Centralized Log Management

Uncover hidden threats with full log data visibilty

The Value of Log Analysis

Log analysis is a powerful tool for uncovering and analyzing suspicious system activities. System logs include network activities, system events, user actions and more across the operating environment. Unfortunately, continuously accessing and analyzing log data from each individual system is tedious and simply impractical.

The Solution: Centralized Log Management

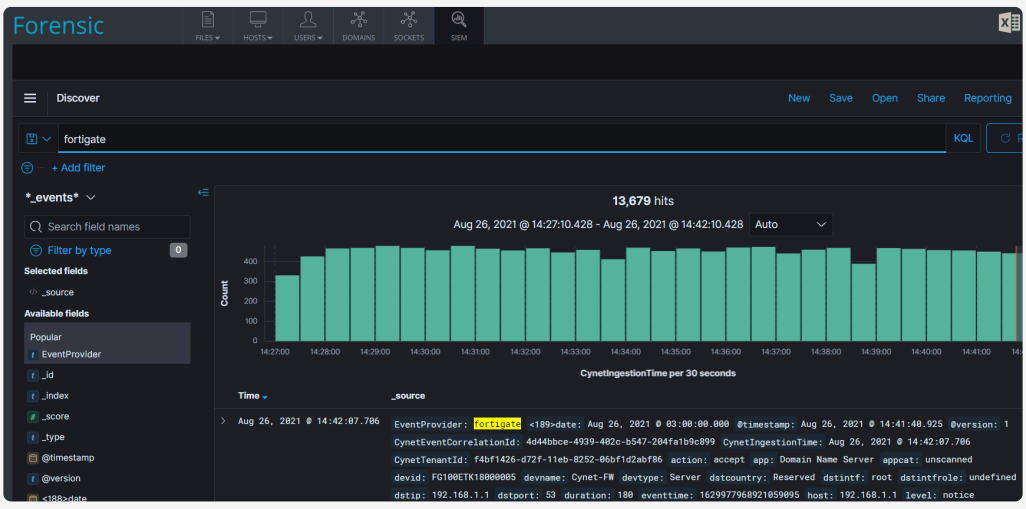
Cynet Centralized Log Management automatically collects the highest priority log data needed to quickly and accurately uncover threats across your environment. Events and data are collected from network devices and applications, SaaS applications and all Cynet hosts. Log data is collected, integrated and normalized in the Cynet data lake, accessible directly from the Cynet console. You can also use Centralized Log Management to meet compliance requirements around log retention and quickly assess adherence to compliance requirements.

Key Benefits

- Centralized Log Management analysis threat for critical
- Gain actionable insights using intuitive analysis and visualization tools
- Easily comply with log retention requirements
- Improve visibility to eliminate security gaps and oversights
- Outsource log collection and retention with Cynet SaaS

Leverage Existing Log Data for Actionable Insights

System logs contain a veritable goldmine of transaction and event history for uncovering and investigating security threats. Unfortunately, the time and effort required to mine this data leads to it being underutilized or ignored. Harness the power of your existing system log data with Cynet Centralized Log Management by leveraging intuitive search, analysis, visualization and reporting tools.



Easily Connect the Dots

The ability to view, query and correlate events from firewalls, AD and endpoints in one forensic investigation experience enables you to connect the dots regarding a security incident.

Example showing the distribution of firewall provider security events by time.

Certified Data Sources

The data sources below are certified data sources for Cynet CLM. For each data source, you must open a designated communication port between the data source and the Logstash server, and set the required log format.

The list of data sources continues to expand; please visit https://help.cynet.com/en/articles/75-centralized-log-management for the most up-to-date list.

