SIEMs Review

QRADAR,ARCSIGHT,SPLUNK

By: M.Sharifi
Sharifi1984@gmail.com

1.QRadar

- IBM's QRadar Security Intelligence Platform comprises the QRadar Log Manager, Data Node, SIEM, Risk Manager, Vulnerability Manager, QFlow and VFlow Collectors, and Incident Forensics,
- The QRadar platform enables collection and processing of security event and log data, NetFlow, network traffic monitoring using deep-packet inspection and full-packet capture, and behavior analysis for all supported data sources.
- Combination of flow-based network knowledge , security event correlation , asset-base vulnerability assessment Monitor and display event in real time or perform advance research
- QRadar SIEM can import VA information from various third-party scanners.VA information helps QRadar Risk Manager identify active hosts, open ports, and potential vulnerabilities.

Qradar Capabilities:

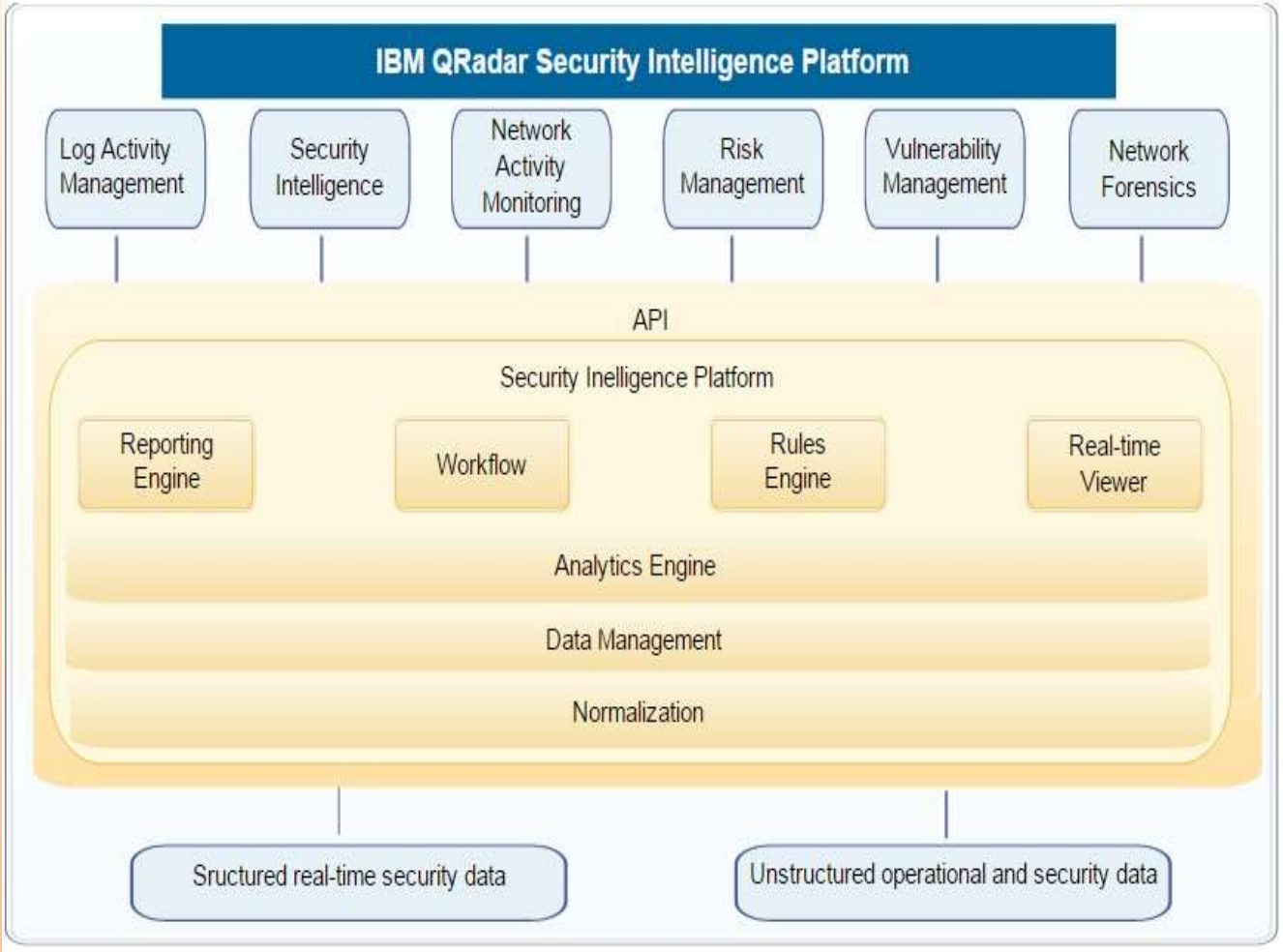
- ✓ Log activity
- ✓ Network activity
- ✓ Assets
- ✓ Offences
- ✓ Reports
- ✓ Data collection

