1

Role

platform operator	SIEM	non-functional	Deployability in containers

Role

Infrastructure administrat	Log processing	non-functional	Containerizability
	Asset management	non-functional	Asset types
	System administration	non-functional	automated configuration
			operations monitoring

Role

Incident handler	SOAR	functional	categorization
	Incident recording and r	functional	incident recording

Role

DevSecOps	SOAR	functional	playbook
	CTI	functional	Enrichment data
	Vulnerability scanner	functional	database update
	system administration	functional	automation

Role

Service provider	SIEM	Non-functional	Multi-tenancy

Role

Platform operator	SIEM	Non-functional	Multi-tenancy

Role

Data Scientist	detection using ML	functional	Anomaly detection
			ML update
			Model evaluation

Role

ML specialist	detection using ML	non-functional	Detection accuracy
	EDR/XDR	non-functional	Modular models
			Multi-data collection

Role

ML engineer	detection using ML	non-functional	response speed
			computational scalability
			training pipeline

Role

Architect	Detection using ML	non-functional	model evaluation
			model management
	EDR/XDR	non-functional	support for multiple environments

Role

SOC team lead	data visualization	non-functional	configurable dashboards

Role

operator	data visualization	non-functional	single sign-on

Role

operations team	alerting	non-functional	multi-channel delivery
	optional extensions	non-functional	system recovery

Role

SOC lead	alerting	non-functional	alert customization

Role

SOC operator	alerting	functional	immediate alerts
		non-functional	real-time alerts
	EDR/XDR	functional	dashboard
	knowledge base	functional	search
	ticketing	functional	ticket creation

Role

SLA operator	alerting	non-functional	escalation rules

Role

SOC analyst	EDR/XDR	functional	threat detection
	CTI	functional	Visualization
	incident recording and r	functional	incident recording
	reporting	functional	content filtering
	optional extensions	non-functional	threat hunting mode

Role

forensic analyst	optional extensions	functional	forensic analysis
	EDR/XDR	non-functional	access to history
		functional	threat detection

Role

System integrator	SIEM	Functional	Collection of security data logs
			system integration
		Non-functional	OS compatibility
	Log processing	Functional	log collection
			extensions
		Non-functional	Multi-source collection
			Linking with SIEM
	SOAR		
		Functional	process orchestration
		Non-functional	automated scenarios
			API interface
			ecosystem integration
	Detection using ML		
		non-functional	Multi-source data
			Integration of ML outputs
	Data visualization	Functional	SIEM integration
		Non-functional	dynamic update
			Data linking
	Alerting		
		non-functional	linking with response
	EDR/XDR		
		Functional	Incident forwarding
		non-functional	
			flexible data collection
	CTI	Functional	Threat data collection
			SIEM integration
		Non-functional	Automated CTI collection
			Linking CTI with systems
			Standard CTI format
	Asset management	Functional	Asset database integration
			import/export
		Non-functional	Integration with monitoring
	Vulnerability scanner	non-functional	output integration
	Security data sources	Functional	Endpoint log collection
			log collection from security tools
		Non-functional	source extensibility
			support for log types
	Knowledge base		
		Non-functional	Linking to systems
	Ticketing	Non-Functional	Integration with response systems
	Incident recording and management		
		non-functional	Incident management integration

