DATASHEET

Threat Hunting Services

Reduce blind spots and support efforts to counter advanced, evasive threats with custom queries

Binary Defense takes a human-driven, technology-assisted approach to detect patterns of threat actor behavior that leverages Threat Hunters' expertise and curiosity to proactively detect quiet attackers through custom hunting queries tuned for your unique environment using timely threat intelligence, malware reverse engineering, and insights from threat activity discovered in other environments. Our Threat Hunters are truly an extension of your team who take the time to learn your environment and provide detailed and actionable interactive guidance to improve your security visibility, enhance existing detection capabilities, decrease your response time, and drive resiliency. The same Threat Hunters are assigned to consistently interact with your security team, developing trusted relationships and enabling your team to ask questions and get detailed explanations of the threat intelligence and hunting queries that we've developed for you. When you need follow-up investigation, analysis, or even reverse engineering of suspected malware, our Threat Hunters are there as your partners in defense.

> "With Binary Defense Threat Hunting, we have skilled, experienced threat hunters watching and creating new detections for our environment at all times. We wouldn't be able to afford that level of talent at an Energy Company of our size. They feel like they are an extension of our team."
>
> -Senior Security Engineer, Energy Company

Strengthen Your Defenses with Threat Hunting

Improve Security Posture

- Find stealthy attacks that can't be found with AI tools or common security approaches
- Find misconfigurations and potential weaknesses to strengthen your overall cybersecurity defenses
- Create new detection rules based on threat hunting results
- Implement recommendations on your security

Expert Threat Hunters

- Expert analysts with advanced malware analysis and security investigation skills
- Use threat intelligence, intuition, and experience to discover anomalies and develop patterns of threat activity over time to identify hidden threats
- Provide detailed and actionable guidance on the next steps to respond to a threat for seamless integration with incident response
- 100% US-based Hunters with former law enforcement and IT security experience

Binary Defense Threat Hunting Models

Continuous Analytical Threat Hunting

- Included with MDR Core & MDR Plus
- Historical/retrospective queries and analysis based on Indicators of Compromise and static signatures
- Universal application across broad customer set
- Supported by automation and orchestration for efficiency
- Delivered in a shared/mutualized services model architecture, instrumentation, and controls to make your environment more resilient

Hypothesis-Based Threat Hunting

- Dedicated Service
- Adversarial research and modeling
- Hunts customized to client enterprise and business
- Proactive validation across client environments
- Malware reverse engineering
- Adds context from vulnerability/exploit research
- Feedback loop into detection engineering
- Dedicated human analysis enforcement and IT security experience

1. Research emerging attacker techniques and tools
2. Evaluate current security platforms and event logs
3. Find misconfigurations, network anomalies and gaps in coverage
4. Notify clients where gaps exist to strengthen posture
5. Write new detections and add to security configurations
6. Test new attacker techniques and detection methods in a laboratory environment
7. Reverse engineer malware to learn attackers' methods
8. Repeat, repeat, repeat

Binary Defense is a trusted leader in Managed Detection and Response (MDR), helping organizations across industries stay ahead of modern cyber threats. Our team of SOC analysts, threat hunters, detection engineers, and researchers works around the clock to deliver outcomes that matter: earlier threat detection, faster response, and stronger long-term security.

We take an attacker's mindset to defense, combining deep expertise with proactive tradecraft to protect what matters most.

Learn more at binarydefense.com, explore our blog for the latest insights, or follow us on LinkedIn.

600 Alpha Parkway, Stow OH 44224
sales@binarydefense.com

BINARY DEFENSE