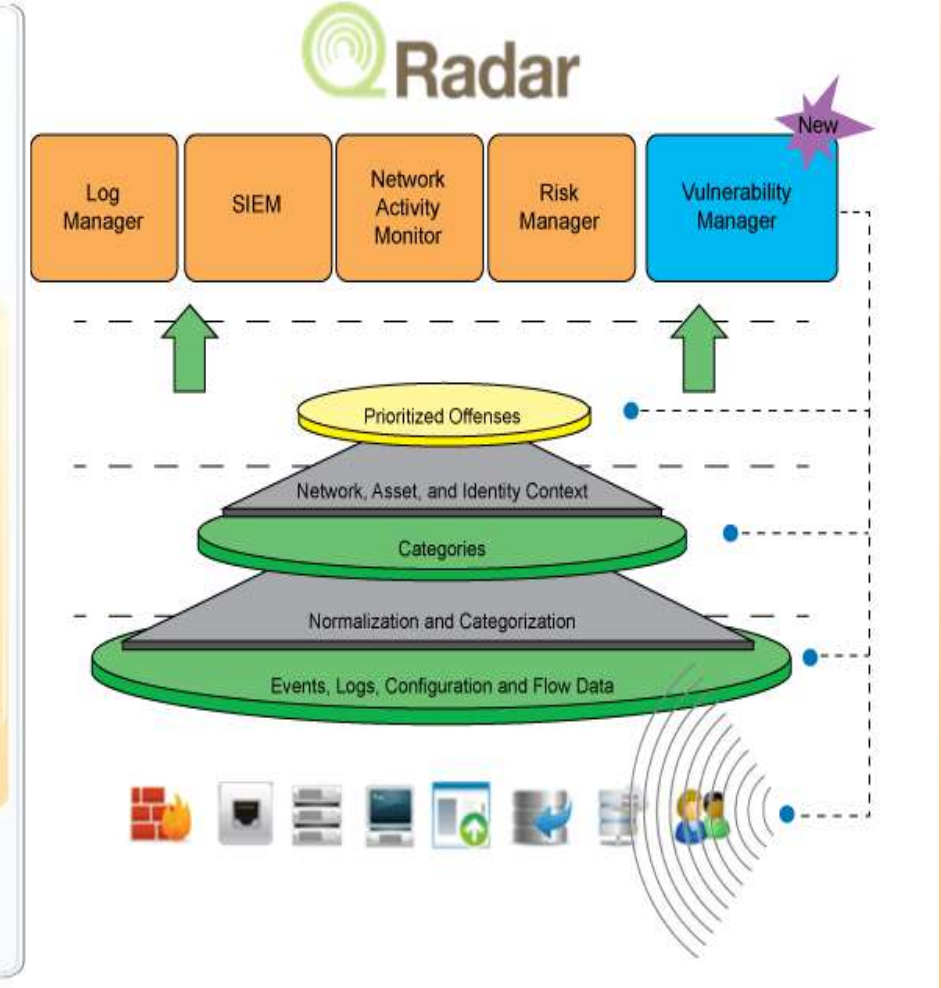
QRadar Log Manager – turn key log management solution for Event log collection & storage
QRadar SIEM – Integrated Log, Threat & Risk Management solution
QRadar Risk Manager – Predictive threat & risk modelling, impact analysis & simulation
QRadar QFlow – Network Behavior Analysis & Anomaly detection using network flow data
QRadar vFlow – Application Layer monitoring for both Physical & Virtual environment

WEB Interface

- Flow search
- Offenses
- Log activity
- Most recent reports
- System summary
- Risk Monitoring Dashboard
- Monitoring policy compliance
- Monitoring risk change
- Vulnerability Management items
- System notification
- Internet threat information center

Qradar Architecture





Gartner Report about IBM Security

- Real-Time Monitoring
- Incident Response and Management
- Advanced Threat Defense
- Business Context and Security Intel
- User Monitoring
- Data and Application Monitoring
- Advanced Analytics
- Deployment and Support Simplicity
- Use Cases

STRENGTHS

- QRadar provides an integrated view of log and event data, with network flow and packets, vulnerability and asset data, and threat intelligence.
- Network traffic behavior analysis can be correlated across NetFlow and log events.
- QRadar's modular architecture supports security event and log monitoring in IaaS environments, including native monitoring for AWS CloudTrail and SoftLayer.
- QRadar's technology and architectural approach makes it relatively straightforward to deploy and maintain, whether as an all-in-one appliance or a large-tiered, multisite environment.
- IBM Security App Exchange provides a framework to integrate capabilities from third-party technologies into the SIEM dashboards and investigation and response workflow.

CAUTIONS

- Endpoint monitoring for threat detection and response, or basic file integrity requires use of third-party technologies.
- Gartner clients report mixed success with the integration of the IBM vulnerability management add-on for QRadar.
- Gartner clients report the sales engagement process with IBM can be complex and requires persistence.

2. ArcSight

Hewlett Packard Enterprise (HPE) sells its ArcSight SIEM platform to midsize organizations, enterprises and service providers. The platform is available in three different variations: the ArcSight Data Platform (ADP), providing log collection, management and reporting; ArcSight Enterprise Security Management (ESM) software for large-scale security monitoring deployments; and ArcSight Express, an appliance-based all-in-one offering that's designed for the midmarket, with preconfigured monitoring and reporting, as well as simplified data management.

In 2015, HPE redesigned and simplified the ArcSight SIEM architecture and licensing model. Further enhancements include new features in the analyst user interface allowing more granular control over incoming events and incidents. New module releases included HPE ArcSight UBA; HPE ArcSight DNS Malware Analytics, providing malware detection based on DNS traffic analysis; HPE ArcSight Marketplace, a community exchange for integration with other vendor solutions; and SIEM context such as dashboards and report templates.

Features and benefits:

- Data enrichment
- Categorization and normalization of data
- Multidimensional real-time correlation
- Ultra-fast investigations and forensics
- Out-of-the-box security use cases
- Workflow automation

Optional packages:

- High availability (HA)
- Threat detector
- Threat central and reputation security monitor
- Compliance packages
- Interactive discovery
- Risk insight

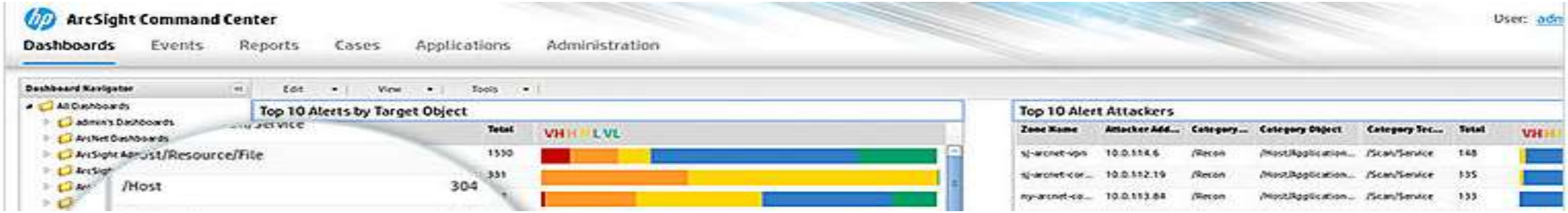
ArcSight Enterprise Security Manager (ESM): Correlation and analysis engine used to identify security threat in real-time& virtual environments

