SOLUTION NOTE

VISIBILITY, AUTOMATION AND CONTROL WITH BLOXONE® THREAT DEFENSE TO COMPLY WITH TSA CYBERSECURITY DIRECTIVES NOW AND IN THE FUTURE

OVERVIEW

New cybersecurity directives from the Transportation Security Administration (TSA) have been issued to help prevent any future attacks on our critical energy infrastructure.

Organizations were given 30 days to assess and remediate any vulnerabilities while also establishing reporting resources available 24x7 to the TSA.

Organizations need solutions that give them visibility, automation and control to meet these new assessment, remediation and reporting requirements. Operating at the DNS level, Infoblox BloxOne Threat Defense monitors activity to see threats that other solutions do not and stop attacks earlier in the threat cycle. Through pervasive automation and ecosystem integration, it drives efficiencies in SecOps and uplifts the effectiveness of the existing security stack while enabling reporting to meet TSA requirements. It secures digital and work-from-anywhere efforts and lowers the total cost for cybersecurity.

CYBERSECURITY DIRECTIVES PUBLISHED TO PROTECT CRITICAL INFRASTRUCTURE

2021 ushered in a new wave of directives from the Transportation Security Administration (TSA). Aimed at the Gas and Oil industry but relevant for Energy providers as well, these regulations have been structured in a way to help prevent future compromise of our infrastructure like the Colonial Pipeline breach in May. While meeting these requirements is critical right now, organizations that strengthen their security posture may find themselves already compliant with future TSA directives when published.

The 2021 TSA Security Directive requires three critical actions:

1. Organizations must report cybersecurity incidents to the Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA). Reports must be made as soon as possible but no later than 12 hours after a cybersecurity incident is identified. Examples of incidents they must report include:

   a. Unauthorized access of an Information or Operational Technology system

   b. Discovery of malicious software on an Information or Operational Technology (OT) system

   c. Activity resulting in a denial of service to any Information or Operational Technology system

   d. A physical attack against the organization's network infrastructure, such as deliberate damage to communications lines, and

   e. Any other cybersecurity incident that results in operational disruption to the organization's Information or Operational Technology systems, etc.

2. Organizations must designate a Cybersecurity Coordinator who is required to be available to TSA and CISA to coordinate cybersecurity practices and address any incidents that arise.
    a. There must be a primary and an alternate cybersecurity coordinator with the names, titles, and contact information provided to the TSA.
    b. As the primary contact for cyber-related intelligence information, activities and communications to the TSA and CISA, they must be available 24 hours a day, seven days a week.
3. Organizations must review their current activities against TSA recommendations to assess cyber risks, identify any gaps, develop remediation measures, and report the results to TSA and CISA. Within 30 days of the original directive, organizations had to perform their security assessment and report their findings using the TSA designated form.

Further specific detail on the TSA Directives can be found here including a comprehensive set of definitions.

MEET INCIDENT REPORTING REQUIREMENTS

Meeting TSA guidelines for incident reporting requires **visibility** to your entire network from centralized locations through to branch or remote locations and remote workers. BloxOne Threat Defense delivers crucial visibility as it knows what to look for and can easily identify malicious traffic. Fueled with threat intelligence from Dossier, a capability of BloxOne Threat Defense, your organization will speed incident identification, investigation and remediation. Threat Insight, another capability in BloxOne Threat Defense, uses machine learning and AI to easily detect DGAs, DNSMessenger, tunnelling and other malicious activity. In summary, BloxOne Threat Defense helps detect and protect your organization from exploits while supporting critical reporting requirements.

BloxOne Threat Defense also integrates with your SIEM to help you report incidents in the format TSA requires, leveraging your existing security infrastructure. And, with DNS being the source of truth for network services, accessing the specifics you need to report on becomes that much easier with BloxOne Threat Defense.

TOOLS A 24X7 SECURITY COORDINATOR NEEDS

Security automation with BloxOne Threat Defense helps speed investigation and remediation activities, making Security Operations more effective and productive. It enables third-party security tools to work in unison to better remediate threats through extensive out-of-the-box and flexible REST API integration and automation options.

Comprehensive visibility and automation with BoxOne Threat Defense is an essential tool for 24x7 pervasive security.

