	ARCHITECTURE - KEY DIFFERENTIATORS	SECNOLOGY	COMPETITORS
1	Total Number of Modules	4	More than 50
2	Additional Costly Options	0	Many
3	Scalability Capability	Unlimited	Some of Them
4	Scalability Cost	0	per CPU - per VM
5	High Availability Cost	0	per CPU - per VM
6	Free on-demand Custom Parsers	10	0
7	Free on-demand Vendors Support	10	0
8	Free Compliance Reports PCI-DSS, SoX, HIPAA	Yes	No
9	Smooth Stepwise Events Licencing	Yes (events per year)	No (events per second or day)
10	Recover Unused Credit Licensing	Yes	No
11	Time to Setup Initial Installation	5 minutes	Many Hours
12	Standard Project Deployment Duration	Few Days	Many Weeks
13	Architecture Bottleneck	No	Yes
14	Speed & Performance	High	Medium
15	High Availability	Easy	Very Complex
16	Multiple Site High Availability	Yes	Some of Them
17	Customizable User Interface per User	Yes	No
18	Actionnable Jobs on Data Reports	Yes	No
19	Free Supported Protocols	22	< 12
20	Type of Supported Devices	All	Predefined List
21	Number of Collected Events on standard CPU	200 000 eps	80 000 eps
22	Adherence to the Database storage	None	Yes
23	Simultaneous Concurrent Data Access	Yes	Some of Them
24	Additional Softwares Required	No	Yes
25	Software Data Corruption	Never	Possible
26	Disk Space Overhead	120% of raw data	>900% of raw data
27	Dedicated Platforms required	No	Most of Them
28	Nb of Platforms required to process 50 GB/day	1	6
29	Minimum requirement to process 50 GB/day	Dual CPU, 16 GB RAM	8-Proc, 512 GB RAM/U
30	Compatible with your Filer, NAS, or SAN	Yes	Depends on Vendors
31	Choice of your Data Storage Type and Location	Yes	Some of Them
32	Full Features Virtualization Support	Yes	Some of Them
33	Daily Data Volume Processing	No Limit	Limited
34	Global Data Volume Capacity	No Limit	Limited
35	Ability to Process Far History	Yes	No
36	Raw Log Retention	All Events	Only Matched Events
37	Data Retention Period	No Limit	Maximum 12 months
38	Data Accessibility	Always	Limited to 3 months
39	Simultaneous Data Indexing and Parsing	Yes	No
40	Autonomy versus other IT dept.(DBA)	Yes	No
41	Stealth Environment Integration	Yes	No
42	Continuous Handholding required	No	Yes
43	Number of FTE required to maintain ops	0,3	1,5
44	Standard Training Duration	3 days	3 weeks
45	Coding & Programming Skilled Staff required	No	Mandatory
46	Standard Payback ROI	4 months	36 months

	APPLICATION USAGE - KEY DIFFERENTIATORS	SECNOLOGY	COMPETITORS
1	Security Event Management	Yes	Some of Them
2	Action & Response Automation	Yes	Some of Them
3	Event Orchestration	Yes	Some of Them
4	Big Data Mining	Yes	Some of Them
5	Search Engine	Yes	Some of Them
6	Forensics Investigation with Flow recording	Yes	Some of Them
7	Event Data Collection	Yes	Some of Them
8	Cross Devices Event Correlation	Yes	Some of Them
9	Configuration Audit & Analysis	Yes	Some of Them
10	User & Entity Behavious Analytics	Yes	Some of Them
11	Real-Time Users Activity Monitoring	Yes	Some of Them
12	Real-Time Users Rights Auditing	Yes	Some of Them
13	Threat Identification Remediation	Yes	Some of Them
14	Alert Triage Automation	Yes	Some of Them
15	Threat Detection	Yes	Some of Them
16	Threat Remediation Automation	Yes	Some of Them
17	Vulnerability Detection	Yes	Some of Them
18	Vulnerability Remediation Identification	Yes	Some of Them
19	Policy Control Management	Yes	Some of Them
20	Users & Entity Access Rights Management	Yes	Some of Them
21	WorkFlow Automation	Yes	Some of Them
22	IT & Business Governance	Yes	Some of Them
23	IT & Business Automation	Yes	Some of Them
24	File Integrity Monitoring	Yes	Some of Them
25	Big Data Visualization	Yes	Some of Them
26	SIEM Front-End Proxy	Yes	Some of Them