ArcSight Logger: Log storage and Search solution

ArcSight Identity View: User Identity tracking/User activity monitoring

ArcSight Connectors: For data collection from a variety of data sources

ArcSight Auditor Applications: Automated continuous controls monitoring for both mobile& virtual environments



Built-in dashboards for real-time security analytics:

- malware activity
- firewall
- IPS
- endpoint logs
- user activity

These dashboards help you understand the threats and risks that enable you to make smart decisions about where to focus your security team's time and attention.

Also included are dashboards that monitor critical infrastructure, such as Cisco appliances, Microsoft® Windows®, and Linux® servers to quickly report on business critical infrastructure

ArcSight Architecture

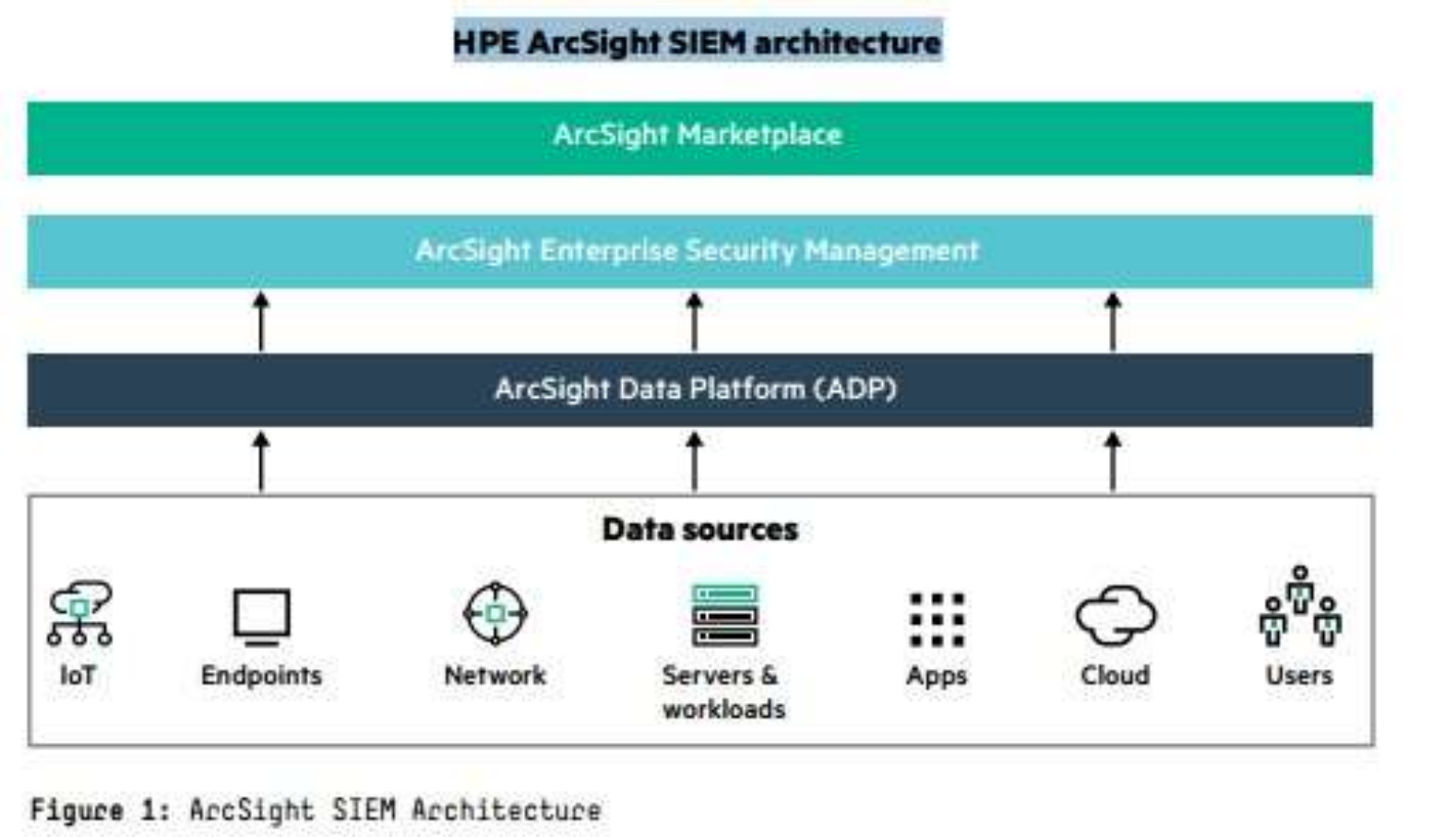


Figure 1: ArcSight SIEM Architecture

Gartner Report about ArcSight

ArcSight SIEM platform to midsize organizations, enterprises and service providers.
The platform is available in three different variations: the ArcSight Data Platform (ADP), providing log collection, management and reporting; ArcSight Enterprise Security Management (ESM) software for large-scale security monitoring deployments; and ArcSight Express, an appliance-based all-in-one
The ArcSight Data Platform (composed of ArcSight Connectors, ArcSight Management Center and Logger) can be deployed independently as a log management solution, but is also used as the data collection tier for ArcSight ESM deployments.
Premium modules, adding capabilities such as user and entity behavior analytics (ArcSight User Behavior Analytics [UBA]), DNS malware detection and threat intelligence, can be used to extend the SIEM's capabilities.
HPE ArcSight can be deployed as an appliance, software or virtualized instance, and supports a scalable n-tier architecture with HPE ArcSight Management Center available to manage large and complex deployments.
HPE ArcSight Express is available as an appliance only.

