and for many organizations that means hundreds or thousands of devices that need to be protected, including rogue devices. Today, defending against cyber attacks is largely defensive, complex, time-consuming, inefficient, and expensive.

This white paper presents a new offense-based approach — one that proactively evaluates risks across business systems, prioritizes protective actions, and mitigates attacks. When you understand what's possible, you can prevent a cyber attack before it happens.

ENDPOINT DEVICE CYBERSECURITY STATISTICS

68% of organizations have had an endpoint attack that compromised corporate data; 81% of those attacks involved malware[1]

80% of cyber incidents are the result of a new or unknown zero-day attack[4]

53% of organizations were hit with a ransomware attack in 2021; 69% of CISOs anticipate their company will suffer a ransomware attack in 2022[2]

55% of security professionals say smartphones are the most vulnerable endpoint device[1]

33% of workers use an endpoint device to work remotely[3]

1 Ponemon Institute, Cybersecurity in the Remote Work Era: A Global Risk Report
2 Black Kite, 2022 Third-Party Breach Report
3 SailPoint, The Cybersecurity Pandora's Box
4 Ponemon Institute, The Third Annual Study on the State of Endpoint Security Risk

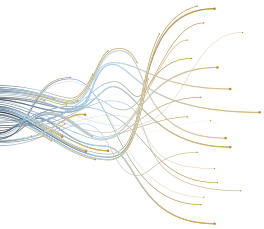
BECAUSE THREAT HUNTING
ISN'T ENOUGH

Defending against cyber attacks is vital, but it has become even more complicated, painstaking, and costly over time. The larger your system, the harder it gets. The number of attack paths grows exponentially with every new device that is connected to the network, each one adding a new entry path for threat actors to exploit.

Attackers don't need special technical skills, zero-day exploits, or nation-state backing to access your systems. They just need to take advantage of errors — which can be as simple as forgetting to change a policy or using the access credentials of a forgotten identity — and they can take control of your entire system. This is well-known, but seemingly impossible to predict and fix.

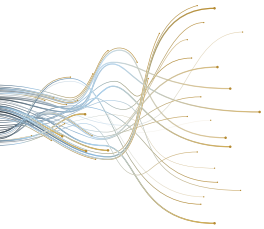
PREVENTING CYBER ATTACKS IS IMPOSSIBLE.
UNTIL IT'S NOT.

Threat hunting is still a defensive activity and has limitations. Anti-virus (AV) software, vulnerability scans, and other endpoint tools certainly help find and fight threats. But event-focused "threat hunting" has its limitations, which include:



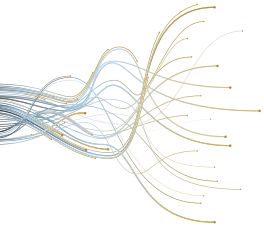
THREAT HUNTING RELIES ON AN OVERWHELMING VOLUME OF DATA AND ALERTS

Because this data is often-siloed, cross-system analysis is difficult, if not impossible. IT and security teams (both in-house and outsourced) waste too much time chasing false alerts and manually analyzing data. Because there is so much generated data, IT and security teams can't prioritize their focus on the actual problems. That makes everything a problem, and nothing is protected.



VULNERABILITIES ARE ONLY A SMALL PART OF RISK BUT GARNER A GREAT DEAL OF TIME AND ATTENTION

Risk comes from many sources, including porous defensive systems, ineffective security strategy systems, and even rogue devices. When defending for just one type of risk, the bad guys take advantage of open opportunities elsewhere in your security program.



THE COMMON VULNERABILITY SCORING SYSTEM (CVSS) IS A FLAWED METRIC

CVSS is heavily vendor-dependent, and it lacks "meta-awareness" of system interactions. For example, it can't tell you what data nodes have the greatest impact on your operations.

Threat hunting is helpful, but it doesn't go far enough to protect your devices from cyber attacks. All potential risk conditions must be investigated, from application misconfigurations and mitigation misalignments to inadvertent exposures.

Most importantly, not all threats are created equal. Risk should be ranked by financial and operational impact, and once that is determined, IT and security resources can be directed to correct the most critical problems. This is the core of risk hunting.

