


A **SIEM**, by any other name


A BREAKDOWN OF CYBERPULSE'S LOG AGGREGATION AND OTHER SIEM-ISH FEATURES


CyberPulse





BENEFITS AT A GLANCE

 Aggregate logs and add them to network metadata for a deeper understanding of your universe.

 Integrate with cloud services.

 See network and log data & threat activity in a single pane of glass.

 Meet compliance regulations with less investment.

 Includes Office 365® logs.




QUESTIONS?

Contact Us!
1.844.CITYNET
sales@citynet.net
www.citynet.net/cyberpulse

Centralize your security tools & skip the giant price tag.

CyberPulse is a Co-Managed Threat Detection and Response Platform. CyberPulse detects, while our Security Operations Center (SOC), powered by ConnectWise, responds. You have full access to view your alert data and can even have your team analyze it alongside us.

Businesses' most-requested SIEM features are built right into the CyberPulse platform. Now you can access these features directly within CyberPulse:

-  **Collect** – CyberPulse brings all your logs into a single pane of glass, right next to the network data you're already sending us.
-  **Detect** – Add log metadata to reveal behavior patterns and identify potential brute force and other attacks.
-  **Respond** – Search for anomalous events, and generate reports and charts.

Enhance CyberPulse's analysis of your environment.

Whether you prefer to call it SIEM, data lake, or log aggregation, adding it enhances your view of your security posture. CyberPulse's SOC, powered by ConnectWise, is now detecting and investigating threats within log metadata. You can store logs for compliance without any other tools. If you're considering a SIEM purchase with those goals in mind, CyberPulse may be the right option for you.

	Feature	Benefit	
COLLECT	Windows event logs	Insight into services activity and changes, including Active Directory.	
	Syslog data	Insight into device activity, including firewall logs, change management tracking, and error logs.	
	Event parsing	Supports strong search and reporting	
	Collected alongside network data	View log data next to the critical network data you're already collecting to enrich the picture around potential incidents.	
	Flexible retention	Keep your data for as long as you want – meet your regulatory retention requirements easily.	
	Easy deployment	If your CyberPulse sensor is already in your environment, just point your logs our way for collection and retention.	
DETECT	Activity detection	Detection rules for dozens of vendors ensure the broadest out-of-the-box coverage possible.	
	Event correlation	The CyberPulse SOC, powered by ConnectWise, includes collected log data in its analysis to correlate events and further identify potentially malicious activities.	
	Alerting	CyberPulse alerts on bad network activity and escalates to you after our SOC has investigated the incident. CyberPulse's SOC, powered by ConnectWise, uses log data to enrich the context of the network activity to provide even more fidelity when investigating a potential incident.	
RESPOND	Dashboards	Understand log (and network) activity at a glance with a fully customizable view.	
	Reports	Gain insight into the data you are looking at and ensure organizational and regulatory compliance by generating reports around interesting data patterns.	
	Searching and hunting	Conduct forensic investigations – access network data and log history in a single pane of glass from CyberPulse.	

Daunted by threat intel?

DON'T BE. CYBERPULSE AND CITYNET SIMPLIFY THE THREAT INTELLIGENCE PROCESS SO YOU DON'T LIFT A FINGER.

Threat intelligence changes the game.

Threat intel sources are now available with wide ranges of cost and quality; we believe you and your managed service provider should be free to choose how to connect to it and use it effectively. Harnessing great threat intelligence the right way ensures rapid detection of known malicious activity on your network that slips past traditional perimeter defenses – and it's where CyberPulse shines.

CyberPulse lets you choose how to use and interact with your intel.

CyberPulse integrates with any threat intel feed, as well as advanced CTI systems, to bring you world-class managed threat detection. CyberPulse puts your threat intel to work for you so you can:

- ✓ **DETECT** the threats your intel warns you about.
- ✓ **VISUALIZE** threats detected both on your network and by others using the same pool of intel.
- ✓ **ACT** when known threats are detected on your network.

