Designing a comprehensive cybersecurity system that can detect, prevent, analyze, and predict cyber threats in real-time is a complex task. Below is a high-level system design to enhance cybersecurity measures. Please note that this is a conceptual design, and implementing such a system would require expertise in various domains of cybersecurity.

**1. Data Collection and Ingestion:**

1. Collect data from various sources, including network logs, endpoint data, system logs, application logs, and external threat intelligence feeds.
2. Data should include network traffic, system events, user activity, and more.

**2. Data Preprocessing:**

1. Normalize and preprocess collected data to make it consistent and suitable for analysis.
2. Identify and filter out irrelevant data to reduce noise and focus on potential threats.

**3. Real-time Threat Detection:**

1. Implement real-time intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor network traffic and endpoints.
2. Utilize advanced threat detection algorithms, behavioral analytics, and machine learning models to identify anomalies and potential threats.
3. Employ signature-based and heuristic-based detection techniques to recognize known and unknown threats.

**4. Incident Response:**

1. When a threat is detected, initiate an automated or manual incident response process.
2. Isolate compromised systems, collect forensics data, and mitigate the threat to prevent further damage.
3. Notify security personnel and stakeholders about the incident.

**5. Threat Intelligence Integration:**

1. Integrate external threat intelligence feeds to enrich the analysis of incoming data.
2. Utilize threat intelligence data to identify patterns and indicators of compromise (IoCs).
3. Stay up to date with the latest threats and vulnerabilities.

**6. Threat Analysis and Correlation:**

1. Analyze security events, incidents, and patterns to determine the scope and impact of the threat.
2. Use correlation engines to link related events and uncover complex attack techniques.
3. Employ context-aware analysis to understand the threat's context in the network.

**7. Predictive Analysis:**

1. Implement predictive analytics using historical data to forecast potential future attacks.
2. Machine learning models can identify attack patterns and trends and predict future attack vectors.
3. Implement anomaly detection to identify deviations from normal behavior.

**8. Security Information and Event Management (SIEM):**

1. Utilize SIEM solutions to centralize event and incident management.
2. Provide a single pane of glass for monitoring, analysis, reporting, and alerting.
3. Integrate with log and event sources, including firewalls, antivirus, and IDS/IPS systems.

**9. User and Entity Behavior Analytics (UEBA):**

1. Implement UEBA systems to analyze user and entity behavior for unusual activities.
2. Detect insider threats and compromised accounts through behavior profiling.
3. Trigger alerts when behavior anomalies are identified.

**10. Reporting and Recommendations:**

1. Generate detailed reports on security incidents, threats, and vulnerabilities.
2. Provide recommendations for improving security protocols and strengthening defenses.
3. Implement a feedback loop for continuous improvement and adaptive security strategies.

**11. Access Control and Segmentation:**

1. Enforce strict access controls and network segmentation to limit lateral movement of threats.
2. Employ micro-segmentation to isolate critical systems and data.

**12. Backup and Recovery:**

1. Regularly back up critical data and systems to facilitate quick recovery in case of a successful attack.
2. Test and update disaster recovery and incident response plans.

**13. Security Awareness Training:**

1. Regularly train employees and end-users to recognize and avoid social engineering attacks and phishing attempts.

**14. Patch Management:**

1. Maintain a robust patch management system to keep all software and systems up to date.

**15. Encryption:**

1. Use strong encryption to protect data at rest and in transit.

**16. Red Team Exercises:**

1. Conduct periodic red team exercises to simulate real-world attacks and test the system's defenses.

**17. Compliance and Regulations:**

1. Ensure compliance with relevant cybersecurity regulations and standards.

**18. Monitoring and Review:**

1. Continuously monitor and review the cybersecurity system's performance, adapting to new threats and vulnerabilities.
2. Remember that a successful cybersecurity system is an ongoing effort that requires continuous improvement and adaptation to evolving threats. Collaboration with cybersecurity experts and staying informed about the latest security trends is crucial for maintaining a strong defense against cyber threats.