12/7/2025

PISCES Cybersecurity Client Report

Recommendations and Observations

Client Recommendations, Group Assignment

Team: David Holmes, Getahun Lode, Jaiden Jongjitirat, and Samuel Teklu
Clients: Burien, East-Sammamish-Water, Kittitas, and Stevens-PUD
Instructor: Heather Johnson
School: Highline College



PISCES

A# Solutions LLC
Website Portfolio

Table of Contents:

Executive Summary: 3

Below provides severity 1 hits found over the 2025 Fall Quarter 4

Client Mantis Overall Ticket System Breakdowns: 5

Client Ticket Severity Graphs: 6

Burien: 6

Stevens-PUD 7

Overall Client Tickets Comparison: 7

Wiki Resource Client City Overview: 7

Scanning and External Threat Activity Overview: 8

Notable Findings: 9

1. Blocklisted IP Targeting Memcached (Port 11211) 9

2. Blocklisted IP Allowed Communication Over Port 443 9

3. Repeated Malicious IP Activity from 65.49.1.102 9

4. High Internal Traffic Volume Between 10.21.1.145 → 10.1.14.12 9

5. Suricata STREAM ESTABLISHED "Packet Out of Window" 10

6. Internal Python Script Making Outbound HTTP Requests 10

Stevens-PUD: 10

1. Attempted phishing/credential theft 10

2. Telemetry traffic is triggering Suricata alerts 11

Other Unresolved/Outstanding Tickets: 11

Open Ticket per Clients: 11

Burien: 11

East-Sammamish-Water: 11

Kittitas: 11

Stevens-PUD: 11

Advisories on Issues Outside Organizational Control: 12

Probing and Reconnaissance 12

Email Spam and Phishing Campaigns 12

PISCES Client-Wide Threat Advisories 12

Threat Environment Overview: 12

Current Regional Threat Trends: 12

Observed Threat Actor Behavior: 13

A# Solutions LLC Website Portfolio

Client Specific Stevens-PUD and East-Sammamish-Water 13
Recommendations for Remediation and Best Practices: 13
General Best Practices for All Clients: 13
Observed Network Recommendations for All Clients: 14
Conclusion: 17
Glossary of Cybersecurity Terms: 18
Works Cited: 20
PISCES Suricata Monitoring Platform — Washington 20

A# Solutions LLC
Website Portfolio

Executive Summary:

This PISCES multi-client cybersecurity assessment provides an overview of the security posture, operational activity, and observed threat behaviors affecting the cities and utilities of Burien, East-Sammamish-Water, Kittitas, and Stevens-PUD during the Fall Quarter period of September–December 2025. The analysis includes ticket system performance, external threat activity, internal network anomalies, notable findings, and prioritized recommendations for improving security across all organizations.

Overall, the project regions experienced steady background scanning and low-severity external threat activity, along with several internal events requiring further validation. Client ticket resolution rates remained strong. We saw that most of the issues were closed and high overall responsiveness. However, several open and "won't-fix" tickets indicate potential gaps in long-term remediation.

Across all clients, the report identified repeated attempts from blocklisted IP addresses, where some were actually allowed through firewall controls. Internal anomalies, such as high-volume traffic between internal hosts and script-based outbound HTTP requests, were detected and require verification to rule out misconfiguration or unauthorized activities. Suricata alerts, many related to stream-based inspection, produced false positives, indicating a need for improved IDS tuning and rule sets.

Stevens-PUD exhibited additional risk due to phishing-related activity and traffic patterns associated with malicious infrastructure. Cases of benign mobile app telemetry also triggered Suricata alerts, further highlighting the need for refined rule sets to reduce noise and improve detection fidelity.

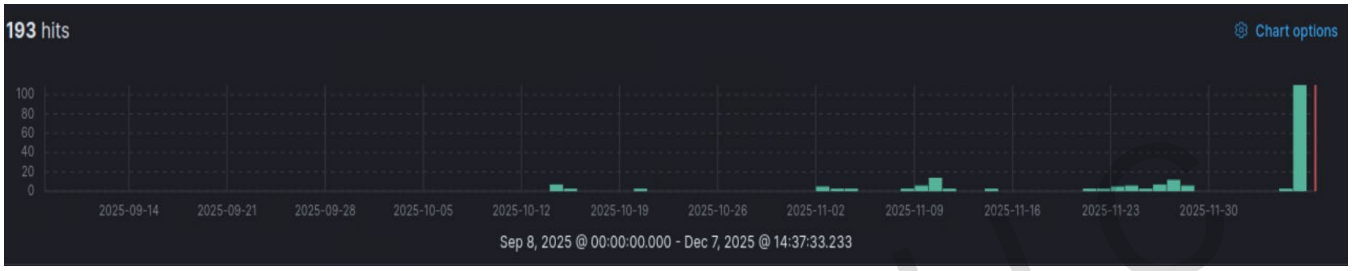
Region-wide, threat trends included increased scanning of exposed services, credential-stuffing attempts, and multiple phishing campaigns, some consistent with activity previously linked to Russian-aligned threat groups targeting water utilities, such as CyberArmyOfRussia_Reborn (CARR) and Sandworm/APT44. Although no evidence indicates successful compromise, these trends underscore the importance of strong email security, firewall hardening, and multi-factor authentication measures.