	DATA PROCESSING - KEY DIFFERENTIATORS	SECNOLOGY	COMPETITORS
1	Available Fields for Correlation	All Fields	Only Few
2	Time Correlation Support	Any	Limited to 1 Hour
3	Number of Correlation Depth Layers	Unlimited	3
4	Multi Gigabytes Correlation	Yes	No
5	Report Display Visualization	+ 100 000 items	Less than 500 items
6	Specific Language Syntax Required	No	Yes
7	Visual Correlation	Yes	Some of Them
8	Know the Unknown	Yes	Some of Them
9	MetaEvent Support	Yes	No
10	Cold and Hot Data Accessibility	Immediate	Procedural
11	Cold and Hot Data Processing	Yes	Only Hot
12	UnMatched Events Investigation	Yes	Impossible
13	Data Archive/Restore	No Need	Mandatory
14	Archive/Restore Service Impact	None	Down Time
15	Archive & Restore Images Compatibility	Yes	Very Complex
16	Specific Backup/Recovery Procedure	No	Mandatory
17	Restore & Roll Back	Immediate	Very Complex
18	Dependencies with 3rd Party Applications	No	Yes
19	Event Log Synchronization	Yes	No
20	Event Data Mining	Yes	Some of Them
21	Number of Supported Native Command Scripts	6	< 3
22	Static Configuration Compliance Analysis	Yes	None of Them

23	Static Configuration Audit Analysis	Yes	None of Them
24	Dynamic Flow Analysis with Security Policies	Yes	None of Them
25	Support for MetaJobs	Yes	No

	PARSING & INDEXING - KEY DIFFERENTIATORS	SECNOLOGY	COMPETITORS
1	Graphical Parser	Yes	No
2	Development Toolkit required	No	Mandatory
3	Standard Log Format Support	Yes	Yes
4	Custom Log Format Support	Yes	Toolkit Required
5	RegExp Parsing	No Need	Mandatory
6	UnMatched Event Awareness	Yes	No
7	Lost & Missing Events	0	Many - Unaware
8	Off-Line Parsing	Yes	No
9	Required Fields	Only Selected Fields	All Fields required
10	Log Normalization	Yes but Not Mandatory	Mandatory
11	Log Aggregation	Yes but Not Mandatory	Mandatory
12	Impact on Column Log Format Modification	Parser Modification	Database Modification
13	Impact on Field Log Format Modification	Parser Modification	Events Lost
14	Unstructured Data Format Support	Yes	No
15	Virtual-Field Support (MetaField)	Yes	No
16	Data Masking	Yes	No
17	Event Categorization	Multiple and Unlimited	Only Once
18	Data Classification	Yes	Some of Them
19	Data Enrichment	Yes	Some of Them
20	Pattern Event Categorization	Yes	No
21	History Event Processing	Yes	No
22	On-the-fly Multiple Data Binding	Unlimited	Only Once
23	Event Data Source Triage	Yes	No
24	On-the-fly Data Categorization	Yes	No
25	On-the-fly Data Segregation	Yes	No
26	Turbo-Indexing on All Raw Data	Yes	Some of Them
27	Turbo-Indexing on Matched Events	Yes	No
28	Turbo-Indexing on Specific Fields	Yes	No
29	Indexes Disk Overhead	15%	> 145%

	DATA MANAGEMENT - KEY DIFFERENTIATORS	SECNOLOGY	COMPETITORS
1	Parallel Reports Generation	Yes	No
2	Multi-Level Drill Down Reports	Yes	Some of Them
3	User Customizable Reports	Yes	Some of Them
4	Multiple Reports Format	Yes	Some of Them
5	Data Policy Segregation	Yes	No
6	Multiple Data Retention Periods	Yes	No
7	Simultaneous Concurrent Data Access	Yes	No
8	Real-Time Rule Processing	Yes	No
9	Regulatory Compliance Support	Unaltered raw Logs	Altered raw Logs
10	External Applications Support	Yes	No
11	Key Metrics Calculation	All	Top 20
12	Raw Data Integrity	Yes	No
13	Raw Data Encryption	Yes	No
14	Raw Data Compression	Yes	No
15	Raw Data Confidentiality	Yes	No

16	Raw Data Availability	Yes	No
17	Raw Data Accessibility	All Time	Limited Timeframe
18	Jobs Execution Triggered on Event	Yes	No
19	Tasks and Command Execution Triggered on Alert	Yes	Some of Them
20	Automated & Custom Alerts	Yes	Some of Them
21	Instant, Real-Time, & Scheduled Reports	Yes	Some of Them
22	Atomic Configuration Import/Export Capabilities	Yes	No
23	Rule-Based Policy Log Segregation	Yes	No

