DATASHEET

Infoblox Domain Mitigation Services

Stop Internet fraud and cyberincidents impacting your company to get your business back on track fast

The Infoblox Mitigation Services team focuses on combating malicious actors and Internet fraud. We apply Infoblox's proprietary blend of investigative skills, automated techniques and industry relationships to resolve issues, including data theft, site spoofing, and other cyberincidents swiftly and with discretion.

INFOBLOX MITIGATION SERVICES

Infoblox Mitigation Services is a comprehensive Internet fraud solution for organizations victimized by malicious cybercriminals. Mitigation Services draws on Infoblox's deep trust-based relationships and our unique position in the global IT environment to help threatened companies respond to limit financial and brand exposure.

The COVID pandemic brought about an enormous increase in phishing incidents and website spoofing, a simple but effective means of stealing credentials, committing fraud and distributing malware. In addition, with more and more organizations adopting cloud infrastructure, cybercriminals are increasingly aiming their attacks at privileged access and secret management systems. In fact, Forrester Research estimates that 80 percent of security breaches now involve privileged access abuse.

Infoblox Mitigation Services are specifically structured to address these types of attacks (as referenced below), stop them as quickly as possible, and enable targeted entities to get back to business as usual. Our Mitigation Services include validation services to confirm an incident has in fact occurred; mitigation through coordination with major ISPs and regulators; and monitoring with reporting to better understand the threatscape and to strengthen your security.

FEATURES AND BENEFITS

Validation: Determining whether suspicious activity is really malicious is the first step in the mitigation process. Our validation team offers unique proprietary human-driven review of potential Internet fraud with a detailed summary of our in-depth review. During regular business hours, our initial response times are usually five minutes or less upon receipt of a potential Internet fraud incident. Once our review is underway, average removal time for domestic Internet fraud is roughly 24 hours or less.

Mitigation: Mitigation provides a continuous removal effort applied to each case, with multiple escalations for cases that cannot be resolved within 24 hours. In other words, once Infoblox confirms Internet fraud or a cyberincident and initiates mitigation, we will continue our efforts until the issue is resolved. As one of the foremost providers of core DNS technology and equipment to the global ISP community, Infoblox is uniquely positioned to leverage established trust-based relationships to ensure your case is prioritized in abuse queues. We also can provide registered trademark enforcement to secure brand reputation.enforcement to secure brand reputation.

GET YOUR BUSINESS BACK ON TRACK WITH INFOBLOX MITIGATION SERVICES

Threat	Description	Benefit
Phishing sites	Criminal websites that attempt to steal user credentials by constructing hoax websites with URLs very similar to the actual web address	Infoblox will work with the affected host to remove content.
Malicious name server	A server that provides Authoritative Domain Name Services only for malicious domain names	Infoblox will work with service providers to remove the criminally controlled infrastructure.
Stolen credentials or other content	Stolen corporate proprietary information (e.g., access credentials, personally identifiable information, credit card data), usually found hosted in a forum or a fraudulent host account	Infoblox will work with the affected host to remove the stolen content.
Malware file hosting location	Malware existing on a publicly available site	Infoblox will review and confirm the existence of potential malware at the reported location and will work to get the malicious files removed from the host.
Malware command and control (C2)	A host location identified as a C2 server fo malware campaigns	Infoblox will collaboratively review the threat and, once confirmed, work with the host to remove it.

FEATURES AND BENEFITS

Monitoring and Reporting:
If Infoblox determines, following the validation step, that the suspicious activity does not pose a threat, Infoblox will continue to monitor the reported web content for potential malicious changes. We also monitor the mitigated threats that we identified to address potential reactivation, which Infoblox will remove at no additional cost to clients. Mitigation Services provided by Infoblox will remain in effect for up to 30 days.

In addition to Infoblox's deep ties to the ISP and communication service provider community, the Mitigation Services team has also worked closely with global regulatory agencies for many years. If criminal activity is validated, the Mitigation Services team is ready to help clients notify local law enforcement and other government agencies when providers fail to address fraud activity.

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com