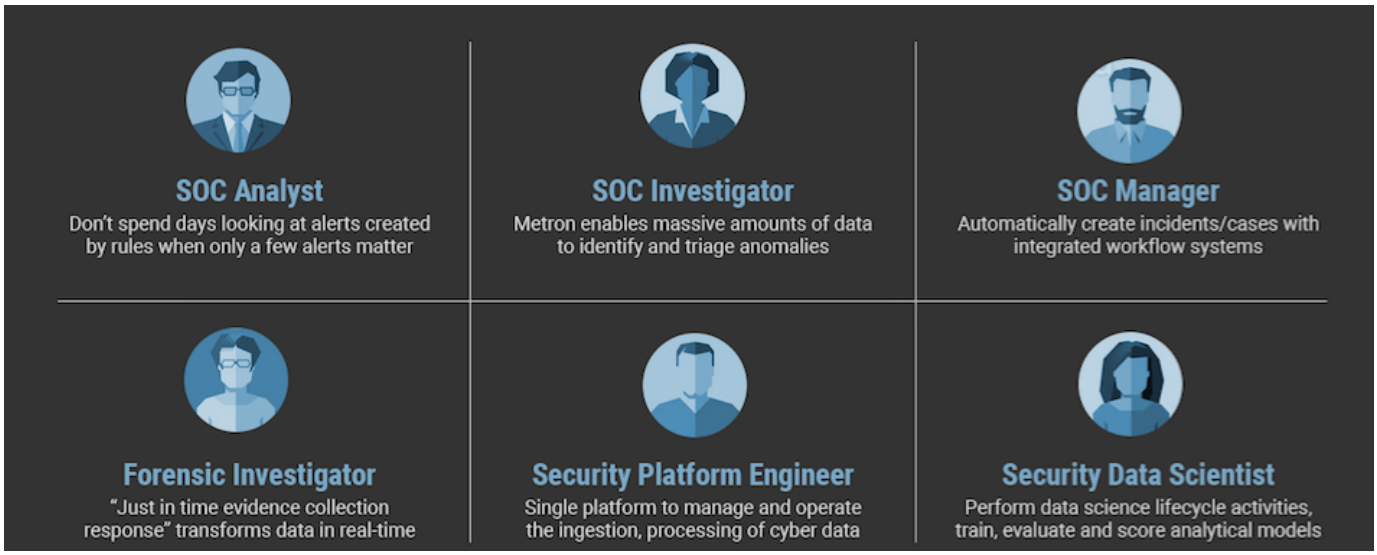
Metron User Personas And Benefits

Metron User Personas

There are six user personas for Metron:



Responsibilities

Persona Name	Description
SOC Analyst	• Profile: Beginner, Junior-level analyst • Tools Used: SIEM tools/dashboards, Security endpoint UIs, Email/Ticketing/Workflow Systems • Responsibilities: Monitor security SIEM tools, search/investigate breaches, malware, review alerts and determine to escalate as tickets or filter out, follow security playbooks, investigate script kiddie attacks.
SOC Investigator	• Profile: More advanced SME in cybersecurity, Experienced security analyst, understands more advanced features of security tools, thorough understanding of networking and platform architecture (routers, switches, firewalls, security), Ability to dig through and understand various logs (Network, firewall, proxy, app, etc..) • Tools Used: SIEM/Security tools, Scripting languages, SQL, command line • Responsibilities: Investigate more complicated/escalated alerts, investigate breaches, Takes the necessary steps to remove/quarantine the malware, breach or infected system, hunter for malware attacks, investigate more complicated attacks like ADT (Advanced Persistent Threats)
SOC Manager	• Profile: Experience managing teams, security practitioner that has moved into management. • Tools Used: Workflow Systems (e.g: Remedy, JIRA), Ticket/Alerting Systems • Responsibilities: Assigns Metron Cases to Analysts. Verifies "completed" metron cases.
Forensic Investigator	• Profile: E-discovery experience with security background. • Tools Used: SIEM and e-discovery tools • Responsibilities: Collect evidence on breach/attack incident, prepare lawyer's response to breach,

Security Platform Operations Engineer	• Profile: Computer Science, developer, and/or Dev/Ops Background. Experience with Big Data technologies and supported distributed applications/systems • Tools Used: Security Tools (SIEM, endpoint solutions, UEBA solutions), provisioning, management and monitoring tooling, various programming languages, Big Data and distributing computing platforms. • Responsibilities: Helps vet different security tools before bringing them into the enterprise. Establishes best practices and reference architecture with respect to provisioning, management and use of the security tools/ configures the system with respect to deployment/monitoring/etc. Maintains the probes to collect data, enrichment services, loading enrichment data, managing threat feeds, etc..Provides care and feeding of one or more point security solutions. Does capacity planning, system maintenance and upgrades.
Security Data Scientist	• Profile: Computer Science / Math Background, security domain experience, dig through as much data as available and looks for patterns and build models • Tools Used: Python (scikit learn, Python Notebook), R, Rstudio, SAS, Jupyter, Spark (SparkML) • Responsibilities: Work with security data performing data munging, visualization, plotting, exploration, feature engineering and generation, trains, evaluates and scores models