	EVENT COLLECTION - KEY DIFFERENTIATORS	SECNOLOGY	COMPETITORS
1	Supported Collection via OPSEC Protocol	Yes	Some of Them
2	Supported Collection via NETFLOW Protocol	Yes	Some of Them
3	Supported Collection via SFLOW Protocol	Yes	Some of Them
4	Supported Collection via JFLOW Protocol	Yes	Some of Them
5	Supported Collection via POP3 Protocol	Yes	Some of Them
6	Supported Collection via UDP Protocol	Yes	Some of Them
7	Supported Collection via TCP Protocol	Yes	Some of Them
8	Supported Collection via CIDEE Protocol	Yes	Some of Them
9	Supported Collection via SNMP Protocol	Yes, Traps & Requests	Some of Them
10	Supported Collection via ADSI Protocol	Yes	Some of Them
11	Supported Collection via MS-EVENTS Protocol	Yes	Some of Them
12	Supported Collection via DPI Protocol	Yes	Some of Them
13	Supported Collection via PCAP Protocol	Yes	Some of Them
14	Supported Collection via REST-API Protocol	Yes	Some of Them
15	Supported Collection via Wireshark Protocol	Yes	Some of Them
15	Supported Collection via SYSLOG UDP Protocol	Yes	Yes
16	Supported Collection via SYSLOG TCP Protocol	Yes	Some of Them
17	Supported Collection via SFTP Protocol	Yes	Some of Them
18	Supported Collection via ODBC Protocol	Yes	Some of Them
19	Supported Collection via SSL Protocol	Yes	Some of Them
20	Supported Collection via SSH Protocol	Yes	Some of Them
21	Supported Collection via Remote Agents	Yes	Some of Them
22	Supported Collection via any CLOUD	Yes	Some of Them
23	Ingest Terabytes per Day on a Single Server	Yes	No
24	Real-time Display of All Events	Yes	Some of Them
25	Real-time Display of Matched + UnMatched Events	Yes	No
26	Keep All Raw Events	Yes	No
27	Keep Raw Matched Events	Yes	Yes
28	Keep Raw UnMatched Events	Yes	Yes
29	Compressed-Encrypted-Sealed Data Archives	Yes	No
30	Detect & Discard Noisy Events	Yes	No
31	Keep Parsed Results	Yes	Yes
32	Real-Time Collection	Yes	Yes
33	On-Demand or Scheduled Collection	Yes	No
34	On-Event Collection	Yes	No
35	Links between Devices & Collectors	Direct or Indirect	Direct Only
36	Support of Acceleration Protocols	Yes	Some of Them
37	Windows & Linux Collectors	Yes	Some of Them
38	Windows & Linux Agents	Yes	Some of Them

	NATIVE SUPPORT - KEY DIFFERENTIATORS	SECNOLOGY	COMPETITORS
1	Embedded Support for Snort	Yes	Some of Them
2	Embedded Support for Nessus	Yes	Some of Them
3	Embedded Support for WireShark	Yes	Some of Them
4	Embedded Support for SharePoint	Yes	Some of Them
5	Embedded Support for Active Directory + LDAP	Yes	Some of Them
6	Embedded Support for Amazon Web Services	Yes	Some of Them
7	Embedded Support for Microsoft Azure	Yes	Some of Them
8	Embedded Support for Microsoft Office 365	Yes	Some of Them
9	Embedded Support for Google Drive	Yes	Some of Them
10	Embedded Support for Google Dropbox	Yes	Some of Them
11	Embedded Support for Symantec Cloud Services	Yes	Some of Them
12	Embedded Support for NetSkope CASB	Yes	Some of Them
13	Embedded Support for Microsoft Exchange	Yes	Some of Them
14	Embedded Support for Microsoft DLP	Yes	Some of Them
15	Embedded Support for Microsoft LAPS	Yes	Some of Them
16	Native Support for NIST	Yes	Some of Them
17	Native Support for IDS-IPS	Yes	Some of Them
18	Native Support for Vulnerability Management	Yes	Some of Them
19	Native Support for Firewalls	Yes	Some of Them
20	Native Support for Forward Proxy	Yes	Some of Them
21	Native Support for Reverse Proxy	Yes	Some of Them
22	Native Support for Data Loss Protection	Yes	Some of Them
23	Native Support for Anti-Virus	Yes	Some of Them
24	Native Support for Anti-Phishing	Yes	Some of Them
25	Native Support for WAF	Yes	Some of Them
26	Native Support for PAM	Yes	Some of Them
27	Native Support for IAM	Yes	Some of Them
28	Native Support for Threat Management	Yes	Some of Them
29	Native Support for End-Point Protection	Yes	Some of Them
30	Native Support for Messaging System	Yes	Some of Them
31	Native Support for Access Gateway	Yes	Some of Them
32	Native Support for Access Point	Yes	Some of Them
33	Native Support for Network Access Control	Yes	Some of Them
34	Native Support for Authentication	Yes	Some of Them
35	Native Support for AD and LDAP	Yes	Some of Them
36	Native Support for Load-Balancer	Yes	Some of Them
37	Native Support for Router	Yes	Some of Them
38	Native Support for Switch	Yes	Some of Them
39	Native Support for Network Probe	Yes	Some of Them
40	Native Support for Deep Packet Inspection	Yes	Some of Them
41	Native Support for Data Compliance	Yes	Some of Them
42	Native Support for Data Governance	Yes	Some of Them
43	Native Support for Business Intelligence	Yes	Some of Them
44	Native Support for Master Data Management	Yes	Some of Them
45	Native Support for ODBC Database	Yes	Some of Them
46	Native Support for Public, Private, & Hybrid Cloud	Yes	Some of Them
47	Native Support for NAS & SAN	Yes	Some of Them
48	Native Support for Security Operation Center	Yes	Some of Them