CAPABILITIES TO HELP ORGANIZATIONS ASSESS AND STRENGTHEN THEIR SECURITY POSTURE

Organizations must perform a vulnerability assessment to identify any gaps within 30 days, then develop and implement appropriate remediation measures. BloxOne Threat Defense can help. It operates at the DNS level to see threat activity that other solutions do not and stops attacks earlier in the threat lifecycle. Through pervasive automation, threat intelligence sharing and ecosystem integration, it drives efficiencies in SecOps, uplifts the effectiveness of the existing security stack, secures digital and work-from-anywhere efforts and lowers the total cost for cybersecurity.

As companies are becoming more virtual, it's critical to secure the remote (and sometimes mobile) workforce. BloxOne Threat Defense will help organizations defend the work-from-anywhere organization. It also helps to extend resilient and accurate enterprise security to users and devices regardless of location, while maintaining centralized visibility and policy control.

Professional Services from Infoblox and from our highly qualified partners can help you assess vulnerabilities, making recommendations to strengthen your security posture with BloxOne Threat Defense and our ecosystem partners.

PERVASIVE VISIBILITY AND CONTROL FROM ANYWHERE

The unique hybrid security of BloxOne Threat Defense uses the power of the cloud to detect a broad range of threats while tightly integrating with your on-premises ecosystem. It also provides resiliency and redundancy not available in cloud-only solutions. Through a common console, administrators, even if remote, can centrally and automatically secure IoT and other devices, apps, virtual machines and switch ports wherever they reside. And, organizations can cut threat investigation time and support more effective incident response with fast access to relevant threat intelligence and valuable context in a unified UI.

CONCLUSION

Strengthen your security posture while meeting the new TSA Security Guidelines with Infoblox BloxOne Threat Defense. With better visibility, automation and control, organizations can more effectively protect their users and networks from cybersecurity threats, make SecOps more efficient, and uplift the entire security stack, while also meeting new mandates from TSA. In fact, one Infoblox customer reported that the new mandate had little impact on their organizations as their security portfolio and best practices, including Infoblox BloxOne Threat Defense, already made them compliant. Implementing this solution will also lower the total cost of your enterprise threat defense by reducing the burden on stretched perimeter defenses. In addition, this solution enables security teams to get more value out of their other security solutions through real-time, two-way sharing of threat intelligence, security event information and through automation that lowers the costs associated with manual effort and potential human error.

MAPPING TSA DIRECTIVE REQUIREMENTS TO INFOBLOX

Requirement	Infolox Relevancy	Benefits
Report confirmed and potential incidents to CISA	• Exec, security reports on Cloud Services Portal • Includes • DNS query logging and reporting • DHCP fingerprint, IPAM metadata	• Easy visibility and analysis • User and device context • Extent of breach
Identify gaps and remediation measures	• Architecture review using Infoblox PS • DEX tool to validate DNS security gap • Monitor threat insight once installed	
Implement specific mitigation measures to IT and OT systems	• Automated discovery using Network Insight • Malware detection/blocking using RPZ • Data exfil blocking using analytics • SecOps ecosystem integration • Threat intel operationalization and threat investigation	• Automatically discover IT/OT assets/single source of truth • DNS as a first line of defense against malware/ransomware/data exfil • Protect sensitive data • Continuous security monitoring • Quickly investigate domain reputation
Develop a cybersecurity response plan	If an event occurs, Infoblox integration with SOAR helps quickly isolate systems	

DNS AND OTHER SPECIFIC CAPABILITIES IN THE DIRECTIVES THAT INFOBLOX CAN HELP ADDRESS

Requirement	Relevant Infolox Features
Client (Source) DNS Query Logging and reporting: Implement software analytics that allow Owners/Operators to rapidly determine which host sourced each DNS query.	• Security reports on Cloud Services Portal • Client(source) DNS query logging and reporting • DHCP fingerprint, IPAM metadata
Rare Domains: Maintain a current list of domains that are frequently visited or searched for by legitimate users within their systems that are not already included in commercially available top one million domain lists. (helps quickly identify rarely queried domains)	• Custom report in Infoblox Reporting and Analytics
Domain reputation: Develop and/or update policies and procedures requiring investigation of the reputation of the domains that are only rarely queried for and/or accessed by legitimate users within the organization to determine if the communication with these domains carries an inappropriate level of risk to the organization.	• Dossier threat indicator research tool to investigate domain reputation
Domain blocking	• Block resolution to malicious domains using RPZ
Network Segmentation to ensure OT system can operate at necessary capacity	• Create internal and external DNS views • Create specific DNS filters to help support segmentation
Zero Trust	• Monitor and/or block connections from known malicious C&C servers to IP addresses and ports for which external connections are not expected

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

Version: 20230918v1