CLOSE ATTACK PATHS BEFORE INFILTRATION

Risk hunting is like hurricane tracking, but would actually stop the hurricane from happening. Technology can map out all the possible paths an attacker could take, rank the most likely paths based on algorithms and behavioral models, and then build defenses around those paths first. Risk hunting anticipates the danger that could happen and does everything possible to minimize the damage.

RISK MANAGEMENT PROGRAMS OFTEN DON'T FOCUS ON TRUE RISKS

Many risk or vulnerability management programs focus on issues such as identifying and fixing vulnerabilities and patch management, rather than on the actual risks to business operations.

Threat hunting is a close companion of vulnerability management. It is designed to identify threat activity, especially after the public release of information on threat actors or vulnerabilities. From the time a threat source's tactics are released to the time the vulnerability is patched, organizations react to the threat alone, without fully recognizing the associated risk (e.g., loss of business continuity, damaged reputation, compliance violations, etc.). In other words, threat hunting does not fully factor in or prioritize the business risks that could do the most damage to the organization.

IT'S TIME TO MOVE FORWARD

In contrast, risk hunting is a proactive effort to fully understand the context of both technical and business risks, designed to prevent the most potentially damaging attacks from happening in the first place. Risk hunting identifies problematic technical conditions and their impact on confidentiality, integrity, and system availability before these weaknesses can be exploited.

Risk hunting can also be used to analyze system anomalies, expanding the data around an event to show the full potential business impact of that event — on revenue, for example. With full awareness of business operations as well as technical systems, risk hunting gives organizations a fuller, clearer view of the potential negative impact of each risk.

THREATS AND THREAT SOURCES

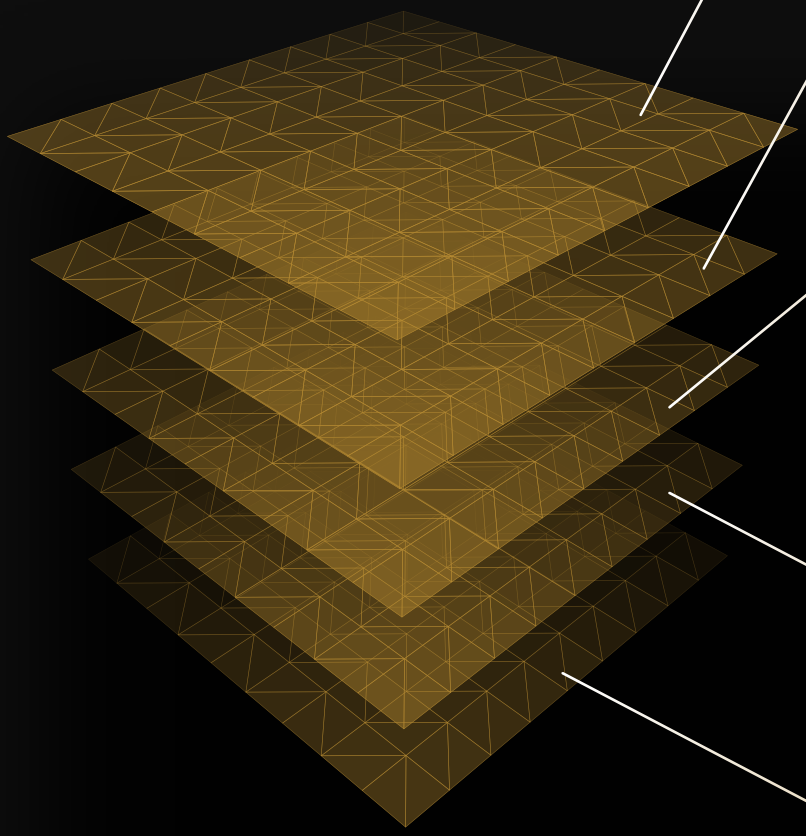
Organizations try to quantify threats, threat actors, and threat sources in many ways. The U.S. Computer Emergency Readiness Team (US-CERT) defines a threat as "persons who attempt unauthorized access to a control system device and/or network using a data communications pathway."[5]

Risk hunting requires knowing threats and threat sources before the cyber attack.