CyberPulse does the legwork.

Your CyberPulse sensor is monitored by Citynet and Connect Wise certified analysts. Armed with familiarity with your network, Citynet walks you through the process and ensures you get the most value from your CyberPulse investment. CyberPulse's custom online tools allow you to see all your threat indicators and participate as much or as little as you wish. If you prefer, with your authorization, Citynet can access your network data.

And you don't need to break the budget.

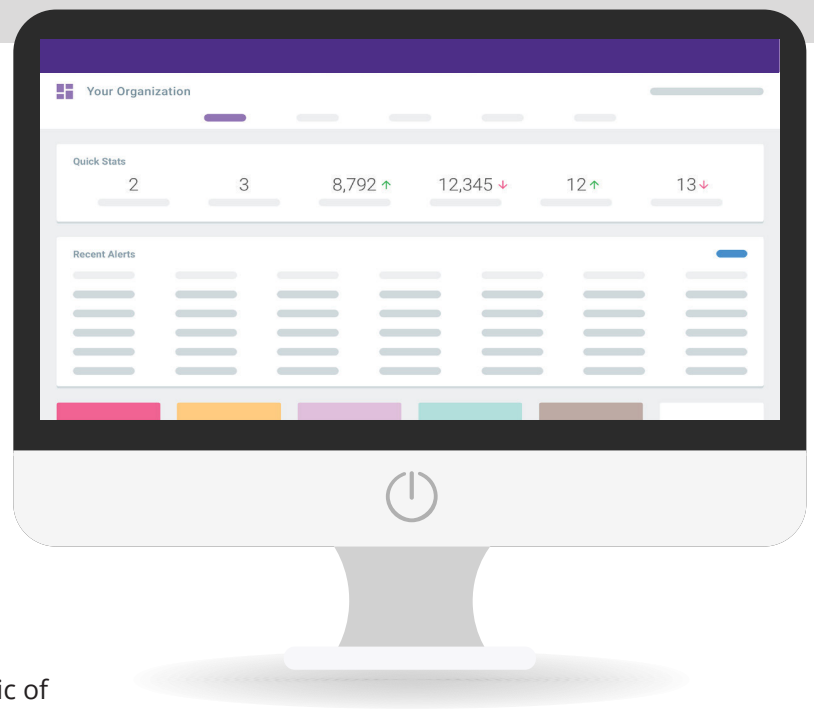
Combined with the expertise and centralized services of Citynet, CyberPulse offers your business a true threat intelligence program without the burdens of hiring threat analysts to process large volumes of data and investing in high-priced security tools.

Start defending with threat intelligence. **Right away.**

CyberPulse lets you **DETECT**, **VISUALIZE** and **ACT** on threat intelligence through three components:

1 CyberPulse Web Application

Our web-based application works with a CyberPulse Sensor to show you any sign of threat activity found on your network. You have full access to view what's happening on your network – and you control who else does.



2 CyberPulse Sensor

Installed in under an hour, our sensors (physical or virtual machine) are placed inside your firewall and monitor the traffic of a network segment via a TAP or SPAN port. Citynet can select the sensor options that best meet your needs.



3 Operations Center (SOC)

While you can see and interact with every alert you receive through CyberPulse, our specialized SOC analysts at Citynet and ConnectWise work each alert to validate real threats and escalate them to Citynet network engineers for fast remediation.

CyberPulse and the Cyber Security Framework

A GUIDE TO NIST CSF CATEGORIES AND BIG WINS WITH CYBERPULSE.

What is the CSF?

The Cyber Security Framework (CSF) was developed by the National Institute of Standards and Technology (NIST) in response to President Obama's Executive Order 13636 to strengthen and standardize critical infrastructure security within the United States. It's a reference tool that guides security practitioners as they work to improve their organization's cyber security posture.