STRENGTHS

- ArcSight ESM provides a complete set of SIEM capabilities that can be used to support a large-scale SOC, including a full incident investigation and management workflow, and a dedicated deployment management console.
- HPE ArcSight User Behavior Analytics provides full UBA capabilities in conjunction with SIEM.
- HPE ArcSight has a wide variety of out-of-the-box third-party technology connectors and integrations.

CAUTIONS

- HPE ArcSight proposals routinely include more professional services than comparable offerings.
- Customer feedback indicates that HPE ArcSight ESM is found to be more complex and expensive to deploy, configure and operate than other leading solutions.
- Although ArcSight is among the top four vendors in competitive visibility with Gartner clients, the trend is decreasing visibility for new installs and increasing numbers of competitive replacements.
- HPE is undertaking a development effort to redo the core ArcSight technology platform. Customers and prospective buyers should track development plans to ensure the availability of features and functions needed to support existing or planned deployments.

3.Splunk

The Splunk Security Intelligence Platform is composed of Splunk Enterprise — the core product from Splunk that provides event and log collection, search and visualization using the Splunk query language — and Splunk Enterprise Security (ES), which adds security-specific SIEM features.

Data analysis is the primary feature of Splunk Enterprise, and is used for IT operations, application performance management, business intelligence and, increasingly, for security event monitoring and analysis when implemented with Enterprise Security.

Splunk Enterprise Security provides predefined dashboards, correlation rules, searches, visualizations and reports to support real-time security monitoring and alerting, incident response, and compliance reporting use cases.

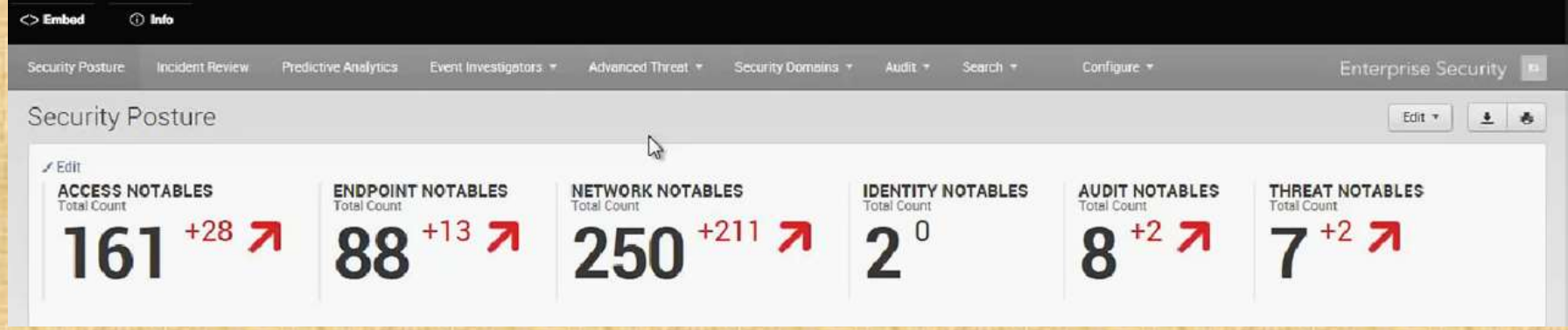
Splunk Enterprise and Splunk Enterprise Security can be deployed on-premises, in public or private clouds, or as a hybrid. Both products are also available as a SaaS offering.

Splunk's architecture consists of streaming input and Forwarders to ingest data, Indexers that index and store raw machine logs, and Search Heads.

splunk>enterprise

- Any Machine Data
- Security and Administration
- Enterprise-Class High Availability and Scale
- Splunk base Apps and Add-Ons
- Open Development Platform
- Enterprise Integration

• Splunk Indexer – used to collect and index logs from IT environment
• Splunk Search Heads – used to search & report on IT logs
• Splunk App for Enterprise Security - used to collect external threat intelligence feeds,
parse log sources and provide basic analytics for session monitoring (VPN, Netflow etc.)



- Collect and index data
- Search an investigate
- Correlate and analyze using Splunk search processing language (SPL)
- Visualize and report
- Monitor and alert
- Mobility

Spunk's architecture consists of streaming input and Forwarders to ingest data, Indexers that index and store raw machine logs, and Search Heads that provide data access via the web-based GUI interface.