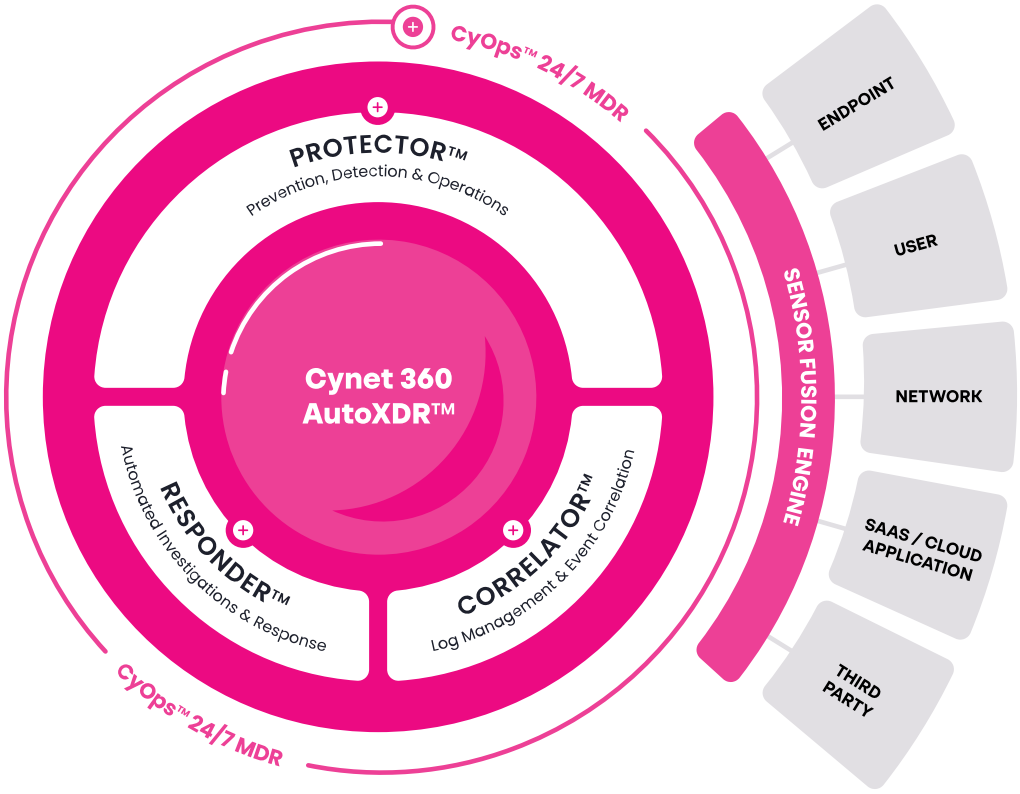
Data Source	Log Format
SonicWall firewall	CEF
Check Point firewall	CEF
Fortigate firewall	CEF
Palo Alto Networks firewall	CEF
WatchGuard firewall	Syslog
VMware ESXi	Syslog
Sophos firewall	Syslog
Cisco Meraki	Syslog
Cisco Firepower	Syslog
Cisco Switch	Syslog
Cisco vWLC	Syslog
NetApp Storage	Syslog
Aruba Switch	Syslog
IBM 3PAR Storage	Syslog
IBM AS400	Syslog
Juniper vSRX ***Coming soon***	TBD
Office 365	Contact Cynet to configure data transfer via webhook
Azure Active Directory	
Zoom	Data transfer via webhook
Cynet 360 Windows Events*	N/A
Cynet 360 File Monitoring*	N/A

*By default, Windows Events and File Monitoring data is displayed in Log Management, with no required license or configuration. This data also appears in the Forensic page. By purchasing a CLM license you extend the default retention period of this data.

About us

Cynet's end-to-end, natively automated XDR platform, backed by a 24/7 MDR service was purpose-built to enable lean IT security teams to achieve comprehensive and effective protection regardless of their resources, team size or skills.

Cynet delivers the prevention and detection capabilities of EPP, EDR, NDR, Deception, UBA rules and CSPM, together with alert and activity correlation and extensive response automation capabilities.



Our vision is to enable security teams to put their cybersecurity on autopilot and focus their limited resources on managing security rather than operating it.

Bring sanity back to cybersecurity with a fresh approach that makes protecting your organization easy and stress-less.

Learn more