5 US-CERT: Cyber Threat Source Descriptions

With so many threat sources proliferating and attacking from all directions, **it's no wonder security teams are overwhelmed.**

US-CERT COMMON THREAT SOURCES[5]



POTENTIALLY SERIOUS

National Governments and Cyber Warfare Programs

- Government Take down
- Espionage
- Infrastructure Disruption
- Destruction

POTENTIALLY HIGH

Hackers — Including Bot Network Operators

- Profit
- Achievement
- Notoriety
- Disruption
- Property Damage
- Casualties

MEDIUM

Industrial Spies and Organized Crime

- Profit
- Destruction
- Competitive Espionage
- Theft of Trade Secrets
- Blackmail

MEDIUM

Hacktivists

- Support for Political Agenda
- Propaganda
- Notoriety

LIMITED

Terrorists

- Terror
- Casualties
- Weakened Economy

NIST 800-82 categorizes threat sources by type (adversarial, accidental, structural, and environmental) and identifies additional, specific threat sources:[6]

INSIDERS

Employees or other internal parties who have access to enterprise assets.

PHISHERS

External parties who attempt to trick insiders into surrendering private or confidential info for monetary gain.

SPAMMERS

Distributors of unsolicited email who sell products or use other schemes to make money.

SPYWARE AUTHORS

Malicious parties who attack users by distributing spyware and malware like ransomware.

6 NIST 800-82: Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security

REACTIVE VS. PROACTIVE SECURITY

Reactive event-driven security tools require a cyber event, which triggers an automated defense or alert. These types of security tools, like Security Information and Event Management (SIEM) systems and supporting technologies such as endpoint protection platforms, are necessary but have limitations, including:

A HIGH-VOLUME OF ALERTS THAT REQUIRE INVESTIGATION

ALERTS THAT REQUIRE MANUAL CROSS-REFERENCING OF DATA BETWEEN TOOLS

A HIGH-NUMBER OF FALSE POSITIVES
(an activity or condition that triggers an alert without posing an actual threat)

DATA SOURCE INCOMPATIBILITY DUE TO DATA NORMALIZATION REQUIREMENTS

LIMITATION OF HISTORICAL ANALYSIS FROM MULTIPLE DATA SOURCES

Advanced SIEM systems try to identify potential intrusions through anomalous behaviors in order to reduce false positives and detect true intrusions sooner. But this approach is still limited to responding to an attack in progress. **It does not — and cannot — protect against an attack before it starts.**

FULLY OPERATIONALIZED
RISK HUNTING

When fully operationalized and deployed, risk hunting focuses on the entire system, aggregating and analyzing information generated from all meaningful data points in the security and IT infrastructure. No further interrogation of endpoints is needed to determine an enterprise's current risk posture and identify critical risk conditions that need to be addressed. With a risk-hunting solution, security teams can identify areas with the greatest impact on revenue, uptime, and other key business operations — not just which vulnerabilities have the highest arbitrary rating.

Although a risk hunting solution is not event-based, it can be event-driven. Events are used to generate analysis of the system, communicating the findings to the IT team. Risk hunting offers specific insights about every possible attack path, from locating the domain controllers to prioritizing threat vectors.