Role

End user	Data visualization	non-functional	language localization

role

team coordinator	ticketing	functional	ticket assignment

role

incident manager	ticketing	non-functional	ticket statuses

role

IT administrator	system administration	non-functional	system backup

role

operator	system administration	functional	administration interface

role

compliance officer CISO	optional extensions	non-functional	mapping to standards

Role

Security analyst	SIEM	Functional	Event correlation	Correlation of security events
			Threat detection	Real-time threat detection
			Dashboard	Clear visualizations and dashboards
		non-functional	Integration with tools	Integration with other tools (e.g. XDR, visualization tools)
			Event correlation	Analytical capabilities and data correlation (Data correlation)
			User interface	User interface and UX (GUI)
	Log processing			
		Functional	Filtering	Log normalization and filtering
			Search	Searching in collected logs
		non-functional	Log normalization	Support for log normalization
			Log search	Powerful searching and filtering of records
	SOAR			
		Functional	Automation	Automation of responses to security incidents
			Categorization	Incident categorization and triage
		non-functional	Playbook	Creating and editing playbooks
			Automated scenarios	Support for workflows and playbooks (automated response scenarios)
			Configurable playbooks	Flexibility in scenario configuration
			Incident categorization	Ability to categorize incidents and the rules for handling them
	Detection using ML			
		Functional	Anomaly detection	Detection of network and operational anomalies using ML
			Detection accuracy	Accuracy of anomaly detection (e.g. network, phishing, spam, malware)
		non-functional	Training pipeline	Data collection and preparation for model training (data pipeline)
			Model explainability	Ability to explain the result of an ML model (explainability)
	Data visualization			
		Functional	Dashboard	Creating interactive dashboards
			Template	Support for templates for different types of visualizations
			Correlation	Data correlation in visualizations
		non-functional	Graphical interface	Graphical user interface (GUI)
			Correlation visualizations	Correlation rules and their visualization
	Alerting			
		Functional	Automation	Generation of notifications about security events
			Rules	Defining rules for alerts
			Automatic alert completion	Notifications via e-mail and other channels
		non-functional	Real-time alerts	Support for real-time incident notifications
			Conditional rules	Support for conditional alert generation ("if-then" logic, correlation)
			Linking with response	Support for integration with ticketing and SOAR
	EDR/XDR			
		Functional	Monitoring	Monitoring of activities on endpoint devices
			Incident response	Incident response on endpoint devices
			Audit data collection	Collection and processing of audit data
		Non-functional	Threat detection	Detection and classification of malware, intrusions, suspicious behaviour
	CTI			
		Functional	IOC creation	Creation and updating of threat indicators
		non-functional	Threat visualization	Ability to visualize threats (e.g. MITRE ATT&CK)
			Classification	Automated CTI playbooks
	Asset management			Support for integration of playbooks for CTI processing
		Functional	IT asset records	Recording and management of all assets in the organization
			Classification	Differentiation of assets by type and criticality
		Non-functional	Asset types	Support for various asset types (hardware, software, cloud, containers, services)
	Vulnerability scanner			
		Functional	Vulnerability detection	Identification of vulnerabilities in the IT infrastructure
			Scan scheduling	Ability to schedule and repeat scans
			Vulnerability overview	Display of results and prioritization of vulnerabilities
			Reporting	Report export and notifications about findings
		non-functional	Scan scheduling	Support for both scheduled and ad hoc scanning
			Risk prioritization	Support for EPSS and CVSS scoring
	Security data sources			
		Functional	Endpoint log collection	Collection of logs and audit data from servers and endpoints
			Data collection from the infrastructu	Collection of network data from the infrastructure
			Data normalization	Normalization of collected data
		Non-functional	Normalized logs	Standardization and normalization of data formats
	Knowledge base	Functional	Knowledge base	Central knowledge repository for the SOC team
	Ticketing			
		non-functional	Ticket statuses	Ability to change ticket status and the processing workflow
			Integration with response systems	Integration with SOAR and SIEM systems
	Incident recording and management			
		Functional	Linking incidents with data	Linking incidents with tickets and logs
			Archiving	Retention of records for audit and forensic purposes
		non-functional	Detailed incident record	Ability to record complete incident details (time, source, impact, measures)
			Incident categorization	Ability to classify and categorize incidents (e.g. by type, severity, service)

Role

System administrator	SOAR	non-functional	Secure actions
	Data visualization	non-functional	single sign-on
	alerting	non-functional	multi-channel delivery
			encrypted alerts
	EDR/XDR	non-functional	support for multiple environments
	Asset management	non-functional	asset categorization
	Vulnerability scanner	non-functional	agentless scan
	Security data sources	non-functional	agent support
	Knowledge base	non-functional	knowledge permissions
	Ticketing	non-functional	ticket permissions
	Incident recording and r	non-functional	audit data
	Reporting	non-functional	controlled access to outputs
			Report export
	System administration	non-functional	role-based access

Role

Operator	data visualization	non-functional	dynamic update
			graphical interface
	alerting	non-functional	real-time alerts
	EDR/XDR	non-functional	automatic response
			EDR data visualization
	CTI	non-functional	Real-time enrichment
	asset management	non-functional	asset management UX
	vulnerability scanner	non-functional	performance range
	security data sources	non-functional	log validation
	knowledge base	non-functional	clear knowledge base
	ticketing	non-functional	ticket management
			e-mail alerts
	system administration	non-functional	administration interface