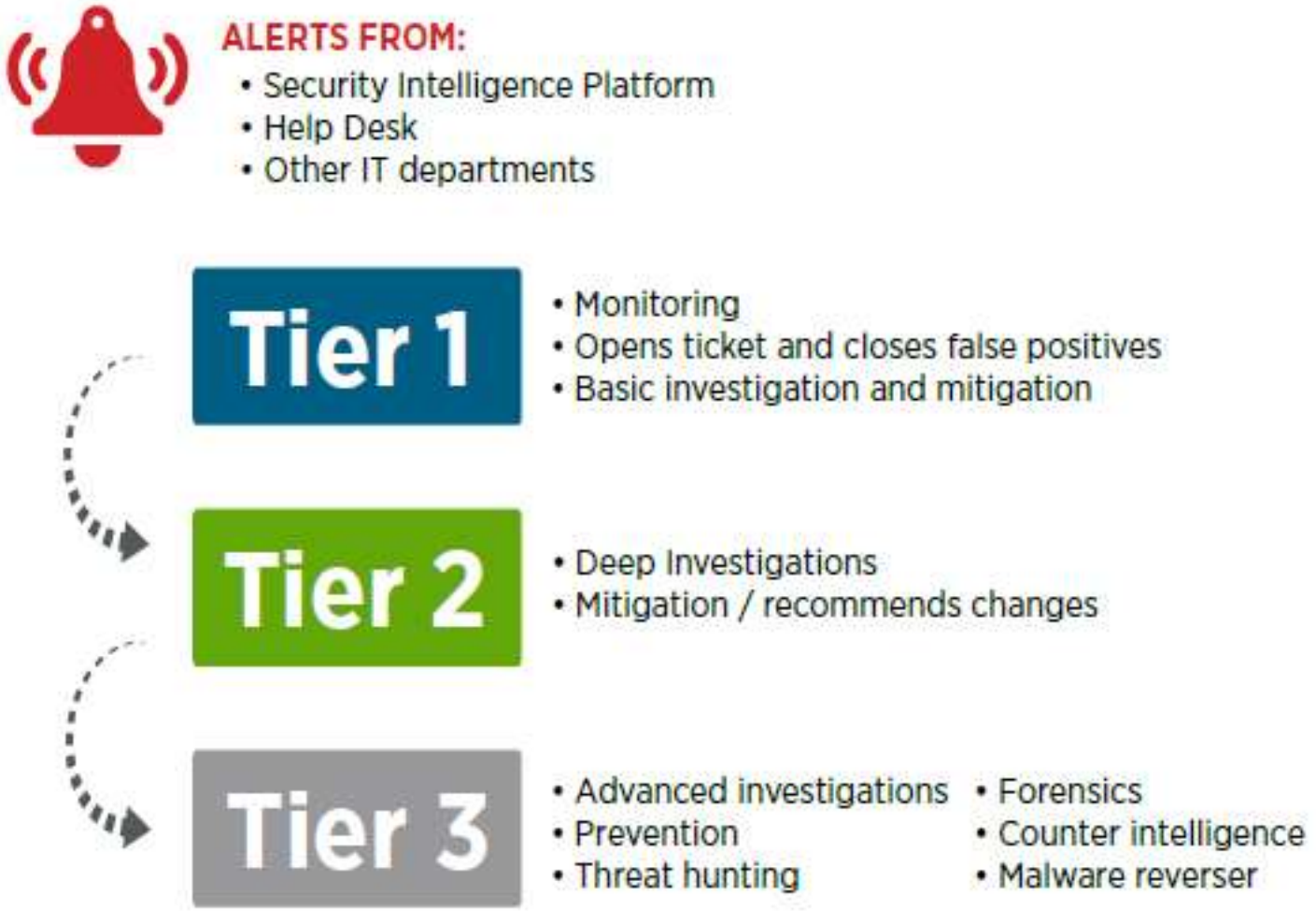


Figure 2: Example of a three-tier SOC and related responsibilities.

STRENGTHS

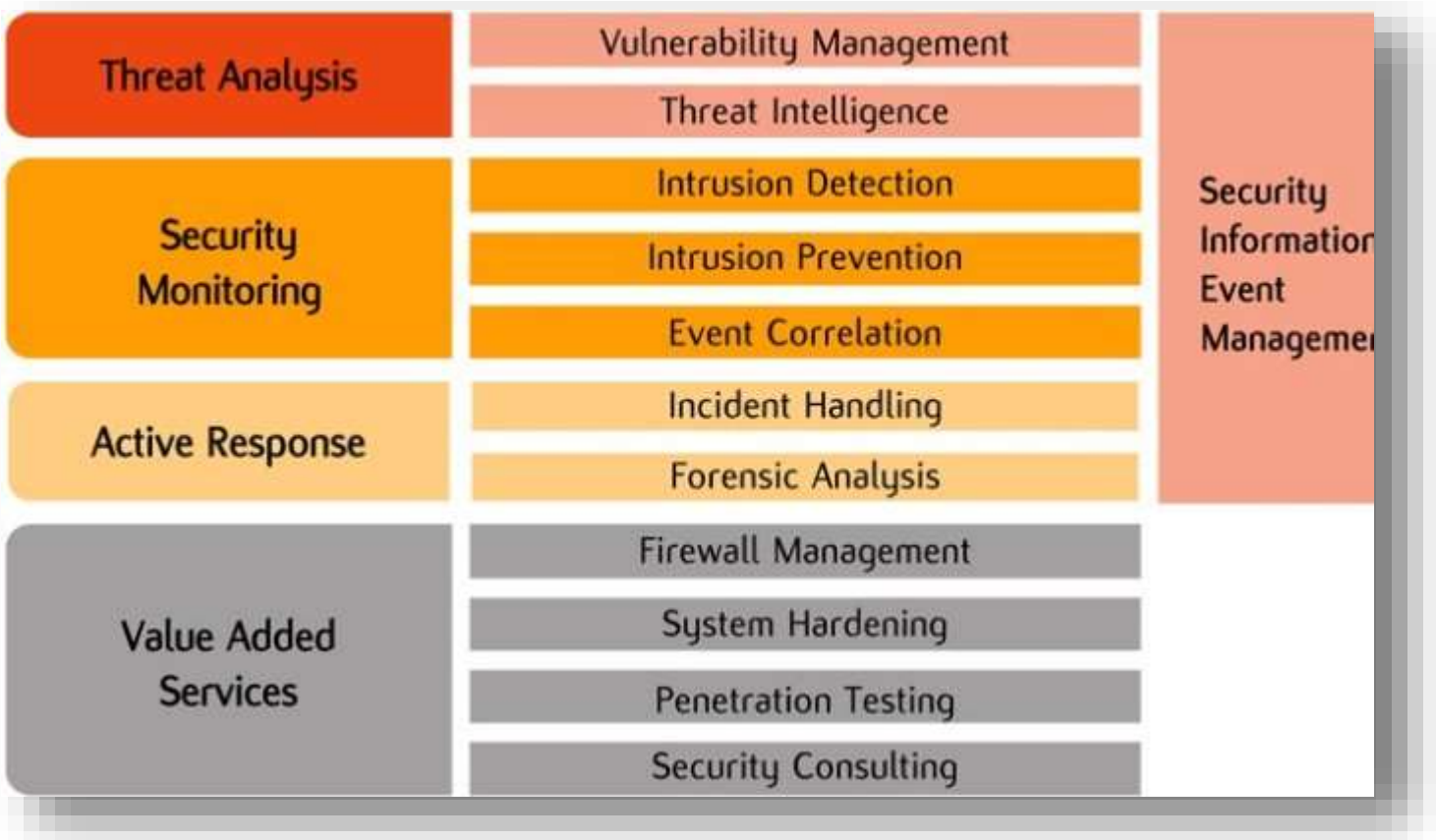
- Splunk's investment in security monitoring use cases is driving significant visibility with Gartner clients.
- Advanced security analytics capabilities are available from both native machine learning functionality and integration with Splunk UBA for more advanced methods, providing customers with the necessary features to implement advanced threat detection monitoring and inside threat use cases.
- Splunk's presence, and investment, in IT operations monitoring solutions provides security teams with in-house experience, as well as existing infrastructure and data to build upon when implementing security monitoring capabilities.