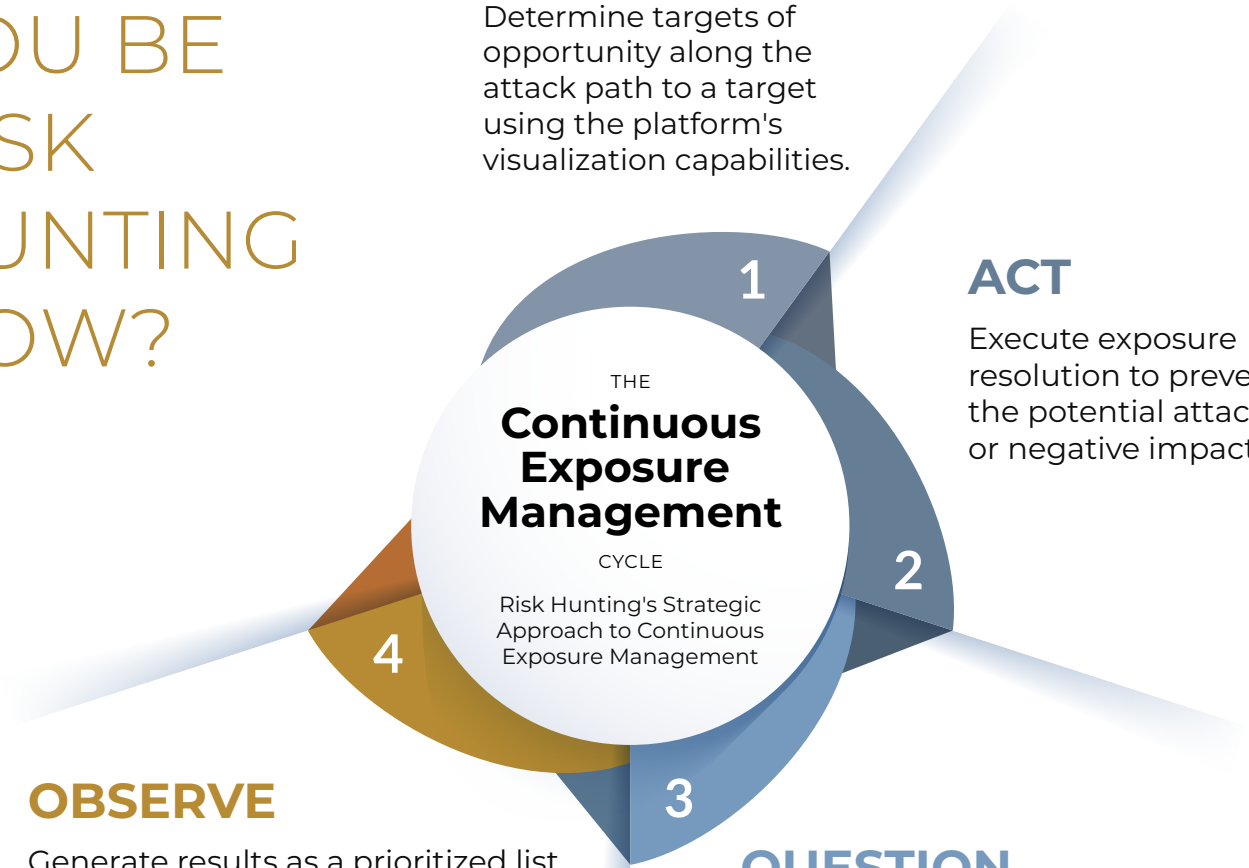
A state-based risk-hunting solution cross-references data automatically and predictively across all data sources to identify all attack paths. It also maps potential consequences along each path — a unique capability that improves response and resolution times, and reduces time wasted on false positives generated by endpoint solutions alone.

THE BREAK-FIX CYCLE

SHOULD YOU BE RISK HUNTING NOW?

ANALYZE

Determine targets of opportunity along the attack path to a target using the platform's visualization capabilities.



ACT

Execute exposure resolution to prevent the potential attack or negative impact.

OBSERVE

Generate results as a prioritized list. Determine which mitigations are being used effectively. Identify the highest impacts to the business. Ask: How do I reduce or eliminate the threat's ability to succeed? How do I mitigate the most risk to the business?

QUESTION

Identify nexus points — points of transition where attacks flow through. Ask: when here, where do we go? Where do impacts occur? Explore the outcomes. These can include network and host reconnaissance.

ONCE REVEALD. EXPOSURE RESOLVED.

Risk hunting is based on the state of an entire system, not just events, and is dynamic and real-time. It aggregates data from across the security and IT infrastructures to identify critical risk conditions that need to be addressed — before an attack occurs.

THE PROBLEM

Security teams focused on event-driven threat investigation tend to get stuck in a break-fix cycle, like an endless game of whack-a-mole. It's hard to move beyond this mindset and think holistically about how to address and reach the business outcomes.

