DRP RFP Questionnaire

	Vendor A	Vendor B	Vendor C
1. Operational Excellence and Speed			
What is your average Time-to-Takedown (TTT) across different threat types?			
What percentage of takedowns are executed through direct API or technical integrations versus manual email reporting?			
What established partnerships or trust-based relationships do you leverage with hosting providers and registrars to accelerate remediation?			
What is your typical time-to-value (TTV) from onboarding to the first verified threat takedown?			
What percentage of takedowns are completed without any customer involvement or escalation?			
How do you handle takedown failures or unresponsive providers, and what are your escalation paths?			
Do you provide real-time or batched notification of threats, and what is the typical alert latency?			
What is your fastest and slowest recorded takedown time in the past 12 months, and why?			
Additional notes			
2. Technical Depth and Intelligence			
What percentage of your detections originate from your own collection infrastructure versus third-party feeds?			
Does your platform use machine learning or AI to prioritize threats, and how is this validated?			
Do you cover social media impersonation and fraudulent mobile apps in addition to phishing domains?			
How do you detect and respond to credential leaks and hack-and-leak campaigns?			
Can you monitor for threats specifically targeting executives, employees, or other VIPs?			
How does your platform bypass cloaking or bot-detection techniques?			
Is your threat intelligence primarily collected through your own infrastructure or aggregated from third-party feeds?			
Can you identify attacker infrastructure patterns or campaigns across multiple domains and platforms, not just individual threats?			
Additional notes			

	Vendor A	Vendor B	Vendor C
3. Integration and Ecosystem			
How does your platform integrate with existing SIEM and SOAR platforms such as Splunk or Microsoft Sentinel?			
Do you provide a well-documented API that allows us to automate internal workflows based on your findings?			
What is your verified false-positive rate, and what percentage of alerts are immediately actionable?			
Can your intelligence feeds be used to trigger automated blocking actions within firewalls, email gateways, or web filters?			
What rate limits, authentication models, and uptime guarantees apply to your API?			
Do you support bidirectional integrations, allowing our systems to trigger actions or enrichment queries within your platform?			
Do you provide prebuilt playbooks or automation templates for common SOC workflows (e.g., blocking domains, enriching incidents)?			
Additional notes			
4. Trust, Security, and Compliance			
Are you compliant with GDPR, SOC 2, and other relevant regional data protection regulations?			
Do you perform regular third-party penetration testing on your platform, and can you share a summary of findings?			
Can your reports provide a detailed, time-stamped audit trail suitable for regulatory or legal review?			
Where is customer data hosted, and what controls are in place to protect sensitive brand and threat intelligence data?			
Does your pricing model scale predictably with our digital footprint, or are there per-incident fees that could increase costs during an active attack?			
What is your data retention policy for collected threat intelligence and customer-provided information?			
What controls are in place to restrict and audit internal employee access to customer data and investigations?			
Additional notes			