CAUTIONS

- Splunk Enterprise Security provides only basic predefined correlations for user monitoring and reporting requirements, compared with richer content for use cases provided by leading competitors.
- Splunk license models are based on data volume in gigabytes indexed per day. Customers report that the solution is costlier than other SIEM products where high data volumes are expected, and recommend sufficient planning and prioritization of data sources to avoid overconsuming licensed data volumes. In the past 12 months, Splunk introduced licensing programs to address high-volume-data users.
- Potential buyers of Splunk UBA should plan appropriately, as it requires a separate infrastructure and leverages a license model different from how Splunk Enterprise and Enterprise Security are licensed.

Comparison

It’s a comparison vision to compare most important SIMs



IBM QRadar

Strengths :

- Very simple deployment & configuration
- Integrated view of the threat environment using NetFlow data , IDS/IPS data & Event logs from the environment
- Behavior & Anomaly Detection capabilities for both NetFlow & Log data
- Suited for small, medium & large enterprises
- Highly Scalable & Available architecture

Weakness

- Limited customizations capabilities
- Limited Multi-tenancy support
- Limited capability to perform Advanced Use Case development & analytics

HP ArcSight

Strengths

- Extensive Log collection support for commercial IT products & applications
- Advanced support for Threat Management, Fraud Management & Behavior Analysis
- Mature Event Correlation, Categorization & Reporting
- Tight integration with Big data Analytics platform like Hadoop
- Highly customizable based on organization’s requirements
- Highly Available & Scalable Architecture supporting Multi-tier & Multi-tenancy

Weakness

- Complex deployment & configuration
- Mostly suited for Medium to Large Scale deployment
- Requires skilled resources to manage the solution
- Steep learning curve for Analysts & Operators

Splunk

Strengths

- Extensive Log collection capabilities across the IT environment
- Log search is highly intuitive – like Google search Flexible dash boarding & analytics capability
- improves Log visualization capabilities
- Built-in support for external threat intelligence feeds both open source & commercial
- “App Store” based architecture allowing development of Splunk Plugins to suit monitoring & analytics requirements

Weakness

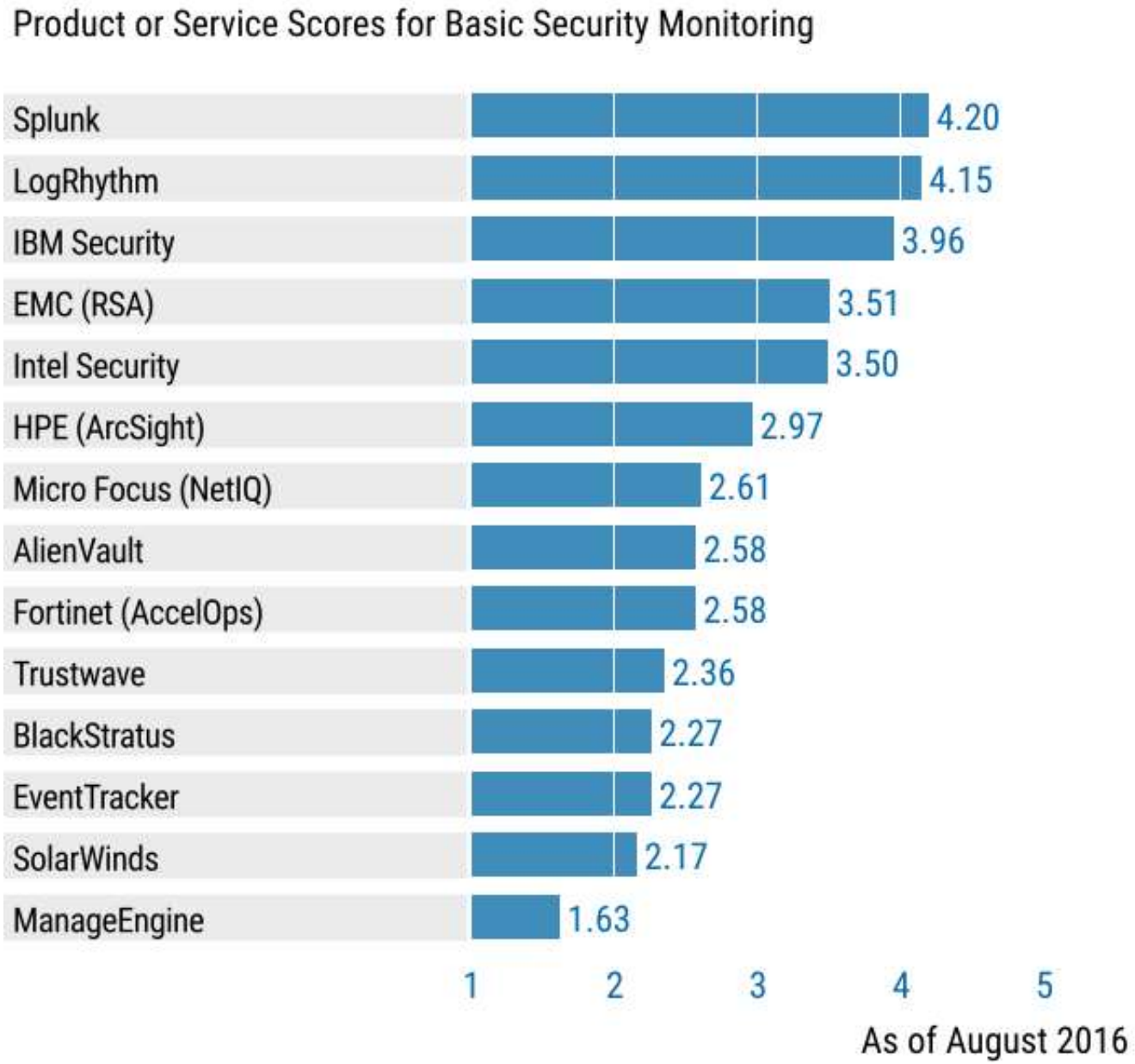
- Pre-SIEM solution with very limited correlation capabilities
- Even though easy to deploy, increasingly difficult to configure for SIEM related functions