THE SOLUTION

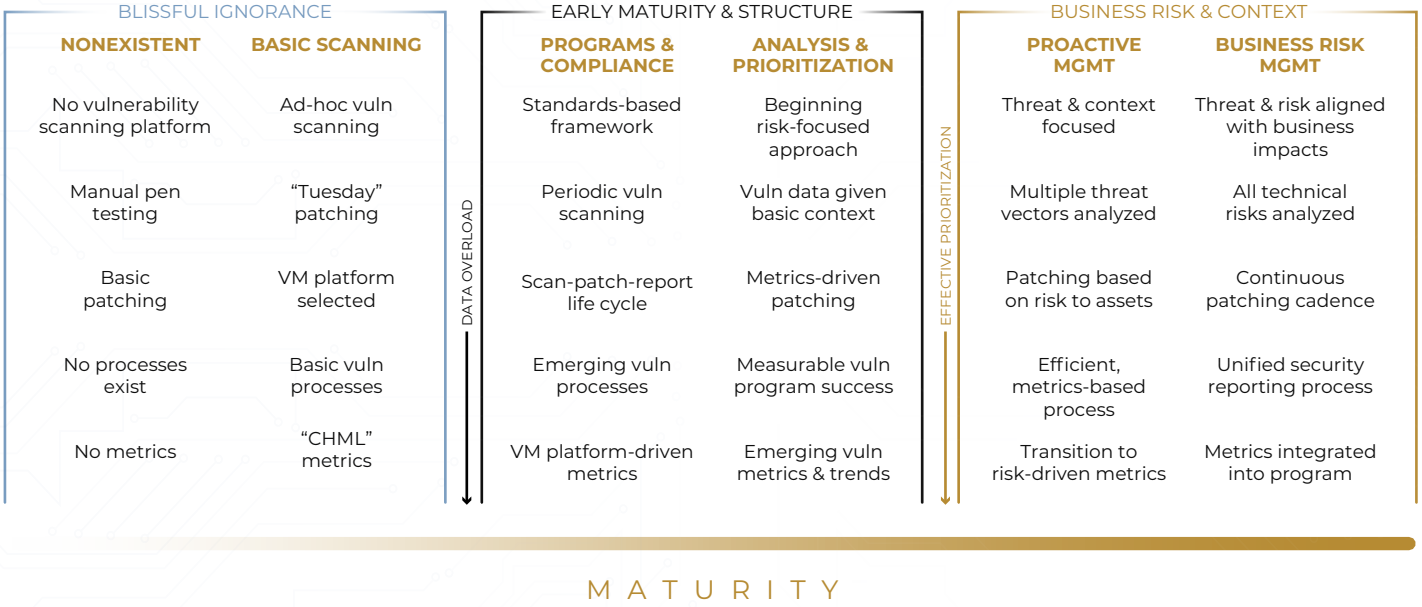
Preemptive action is taken to "fix it before it breaks" with a state-based risk-hunting platform, which is more effective than trying to "fix it after it breaks" with event-driven security tools. Risk hunting provides a seamless transition from a threat-and-vulnerability focus to a risk-and-priority focus. Security teams can go on the offensive and become proactive risk hunters. The goal is to think like the adversary and use that perspective to take a new approach to protecting endpoint devices.

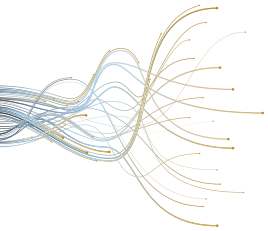
Organizations of any size can benefit from risk hunting — especially those with hundreds or thousands of devices across their systems. In many environments, security programs produce more data than can be effectively managed. An organization may have policies and tactical tools to identify vulnerabilities and detect attacks, but those tools generate so much information, IT teams are likely to be overwhelmed. Although every organization generates data, each business has unique risk challenges. To determine if risk hunting is the right tool for your company, you first need to know your risk level determined by the Cyber Risk Maturity Matrix.

