Implementation of Security Operations Center in BRPL			
Page No	**Clause No**	**NIT Clause**	**Revised NIT Clause**
47	Scope and Technical Specifications	1.14. The Platform must include log management, NG SIEM, Host Forensics, UEBA, NDR,File Integrity Monitoring, Security Analytics, Big Data Analytics, Security Automation and Orchestration engine (includes but not limited to Incident Management, Incident Response), Advanced Correlation within the same platform with no additional 3rd party solution)	The proposed solution should integrate with FIM (File Integrity Monitoring) and must alert on anomalous user activity related to important files. Reduce false positives by corroborating with other data
48	Scope and Technical Specifications	1.18 The proposed solution built-in FIM (File Integrity Monitoring) must alert on anomalous user activity related to important files. Reduce false positives by corroborating with other data	The proposed solution should integrate with FIM (File Integrity Monitoring) and must alert on anomalous user activity related to important files. Reduce false positives by corroborating with other data
73	Technical Specification	116) Customized Reports: The proposed solution must provide the ability for customers to create their own reports with report templates, reporting wizard as well as an advanced interface for power users to create their own custom report queries.	Customized Reports: The proposed solution must provide the ability for customers to create their own reports with report templates and reporting wizard
90	Network Detection and Response (NDR) Specifications:	3.2) Network Detection and Response (NDR) solutions leverage the inherent flow technologies present in network devices. These tools should possess the capability to capture packets from ongoing streams of real-time network traffic and transform this raw data into actionable analytics, represented through numerical data, charts, and tables. This analytical output serves to quantify precisely how the network is utilized, by whom, and for what purposes.	Network Detection and Response (NDR) solutions leverage the inherent packet/ flow technologies present in network devices. These tools should possess the capability to capture packets from ongoing streams of real-time network traffic and transform this raw data into actionable analytics, represented through numerical data, charts, and tables. This analytical output serves to quantify precisely how the network is utilized, by whom, and for what purposes.
90	Network Detection and Response (NDR) Specifications:	3.4) NDR solution should be able to use the existing network environment as a sensor grid to analyze traffic flow across the across the existing network and security solutions in a nondisruptive manner	NDR solution should be able to use the existing network environment to analyze traffic across the across the existing network and security solutions in a nondisruptive manner.
90	Network Detection and Response (NDR) Specifications:	3.11) The solution should be able to combine the flow records coming from different network devices like routers, switches, firewalls that are associated with a single conversation	The solution should be able to combine the packet / flow records coming from different network devices like routers, switches, firewalls that are associated with a single conversation
90	Network Detection and Response (NDR) Specifications:	3.12) The solution must be able to stitch flows into conversations even when the traffic is NATed by the firewall; clearly showing the original and translated IP address.	The solution must be able to stitch packets/ flows into conversations even when the traffic is NATed by the firewall; clearly showing the original and translated IP address.
94	Scope and Technical Specification - NDR	5.4) The solution should have capability to instruct network security devices such as firewalls to block certain types of traffic, quarantine the host, etc.	Clause 5.4 is deleted . Added as Clause 53.1 in Automation and Response-Page - 82 (SOAR Specification)
95	Scope and Technical Specification - NDR	7.4) The solution should support the capability to alert the admin and provide mitigation action like quarantine or block the endpoint or custom scripts like ACL push or block the further spread of the malware/worm.	Clause 7.4 is Deleted . Added as Clause 53.2 in Automation and Response-Page - 82 (SOAR Specification)
89	UEBA (User Entity and Behavior Analytics) Specification:	52) Use of supervised machine learning algorithms	Use of supervised/Unsuprevised machine learning algorithms

90	Volume III, Technical Specifications. Network Detection & Response	3.2) Network Detection and Response (NDR) solutions leverage the inherent flow technologies present in network devices. These tools should possess the capability to capture packets from ongoing streams of real-time network traffic and transform this raw data into actionable analytics, represented through numerical data, charts, and tables. This analytical output serves to quantify precisely how the network is utilized, by whom, and for what purposes.	Network Detection and Response (NDR) solutions leverage the inherent packet/ flow technologies present in network devices. These tools should possess the capability to capture packets from ongoing streams of real-time network traffic and transform this raw data into actionable analytics, represented through numerical data, charts, and tables. This analytical output serves to quantify precisely how the network is utilized, by whom, and for what purposes.
91	Volume III, Technical Specifications. Network Detection & Response 3.12	3.12) The solution must be able to stitch flows into conversations even when the traffic is NATed by the firewall; clearly showing the original and translated IP address.	The solution must be able to stitch packets/ flows into conversations even when the traffic is NATed by the firewall; clearly showing the original and translated IP address.
86	UEBA (User Entity and Behavior Analytics) Specification: Pt 6	The agents of the solution should not be open sources, the agents should be from the same OEM and should not contain any malicious code. OEM to provide declaration for the same.	The agents of the solution should not be open sources, the agents should be from the same OEM and should not contain any malicious code. OEM to provide declaration for the same. OEM can also suggest agenless approach/solution.
87	UEBA (User Entity and Behavior Analytics) Specification: Pt 15	Use of supervised machine / deep learning algorithms	Use of supervised machine / deep learning algorithms or other diferent methodology to detect anomolies
87	UEBA (User Entity and Behavior Analytics) Specification: Pt 19	The solution should be an endpoint based UEBA, where the UEBA will take inputs from endpoint protection devices to further detect anomalies	The solution should be an endpoint based UEBA, where the UEBA will take inputs from endpoint protection devices to further detect anomalies. OEM can also suggest agenless approach/solution.
87	UEBA (User Entity and Behavior Analytics) Specification: Pt 24	The proposed solution must have built in File Integrity Monitoring, Process activity monitoring, Registry Integrity Monitoring with no additional cost	The proposed solution should integrate with FIM (File Integrity Monitoring) and must alert on anomalous user activity related to important files. Reduce false positives by corroborating with other data
89	UEBA (User Entity and Behavior Analytics) Specification: Pt 52	Use of supervised machine learning algorithms	Use of supervised/Unsuprevised machine learning algorithms
47	SCOPE OF WORK: Pt. 1.14	The Platform must include log management, NG SIEM, Host Forensics, UEBA, NDR, File Integrity Monitoring, Security Analytics, Big Data Analytics, Security Automation and Orchestration engine (includes but not limited to Incident Management, Incident Response), Advanced Correlation within the same platform with no additional 3rd party solution)	The Platform must include log management, NG SIEM, UEBA, NDR, Security Analytics, Big Data Analytics, Security Automation and Orchestration engine (includes but not limited to Incident Management, Incident Response), Advanced Correlation within the same platform with no additional 3rd party solution)
48	SCOPE OF WORK: Pt. 1.18	The proposed solution built-in FIM (File Integrity Monitoring) must alert on anomalous user activity related to important files. Reduce false positives by corroborating with other data	The proposed solution should integrate with FIM (File Integrity Monitoring) and must alert on anomalous user activity related to important files. Reduce false positives by corroborating with other data
29	8.0 TERMS OF PAYMENT AND BILLING	8.1 Payment shall be made in milestone (MS) as per following: Part A - For Supply MS-1: 70% of contact value for of Pricing schedule shall be released subject to fulfillment of following pre-requisites: **(iii) Delivery and installation of required for hardware and licenses.**	8.1 Payment shall be made in milestone (MS) as per following: Part A - For Supply MS-1: 70% of contact value for of Pricing schedule shall be released subject to fulfillment of following pre-requisites: **(iii) Delivery of required hardware and licenses.**