Role

SOC team	EDR/XDR	non-functional	linking with tickets

Role

IT support	EDR/XDR	non-functional	linking with tickets
	ticketing	non-functional	ticket management

Role

ML analyst	EDR/XDR	non-functional	Data export

Role

SOC specialist	optional extensions	functional	forensic analysis

Role

CTI analyst	CTI	functional	threat data collection
			CTI data normalization
			IOC creation
			visualization
			Creation of a response scenario
		on-functional	Scope of CTI layer
			automated CTI collection
			linking CTI with systems
			manual CTI validation
			real-time enrichment

Role

administrator	EDR/XDR	on-functional	Secure data
			CTI data security
	Asset management	non-functional	asset search
	vulnerability scanner	non-functional	test update
	security data sources	non-functional	support for log types
		non-functional	data archive
	system administration	functional	administration interface
		functional	system update

Role

IT technician	vulnerability scanner	non-functional	performance range

Role

IT infrastructure admin	asset management	non-functional	asset backup

Role

manager	SIEM	non-functional	OSS support
	Detection using ML	non-functional	model explainability
	data visualization	non-functional	visualization templates
	alerting	non-functional	alert audit
	Asset management	functional	classification
	vulnerability scanner	non-functional	open tool
	knowledge base	functional	knowledge base
		non-functional	record creation
	Ticketing	functional	ticket assignment
		on-functional	assignment of a resolver
	Reporting	functional	content filtering
		on-functional	measuring solution performance
	Optional extensions	functional	SLA monitoring and reporting
		non-functional	audit outputs

Role

analyst	Log processing	functional	Visualization
		non-functional	Visualization compatibility
	SOAR		
		non-functional	reverse response
	Detection using ML		
		Functional	incident prediction
	Data visualization	on-functional	dynamic update
			Configurable dashboards
			Visualization templates
	Alerting		
		Non-functional	Alert customization
	EDR/XDR	on-functional	multi-data collection
			automatic response
			EDR data visualization
	Asset management		
		on-functional	Integration with monitoring
			Asset search
	Vulnerability scanner		
		on-functional	test update
			GUI usability
	knowledge base	functional	record management
			search
		non-functional	Clear knowledge base
	Incident recording and management		
		Functional	Incident evaluation
			GUI usability
		on-functional	linking with evidence
			incident management integration
	Reporting		
		functional	Export
		on-functional	scheduled and manual outputs
			report export
			configurable outputs

Role

security investi	optional features	non-functional	forensic data visualization

Role

integrator	EDR/XDR	non-functional	Data export
	CTI	on-functional	automated CTI collection
			linking CTI with systems
	vulnerability scanner	non-functional	output integration

Role

Network specia	security data sources	non-functional	standard protocols

Role

quality controll	security data sources	non-functional	log validation

Role

customer	reporting	non-functional	visualized reports
	optional extensions	functional	SLA monitoring and reporting

Role

team leader	CTI	non-functional	threat visualization
	knowledge base	functional	access management
		non-functional	clear knowledge base
	ticketing	functional	ticket assignment
	incident recording and manager	non-functional	incident permissions
	reporting	non-functional	configurable outputs

Role

auditor	vulnerability scanner	on-functional	GUI usability
			compliance support
	security data sources	non-functional	log validation
	ticketing	non-functional	immutable history
	reporting	functional	controlled access to outputs
		non-functional	report archive
	optional extensions	non-functional	compliance check

Role

service administ	reporting	non-functional	automatic distribution

Role

Security manager	SIEM	Functional	Dashboard
			Reporting
		Non-functional	Regulatory compliance
	SOAR		
		Functional	Records
		Non-functional	activity audit
	Detection using ML		
		Functional	Incident prediction
	Data visualization		
		Functional	Dashboard
	Alerting		
		Functional	Sending notifications
		Non-functional	Escalation rules
	EDR/XDR		
		Functional	Dashboard
	CTI		
		Non-functional	Scope of CTI layers
	Asset management	Non-functional	Asset change audit
	Vulnerability scanner	Functional	Vulnerability overview
		Non-functional	Compliance support
	Ticketing		
		Functional	Notification
		Non-functional	Processing history
	Incident recording and management	Functional	Incident evaluation
		Non-functional	Incident export
	Reporting		
		Functional	Security report
			Automation
		Non-functional	Visualized reports
	System administration		
		Functional	System change audit
	Optional extensions	Functional	Compliance monitoring
		Non-functional	Compliance check