THE REALITY OF RISK HUNTING

More than just an upgrade over traditional threat hunting, risk hunting helps organizations achieve the highest level of maturity. The real-world impacts of risk hunting are even more advantageous than they may seem on the surface. That said, it takes a whole new way of thinking about cybersecurity, and that doesn't come without some planning and preparation. It's important to explore the reality of risk hunting — what it takes to make it work and why that effort is more than worthwhile.

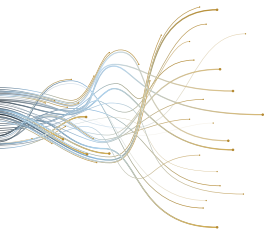
THE CYBER RISK MATURITY MATRIX





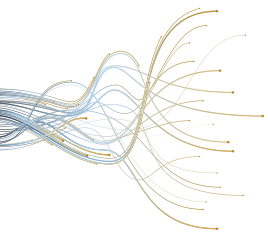
BLISSFUL IGNORANCE

Vague understanding of the scope of threats and vulnerabilities; undocumented, inconsistent, ad-hoc processes; weak or missing tools; insufficient staffing; inability to fully understand the potential for attacks and consequential business damage.



EARLY MATURITY & STRUCTURE

Threat/vulnerability metrics (e.g., time-to-detection and resolution), but no clear view of organizational impact; starts to focus on security standards and risk management, but requires time-consuming, event-focused analysis across data silos.



BUSINESS RISK & CONTEXT

Clear understanding of risks based on real attack paths, context of vulnerabilities, and potential business impacts; metrics tightly aligned with business operations; real-time view of risks at strategic, tactical, and technical levels; continuous re-prioritization of risks to guide patches; efficient threat hunting based on real-time attack-path mapping to and from targets.

BENEFITS OF RISK HUNTING

MINIMIZE CYBER RISKS

From lawsuits to compliance violations to loss of business continuity, cyber risk takes many forms that can be catastrophic. The holistic approach of risk hunting gives companies, for the first time, the means to manage and lower that risk in a meaningful way.

PREPARE AND ACCELERATE DIGITAL TRANSFORMATION

As IT increasingly drives everything businesses do, it must think differently about cyber risk. Tomorrow's IT is too big (and too important) to secure reactively. A proactive approach based on risk hunting helps companies prepare for — and even accelerate — their digital transformation efforts. Risk hunting turns cybersecurity into a competitive advantage.

LOWER THE COST OF CYBERSECURITY

Relying on risk hunting to proactively prevent attacks alleviates the burden on resources (time, staff, budget, etc.) centered on things like detection and resolution.

BOLSTER OTHER DIGITAL DEFENSES

Shutting down attack pathways, particularly the most vulnerable, takes the pressure off defenses that catch attacks further downstream. They have less to look for and, therefore, a better chance of catching and stopping whatever they encounter.

SUPPORT LEAN SECURITY TEAMS

Very few security teams have all the people, skills, and tools they need. Risk hunting makes up for those gaps by shutting attacks down early and automatically. That means fewer alerts for the security team and more time to spend on higher-value activities.

CHANGE YOUR MINDSET

THINK PROACTIVELY

The switch from reactive to proactive cybersecurity rewrites the playbook in a fundamental way. Adapting to an entirely new way of thinking poses challenges for individuals, teams, and whole institutions, but with the right partner to help guide and implement, change can be easily achieved.

LEARN NEW TOOLS AND TECHNIQUES

Making risk hunting work requires you to select tools and techniques, then implement, master, and operationalize them. That can be a big effort when the path is uncharted internally, which is why it's important to seek out guidance and follow proven practices. Better to lean on experience than try to experiment.

ACQUIRE ADEQUATE RESOURCES

Each phase of risk hunting — finding, ranking, and fixing attack pathways — is a major undertaking. Make sure there are adequate resources in place, whether on the security team or through a services provider, so that risk hunting is fully resourced from day one.

TAKE EARLY ACTION

Risking hunting can uncover a surprising (and growing) number of open attack pathways. But that information is only valuable if the security team shuts those pathways down systematically. Focus, always, on turning risk hunting into meaningful reductions in cyber risk by acting early and addressing everything — starting with the biggest and most critical risks. A skilled partner will help companies achieve the desired resolution goals.

