BLUVECTOR®

NIST 800-53 COMPLIANCE

Introduction

BluVector created this document for organizations that follow, or are looking to follow, the guidelines in NIST 800-53 Rev 4. The tables below provide details on how BluVector can either be the solution to a specific compliance requirement or can act as part of a system to meet the guidance. The descriptions are written so that they can be included in the compliance process as descriptions of the controls.

Access Control (AC)

800-53 Section	Section Description	How BluVector Meets that Section
Information Flow Enhancement **AC-4**	This requirement specifically calls out the need for boundary protection devices which monitor network traffic and can detect and contain malicious activity.	BluVector is a next generation Network Intrusion Detection System. The four main components of BluVector are: - A patented, supervised machine learning engine (U.S. Patent 9,665,713), trained for 8 years by entities in intelligence, defense and commercial sectors to accurately identify zero-day and polymorphic malware. - A speculative execution engine designed to find fileless malware traversing the network, in real-time. - A targeted logger that delivers context and visibility to threat security teams and their investigations by pre-correlating and highlighting log entries associated with events prioritized for analysis. - An intelligent decision support system delivering workflow automation to contain threats early in the kill chain.
Access Control for Remote Devices **AC-19**	Section B of AC-19 describes the requirements for securing the network communications when mobile devices are connected to corporate networks and cloud resources.	BluVector can monitor network activity of mobile devices connected to both networks and cloud resources.
Use of External Information Systems **AC-20**	This section refers to the methods by which organizations allow bring-your-own-device (BYOD) or non-organizational devices to be connected to the network.	Per the supplemental guidance on this requirement, the use of specific security tools to ensure the safety of that system on the network should be considered. BluVector can detect already compromised systems through C2 traffic coming from that information system or via attempts at lateral movement.

AUDIT AND ACCOUNTABILITY (AU)

800-53 Section	Section Description	How BluVector Meets that Section
Audit and Accountability Policy and Procedures **AU-1**	This section includes the establishment of policy and procedures for the effective implementation of security controls in the AU family.	Through the analysis of all network traffic and creation of Bro network logs of that activity, BluVector acts as a security control for appropriate audit by allowing review of all network activity and alerting to malicious activity.
Audit Events **AU-2**	Organizations must identify and audit events which are significant and relevant to the security of information systems.	BluVector captures all network activity and provides a method by which all network activity can be audited. BluVector can be configured to detect custom events through the use of Suricata or Yara signatures. This follows the supplemental guidance that auditable events can be detected at different points including at the packet level as information traverses the network. BluVector enables central audit of the events in a unified location through SIEM integration.
Content of Audit Records **AU-3**	Information system must provide information to establish what type of event occurred and the identity of systems or individuals involved in the event.	The Bro logs created by BluVector include the information tags defined by AU-3. These tags are time stamp, source and destination addresses, process identifiers, event descriptions, success/fail indications, and filenames involved.
Audit Review, Analysis and Reporting **AU-6**	The organization reviews and analyzes system audit records for indications of inappropriate or unusual activity.	BluVector enables central review of all audit records including all network activity and specifically analyzed and identified malicious activity.
Audit Reduction and Report Generation **AU-7**	Audit Reduction is a process that manipulates collected audit information and organizes that information into a more meaningful summary format for analysts.	With BluVector's intelligent decision support engines, all related network activity logs, event data, extracted files and correlated intelligence are packaged together to provide a consolidated view of the event by the analyst.
Time Stamps **AU-8**	All audit events are given a time stamp.	All events from BluVector are affixed with the time that the event and related events occurred.
Audit Record Retention **AU-11**	The organization can define a duration for which it keeps its audit records.	BluVector can be configured to keep logs related to malicious events. Audit records are created to track system activities including malicious events. These records are stored in the system for an extended period of time. They can also be exported to external storage solutions for longer durations.

SECURITY ASSESSMENT AND AUTHORIZATION (CA)

800-53 Section	Section Description	How BluVector Meets that Section
Security Assessments **CA-2**	The organization builds and executes a security assessment plan.	BluVector provides continuous monitoring of all network activity to provide alerts on any malicious activity when it occurs, satisfying this requirement based on the supplemental guidance.
System Interconnections **CA-3**	Refers to the establishment of connections between information systems.	This requirement explicitly calls for network-based boundary defenses to mediate communications between information systems and external connections. BluVector provides these defenses.
Continuous Monitoring **CA-7**	The organization develops an infrastructure that provides continuous monitoring of the network including correlation and analysis of security-related information generated via monitoring.	BluVector performs continuous detection on the network, looking for malicious activity. Through machine learning and speculative execution, BluVector detects anomalous behavior, and correlates that behavior with threat intelligence. Threat Intel can be imported via direct integrations or through STIX/TAXII.
Internal System Connections **CA-9**	Organizations can define the proper way to connect components to the network by defining the right levels of security to apply to each device and connection.	BluVector sees the network traffic of all devices on the network and allows review of that activity to validate proper use of the network. Additionally, inclusion of network security is part of the standard organizational baseline security control set.

INCIDENT RESPONSE (IR)

800-53 Section	Section Description	How BluVector Meets that Section
Incident Response Policy and Procedures **IR-1**	Creation of incident response policies and procedures.	BluVector's intelligent decision support system comes configured to automatically classify events as good, benign, or bad based on a hunt score (equivalent to a combination of severity and confidence). These classifications can be modified with custom rules and intelligence imported by the analyst. Automated policies for incident response can be triggered based on a given event type and hunt score. For example, when a malicious threat is detected, BluVector can be configured to automatically submit the file to a sandbox for additional analysis, send an alert or block command to other information security systems or send all pertinent intelligence about the event to a SIEM.
Incident Handling **IR-4(3)**	Implementation of an incident handling capability for security incidents that include preparation, detection and analysis, containment, eradication and recovery.	BluVector plays a central role in fulfilling the requirements for incident handling. BluVector's machine learning detection can determine whether files including PDF files, Office files and PowerShell, are benign or malicious. If a threat is identified, it triggers BluVector's analytics framework to create context around the threat to drastically expedite an analyst's decision-making process. BluVector then provides an extensive workflow automation and API framework to simplify the process of containment. Events from BluVector can also be sent to all leading SIEMs in order to facilitate an IR workflow centered around the SIEM.
Incident Monitoring **IR-5**	The organization tracks and documents information system security incidents.	BluVector provides a full view of all events, with each event having all the information required to start a response. This includes event details, threat intelligence, and Bro logs for all related network activity before and after the event.
Incident Reporting **IR-6**	The organization is responsible for reporting when a suspected security event occurs	BluVector can be configured to trigger alerts when malicious or suspicious events are detected via: - SMTP - Alert to SIEM - Alert to another information security product.

SYSTEMS AND COMMUNICATIONS PROTECTION (SC)

800-53 Section	Section Description	How BluVector Meets that Section
Denial of Service Protection **SC-5**	Subsection 3 of this requirement calls for the detection of indicators of denial of service attacks against the information system.	BluVector includes advanced indicators of malicious activity including more than 40 different categories of network behaviors, malware command and control (C2), DoS attacks, botnets, informational events, exploits, vulnerabilities, abnormal SCADA network activity and exploit kit activity.
Boundary Protection **SC-7**	The information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system.	Explicitly called out in this section is the implementation of network-based malicious code protection devices. BluVector detects both file-based and fileless malware at the boundary, in real-time.
Mobile Code **SC-18**	Defines acceptable and unacceptable mobile code including JavaScript, VBScript and PDF.	Fileless malware attacks often disguise themselves as valid mobile code. BluVector analyzes mobile code through its highly advanced speculative code execution.