The first step in strengthening cyber security is identifying where you stand today. You have to start

somewhere, and referencing the CSF for that process saves immeasurable effort and hours of research and planning. It's a little like using tax software to file taxes rather than reading the entire tax code and completing returns manually, but on a larger scale. As a framework, the CSF lets you map your current security controls and processes and identify gaps, giving you a basic measurement of organizational cybersecurity maturity. If your goals include complying with regulatory standards, the CSF helps you cover your bases and prioritize your biggest wins.

NIST Cyber Security Framework (CSF)

CyberPulse integrates with any threat intel feed, as well as advanced CTI systems, to bring you world-class managed threat detection. CyberPulse puts your threat intel to work for you so you can:



How to use this guide

Use the CSF to map out current controls that you are able to satisfy and as a gap analysis. A gap analysis will reveal the most pressing security gaps and help you prioritize budget items for improvements. The CSF also eases communication with stakeholders and demonstrates the measurable value your cyber security program provides.

BEGIN YOUR ASSESSMENT



WHERE DOES CYBERPULSE HELP WITHIN THE CSF?

The table on the next page outlines specific functions and categories where CyberPulse boosts maturity. Feel free to use these mappings and incorporate them into your own CSF assessment. CyberPulse makes the biggest impact with these items:



Threat Detection – anomalies and events.



Open threat intelligence ecosystem to ingest threat intel from multiple sources.



Continuous Security Monitoring for the network and logs.



Detection and response procedures to reduce or eliminate emerging threats.



Security orchestration to quickly respond to any incident.



SIEM and log management to solve regulatory and compliance requirements.

Asset Management (ID.AM)

Subcategory ID.AM-5

- All network asset resources can be assigned tags and values. Notes can be created to document criticality and business value.

Risk Assessment (ID.RA)

Subcategory ID.RA-1

- Uses threat intelligence to detect threats leveraging potential vulnerabilities against assets.
- All threats are documented in the alert system and queue.

Subcategory ID.RA-2

- Natively uses STIX and TAXII to ingest and share intelligence from various intelligence sources.
- Support for ISAC/ISAO intelligence.
- Support for federal government intelligence (e.g. DHS, AIS, and CISC).
- Support for open source intelligence feeds.
- Support for commercial intelligence feeds.

Subcategory ID.RA-3

- Detects threats from external facing attacks as well as potential insider threats and attacks occurring inside the network.

Subcategory ID.RA-4

- Threats are correlated against network tags to determine impact to business operations.

Supply Chain Risk Management (ID.SC)

Subcategory ID.SC-4

- Monitors network activity and system log access from supplier use.
- Sensors can be deployed into supplier networks to monitor third party use and behavior.

Identity Management, Authentication, and Access Control (PR.AC)

Subcategory PR.AC-1

- Monitoring for successful and failed logins within internal networks and cloud resources.
- Log monitoring from event logs, application, and processor information to look for credential misuse or anomalies. (AWS, Azure, O365)

Subcategory PR.AC-2

- Logs from physical access systems can be ingested and reviewed.

Subcategory PR.AC-3

- Logs from remote access systems such as VPNs can be ingested and reviewed.

Subcategory PR.AC-7

- Supports multi-factor authentication.
- Ability to ingest authentication logs for review.
- Ability to detect policy and corporate violations from authentications such as clear text logins.

Data Security (PR.DS)

Subcategory PR.DS-5

- Detects network activity to potentially unapproved business applications such as Dropbox, Box, or OneDrive.
- Detects unencrypted authentication mechanisms.
- Multiple intelligence rules to detect data exfiltration from malicious software.

Protective Technology (PR.PT)

Subcategory PR.PT-1

- Audit logs and access logs can be ingested, reviewed, and retained for audit purposes.
- Multiple retention periods exist for logs.

Subcategory PR.PT-3

- Multiple user account types exist to allow for the principle of least privilege.

Subcategory PR.PT-4

- All network segments can be monitored for network traffic and threat analysis.

Subcategory DE.AE-1

- Data flows can be reviewed and assessed via visualizations to detect abnormalities from baseline behavior.
- User-based traffic can be assessed in O365 for file share and application level access.