SUSTAIN THE EFFORT

Risk hunting should not be a "one and done" effort. Since there are always new attack pathways being created in evolving IT environments, there needs to be continuous monitoring of attack paths and necessary resolution. The security team will need to be equipped to continue risk hunting even as the staff, defenses, risks, and overall security climate undergo change. A trusted services partner can ensure ongoing management of the process.

MAXIMIZE THE BENEFITS OF RISK HUNTING

BY WORKING WITH A SECURITY SERVICES PROVIDER THAT'S AN EXPERT IN THIS SPACE.

HOW TO START RISK HUNTING

Reveald provides a full suite of cybersecurity offensive and defensive managed services, including risk hunting as a core part of exposure management, so you have 24/7 continuous monitoring of changes in your environment. We combine unique offensive expertise with technology that fully operationalizes exposure management and proactive defense with multiple technical tools to find and resolve your cyber risks quickly across the spectrum.

Threat hunting as a defensive approach will continue to have value in security programs — but it is mostly reactive, commencing after a cyber attack has begun. So threat hunting focuses on damage mitigation, after a threat has already penetrated the environment. Risk hunting, on the other hand, proactively considers context and organizational impact to seek out and prioritize technical and business risks. The goal of risk hunting is to mitigate potential damage before an attack occurs. The result is fewer overall downstream threats, alerts, and vulnerabilities which saves time and money while maximizing total risk reduction for the organization.

REVEALD PUTS RISK HUNTING TO WORK

Reveald Continuous Exposure Management puts risk hunting into action as a critical offensive approach to identifying and mitigating cyber threats. This unique solution allows organizations to garner deep insights into the technical and business risks of potential attack paths so they can prioritize critical areas and quickly resolve any exposure points.

Before ingesting and translating information already available from existing systems, Reveald proactively hunts for risk conditions, then prioritizes contextualized risks based on organizational impact so the conditions can be corrected before attacks occur. This provides relevant, real-time, outcomes-based risk information for all business stakeholders, including executive management.

Risk hunting with Reveald rescues security teams from the distraction and stress of data overload and delivers true risk reduction. Our services transform and stop exposure before exploitation can occur. How can risk hunting impact your organization? **Contact us for a strategic consultation.**

REVEALD

WHY RISK HUNTING WINS

	THREAT HUNTING	RISK HUNTING
PARTICIPANTS	Highly specialized security analysts	All interested stakeholder, including executives, security analysts, audit staff, and IT resources
OBJECTIVE	Looks for known attack patterns and isolates potential threats	Looks for adversary-friendly conditions that can negatively impact revenue, uptime, and business-critical processes
FOCUS OF ACTIVITY	Narrowly focuses on tactics, attack detection, mitigation, recovery	Before an attack, proactively identifies and prioritizes conditions that can negatively impact systems, with or without an active threat; during an attack, provides system state data (such as business context), as well as attack path data, to better understand impacts
APPROACH	Uses event-based tools and manual technologies that produce an often-overwhelming number of alerts the must be investigated	Uses a state-based solution that clearly identifies where the security team should focus its time and efforts to reduce risk
DRIVING FORCE	Policy and tools	Governance and business priorities
COVERAGE LEVELS	Tactical and technical	Strategic, tactical, and technical
EXECUTIVE REPORTING	Requires repeated abstraction (often manually across data silos) to translate technical issues into higher-level business risks	Presents data ready for executive review, with prioritized lists of true business risks and recommended actions to reduce risks
TECHNICAL STANDARD ALIGNMENT	Difficult to align with standards; outcomes depend on systems used and analysts' skills	Easy to align with standards; system factors in high-level controls, policies, and

OUR TEAM IS YOUR TEAM

Reveald provides cybersecurity as a full set of offensive and defensive managed services so you have 24/7 continuous monitoring of changes in your environment. We combine unique offensive expertise and proactive defense with multiple technical tools to find and resolve your cyber risks quickly.

CONTACT US