SIEM Vendors – Critical Capabilities Score Card

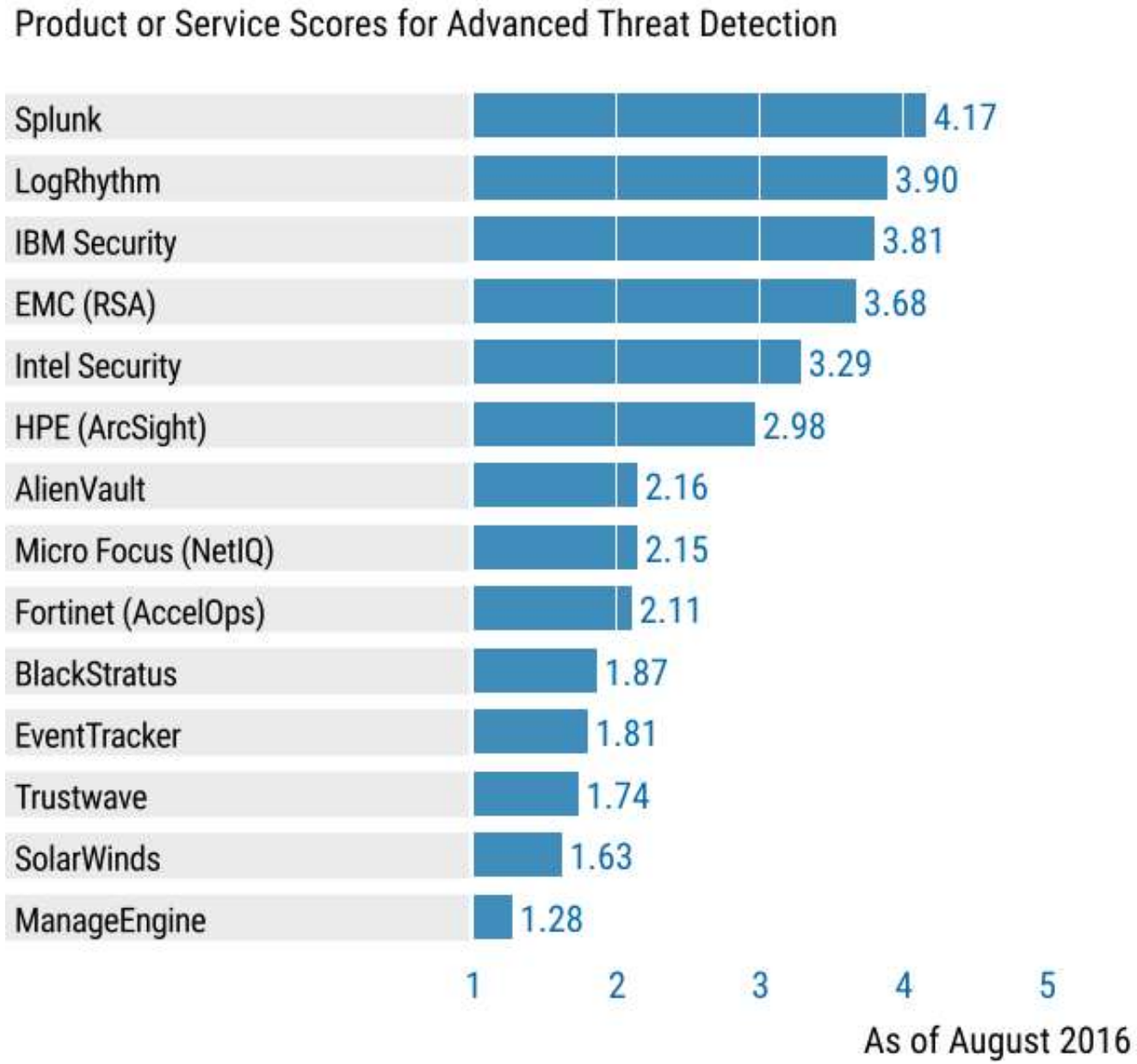
A Summary scoring sheet for SIEM Vendors based on their Core capabilities is given below:

Capability	RSA Security Analytics	Log Rhythm	Splunk	McAfee Nitro	IBM QRadar	HP ArcSight
Real-time Security Monitoring	3.1	3.2	2.5	3.9	4.2	4.4
Threat Intelligence	3.7	2.5	3.0	2.8	3.5	4.5
Behavior Profiling	2.5	2.3	3.0	3.0	5.0	4.0
Data & End User Monitoring	3.6	3.5	1.7	3.6	3.5	4.0
Application Monitoring	3.8	3.5	1.8	3.7	3.3	3.8
Analytics	2.5	2.5	3.8	4.5	3.5	4.0
Log Management & Reporting	3.5	3.8	3.5	3.8	3.9	4.0
Deployment & Support Simplicity	3.0	4.0	2.5	3.5	3.5	3.0
Total (Weighted Score)	**25.7**	**25.3**	**21.8**	**28.8**	**30.4**	**31.7**

