**PISCES Resiliency Architecture**

**STUDENTS:** Paresh Bapat, Keerthi Pitchapati, Daqian Yao, Bonnie Wang, Ruiqi Li, William Chen, Cameron Jennings

---

**PISCES**
- A nonprofit that teaches students from various universities entry-level cyber analyst skills.
- The project's beneficiaries include numerous municipalities that depend on PISCES for cybersecurity due to their limited cyber monitoring, investigation, and response resources.
- In the event of a failure, the absence of a failover in the system leaves these entities vulnerable.

**Elastic**
- PISCES uses ELK (Elastic Search, Logstash, and Kibana) for real-time data logging, queries, and visualization.
- Beats ships lightweight metadata to the stack.
- Implementing Elastic’s Cross-Cluster Replication (CCR) as the failover mechanism ensures continuous operation.

**Stack Features**
- PISCES integrates ELK into their network stack for dynamic logging, monitoring, and analytics.
- Students access stack’s private network through OpenVPN.
- Proxmox is the network manager interface to communicate with the clusters and nodes.
- Suricata and the firewall used for intrusion detection system.
- Incorporates access controls, authentication mechanisms, and data encryption as security measures.
- Leverages Elastic’s Cross-Cluster Replication (CCR) and round-robin DNS for efficient failover.

**Backup Server**
- The backup servers provide resilience to the PISCES platform.
- In the event of a failure of the primary server located in Poulsbo, WA, the backup servers located at the University of Montana assume it’s workload.
- It is designed to maintain synchronization with the primary server.

**Local Cluster**
- Local cluster is the Elastic term to refer to backup servers, remote cluster refers to PISCES primary infrastructure.
- Unidirectional Cross-Cluster Replication is utilized to replicate data from the remote cluster to the local cluster in near real-time, failover in the event of a failure, and fallback once the primary is operational.
- As the backup infrastructure at the University of Montana has yet to be built, we simulated our implementation using virtual machines within the Cyber Range Poulsbo.

**Cross-Cluster Replication**
- Proxmox enables us to configure the remote and local clusters within the console to initialize CCR within the YML files serving as configuration files for Elastic.
- Primary and backup servers running Elastic are able to recognize each other and assume specific roles to ensure replication and continuous operation.
- Current PISCES cluster is dedicated to leader indices and new backup cluster for follower indices.
- An auto-follow pattern replicates data from leader to follower.
- If an outage occurs, backup cluster assumes the roles and the collectors begin to forward data to it.
- Once operational, the PISCES cluster should first replicate data then assume its roles back.

**Data Streams**
- Stack ingests metadata forwarded from collectors within the municipalities network.
- Students can then access data and try to detect malicious activity.
- Data streams must be redirected to backup servers domain in the event of an outage.
- Round-robin DNS used to substitute the backup servers’ domain name when a failure is detected by the system, ensuring continuous logging of data.

**Future Work, References, and Acknowledgments**
- Upgrade Elastic package for more features.
- Write scripts to handle the transfer of data streams.
- Configure OpenVPN to allow students to access backup.

---

**Fig 1:** An Overview of Data Flow from Collection to Visualization

**Fig 2:** Aggregating Logs from Multiple Applications for ElasticSearch

**Fig 3:** Setup, Failover, and Failback Process

**Fig 4:** Setting Up Auto Follow Patterns for Cross-Cluster Replication

**Fig 5:** Setting Up Auto Follow Patterns for Cross-Cluster Replication in Elasticsearch

---

**Industry Mentors:** Mike Hamilton, Deborah Wells, Dillion Kierce
**Faculty Mentors:** Radha Poovendran & Kavya Balsubmaranian
**Sponsors:** PISCES & BECU