Subcategory DE.AE-2

- Threat detection is analyzed against multiple threat feeds.
- Threats are correlated with STIX sightings to determine campaign activity and telemetry against peers.
- Threats are reviewed and analyzed by human analysts to determine true/false positive dispositions and actionability.

Subcategory DE.AE-3

- Event data is retained and available to review and analysis in a data lake/SIEM.
- Event data can be correlated against multiple systems simultaneously.
- Network threat metadata can be correlated with log data in a single data lake.

Subcategory DE.AE-4

- Threats are reviewed and analyzed by human analysts to determine impact and severity

Subcategory DE.AE-5

- Alerting thresholds are set in the application to allow for multiple escalation thresholds.
- Events and alerts can automatically notify ticketing systems and call trees.

Subcategory DE.CM-1

- Full PCAP inspection and correlation against multiple threat feeds for cyber security events.
- Subcategory DE.CM-3
- User behavior such as file access, web traffic, and authentication logs are monitored and correlated against threat intelligence.

Subcategory DE.CM-4

- Network traffic is monitored and correlated against threat intelligence to detect malicious code.
- Log ingestion of endpoint control solutions allow for detection of malicious code on the endpoint.

Subcategory DE.CM-5

- Network traffic for mobile devices, such as Android and iOS, is monitored and can be correlated against threat intelligence to detect malicious code.

Subcategory DE.CM-6

- Remote access from external service providers can be monitored and correlated against threat intelligence for abnormalities and threats.
- Remote sensors can be deployed at service provider network locations for review and threat assessment.

Subcategory DE.CM-7

- Network traffic and system logs can be ingested and reviewed to look for unauthorized authentications or device connections.

Subcategory DE.DP-4

- Threats and events can be escalated to multiple user accounts automatically via ticketing, email notification, or API.

Analysis (RS.AN)

Subcategory RS.AN-1

- Alerts and notifications can be consumed via multiple notification opens including email, ticket creation, or API.
 - Alerts are reviewed, triaged, and investigated by security personnel.
- Subcategory RS.AN-3
- Forensic investigations can be performed from log and network traffic data and analytics.
- Subcategory RS.AN-5
- Automatic ingestion of multiple intelligence sources from internal or external sources.
 - Native ingestion of threat intelligence feeds from STIX/TAXII sources.

Mitigation (RS.MI)

Subcategory RS.MI-1

- Ability to orchestrate asset isolation for incident containment via dynamic firewall blocking.
 - Ability to orchestrate asset isolation for incident containment via remote management and monitoring tools.
- Subcategory RS.MI-2
- Ability to orchestrate asset isolation for incident containment via dynamic firewall blocking.
 - Ability to orchestrate asset isolation for incident containment via remote management and monitoring tools.

Benefits of the ConnectWise SOC



24/7/365 THREAT MONITORING AND RESPONSE

- Cybercriminals don't work regular hours.
- Attacks can hit anytime, and the ConnectWise SOC is ready when the time comes.
- We're continuously monitoring, detecting, and remediating threats to keep your clients secure.



FULLY STAFFED TEAM OF SECURITY EXPERTS

The ConnectWise SOC team includes certified security techs, including security analysts, incident response analysts, security researchers, and threat hunters. Do you already have a few security techs on staff? Our team will take care of alerting and triaging and consult your team when there are issues they need to handle.



CUTTING EDGE SECURITY INTELLIGENCE

The threat landscape is always changing. The ConnectWiseCyber Research Unit (CRU) is dedicated to identifying the latest threats, ensuring our SOC team is on high alert to catch what's lurking in the shadows.



SCALE YOUR SECURITY BUSINESS

It's hard and expensive to build out a security team, let alone a fully staffed, 24/7 in-house SOC.

160+

Security professionals supporting Citynet

Capabilities for threat triage and analysis, log review, threat hunting, and incident response.