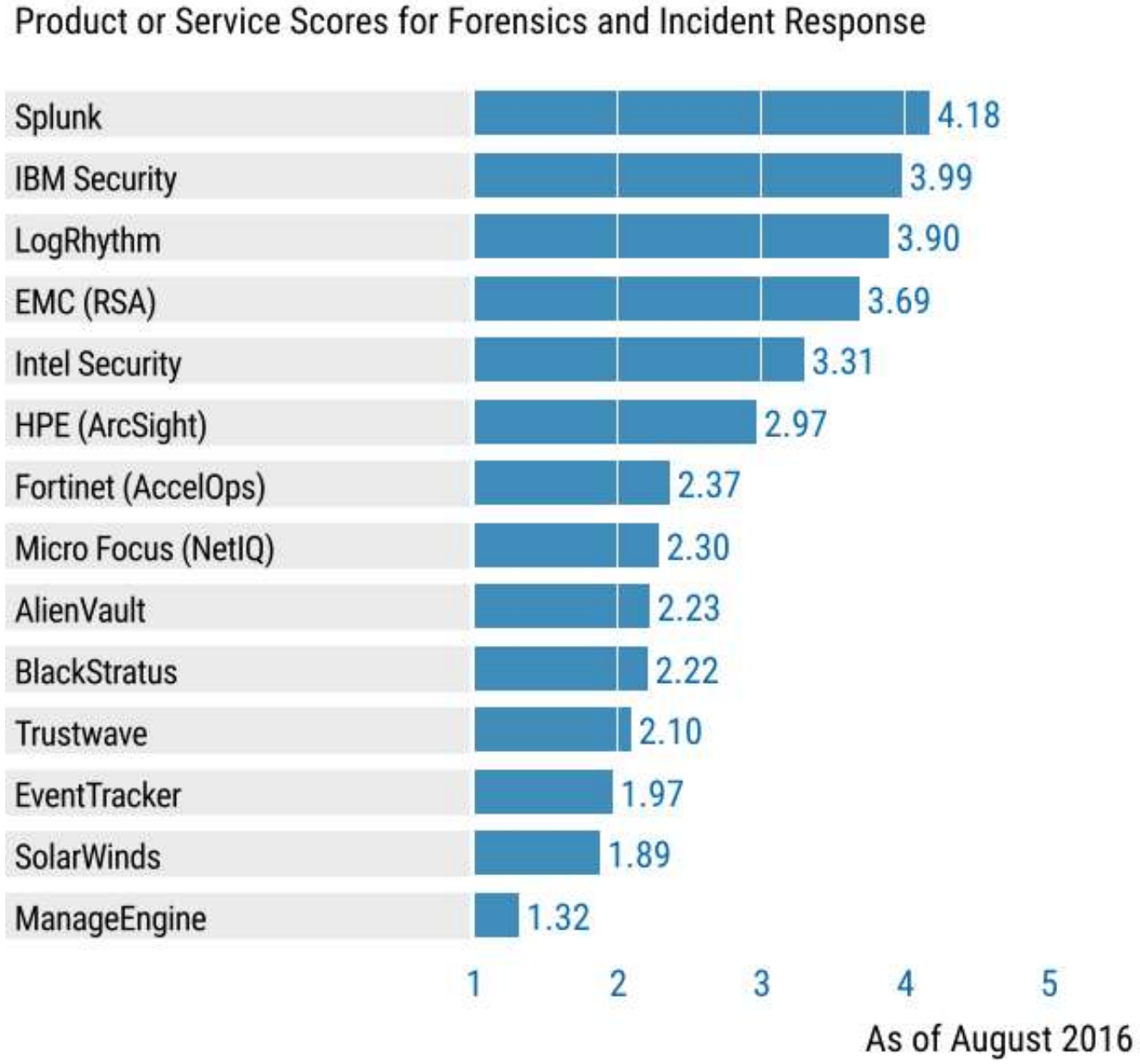
Gartner comparison



Gartner comparison



Gartner comparison



Gartner comparison

Critical Capabilities	AlienVault	BlackStratus	EMC (RSA)	EventTracker	Fortinet (AccelOps)	HPE (ArcSight)	IBM Security	Intel Security	LogRhythm	Manage Engine	Micro Focus (NetIQ)	SolarWinds	Splunk	Trustwave
Real-Time Monitoring	2.7	1.8	3.3	2.2	2.8	3.3	4.1	3.7	4.5	2.0	2.8	2.1	4.3	2.0
Incident Response and Management	2.3	2.7	3.8	2.1	2.6	2.9	4.2	3.1	4.0	1.2	2.3	2.1	4.2	2.5
Advanced Threat Defense	2.5	1.4	3.8	1.8	1.7	2.7	3.5	3.0	4.1	1.0	1.7	1.1	4.0	1.4
Business Context and Security Intel	1.7	1.8	3.8	1.5	2.0	2.9	4.1	3.6	2.8	1.0	1.7	1.0	3.9	1.5
User Monitoring	2.3	2.0	3.5	2.3	2.5	3.1	3.7	3.5	4.1	2.0	3.5	2.3	4.3	2.5
Data and Application Monitoring	2.1	1.7	3.9	1.4	2.0	3.3	3.3	3.7	3.9	1.0	2.7	2.5	4.0	1.8
Advanced Analytics	1.5	1.9	3.7	1.4	1.7	3.0	4.0	2.7	3.9	1.0	1.2	1.0	4.5	1.0
Deployment and Support Simplicity	3.3	3.0	3.3	3.1	3.0	2.7	3.9	3.7	4.5	2.0	3.1	3.0	4.2	3.4
As of August 2016														

Table 2. Weighting for Critical Capabilities in Use Cases