Role

Knowledge manager	knowledge base	Non-functional	change history

role

content editor	knowledge base	non-functional	record sorting

role

documentation admin	knowledge base	non-functional	knowledge export

Role

incident analyst	ticketing	functional	ticket creation	

Role

incident resolver	ticketing	functional	ticket status	
	ticketing	functional	notification	

role

SOC operator	incident recording and manage	non-functional	GUI for incidents

role

incident manager	incident recording and manage	non-functional	incident history

role			
incident investigator	incident recording and manage	non-functional	linking with evidence

Role

Administrator	SIEM	on-functional	asset management UX
			access control
			data management
			update and configuration
	Log processing	functional	visualization
		on-functional	log normalization
			log archiving
	Data visualization	functional	login
		non-functional	visualization backup
	Alerting	functional	rules
			sending notifications
	EDR/XDR	Functional	audit data collection
		non-functional	flexible data collection
	Asset management	Functional	IT asset records
			change tracking
			import/export
		on-functional	asset management UX
			protection of asset data
	Vulnerability scanner	functional	database update
			scan scheduling
			reporting
Reporting		functional	export
Security data sources		functional	endpoint log collection
knowledge base		functional	logging agents
system administration		functional	access control
		functional	system configuration
		functional	automation

Role

Solution architect	SIEM	Functional	Data processing
		Non-functional	system scaling
	Log processing		
		on-functional	Visualization compatibility
			log archiving

Role

Developer	SIEM	Functional	Extensions
		Non-functional	Integration with tools
	SOAR		
		Non-functional	API interface
	Detection using ML	Functional	ML libraries
		on-functional	Multi-source data
			Modular models
	Security data sources		Model management
		Functional	Source extensibility

Role

Auditor	SIEM	Functional	Dashboard
			Reporting
		on-functional	Regulatory compliance
			Data management
			Deployability in containers
	SOAR	Functional	Records
		Non-functional	Activity audit
	Asset management	Non-functional	protection of asset data
		Functional	Change tracking
	Incident recording and management	Non-functional	incident history
		Functional	Archiving
	Reporting		
		Functional	Security report
	Optional extensions		
		Functional	Compliance monitoring
	System administration	Non-functional	System change audit
	CTI	Non-functional	CTI data security
	Alerting	Non-functional	Alert audit
	knowledge base	Non-functional	change history
	Optional extensions	Non-functional	audit outputs

Role

Security architect	SIEM	Functional	Data security
		Non-functional	Data encryption
	SOAR		
		Non-functional	Secure actions
	Detection using ML		
		Functional	Model evaluation
	Data visualization		
		Functional	Login
	EDR/XDR		
		Non-functional	Secure data
	Sources of secure data		
		Non-functional	Secure collection
	Knowledge base		
		Functional	Access control
	Incident recording and manageme		
		Functional	Archiving
	System administration		
		Functional	Access management

Role

System architect	SIEM	on-functional	OSS support
			Deployability in containers
	Log processing		
		Functional	processing scaling
	SOAR		
		Non-functional	reverse response
	Detection using ML		
		Non-functional	response speed
	Vulnerability scanner		
		Functional	Agentless scanning
	System administration		
		Non-functional	Container deployment

Role

DevOps	SIEM		Extensions
		Functional	Deployment
		on-functional	Updates and configuration
			Deployability in containers
	Log processing		
		on-functional	processing scaling
			Containerizability
	Detection using ML	Functional	ML update
		Non-functional	computational scalability
	Vulnerability scanner		
		Functional	Agentless scanning
	Security data sources		
		Functional	Logging agents
	System administration		
		Functional	System configuration
			Automated configuration
		on-functional	Scaling
			Container deployment
	Optional extensions		
		Functional	Backup

vulnerability scanner	non-functio	open tool
	non-functio	secure transfer
security data sources	non-functio	support for log types
optional extensions	non-functio	backup automation

service manage	reporting	non-functio	report archive

role			
system adminis	system administration	functional	access management
	optional extensions	functional	backup