Overall, this assessment concludes that while there were no indications of critical breaches across any client environments, firewall rule consistency, internal traffic validation, IDS tuning, and updated network topology documentation are needed to strengthen each networks end resistance. Continued patching, monitoring, and user training remain essential to maintaining any government secure and operational environment.

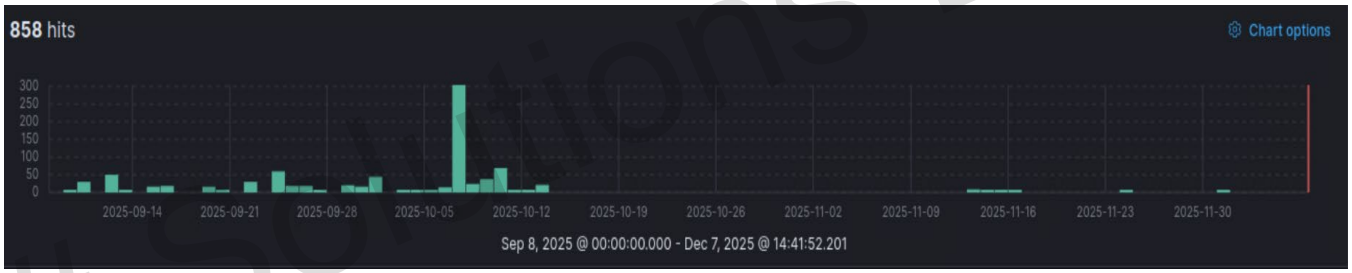
Aff Solutions LLC Website Portfolio

Below provides severity 1 hits found over the 2025 Fall Quarter

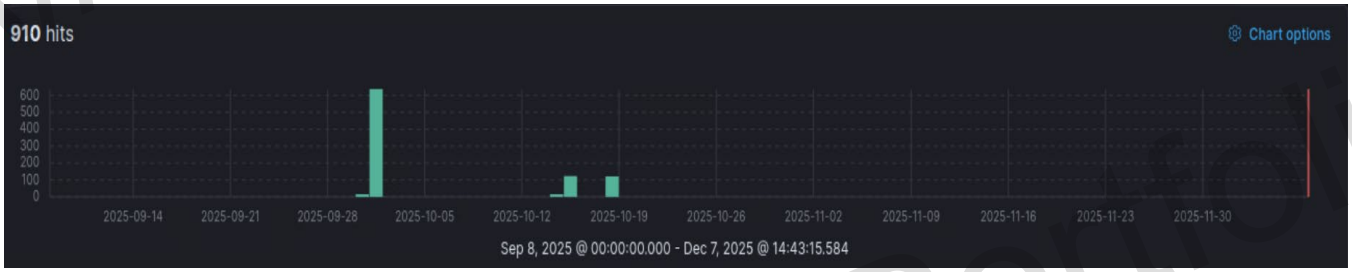
Burien: (193 hits)



East-Sammamish-Water: (858 hits)



Kittitas: (910 hits)



Stevens-PUD: (0 - No hits)

No Alert Severity 1 hit – No graph.

A# Solutions LLC Website Portfolio

Client Mantis Overall Ticket System Breakdowns:

Basic Mantis system review of each client's individual ticket reporting severity and resolution statistics. Each client exhibited different resolution challenges and internal cybersecurity personnel training. Not all tickets have been closed and some individual clients possess tickets open for greater than 4 years.

Client Ticket Status	open	resolved	closed	total	resolved ratio	ratio
Burien	2	69	66	71	97.18%	100.00%
East-Sammamish-Water	2	29	29	31	93.55%	100.00%
Kittitas	2	3	3	5	60.00%	100.00%
Stevens-PUD	4	40	39	44	90.91%	100.00%

* Burien has 3 tickets resolved but listed as Burien won't fix.

Ticket Severity	trivial	tweak	minor	major	block
Burien	-	1	52	18	-
East-Sammamish-Water	-	-	26	4	-
Kittitas	-	-	12	-	-
Stevens-PUD	-	-	38	3	-

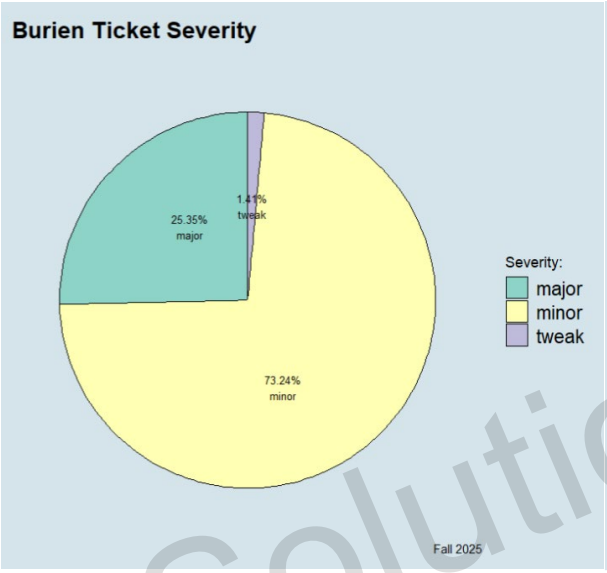
Average Response/Resolution Times	In Days
Burien	5.01
East-Sammamish-Water	2.21
Kittitas	2.58
Stevens-PUD	4

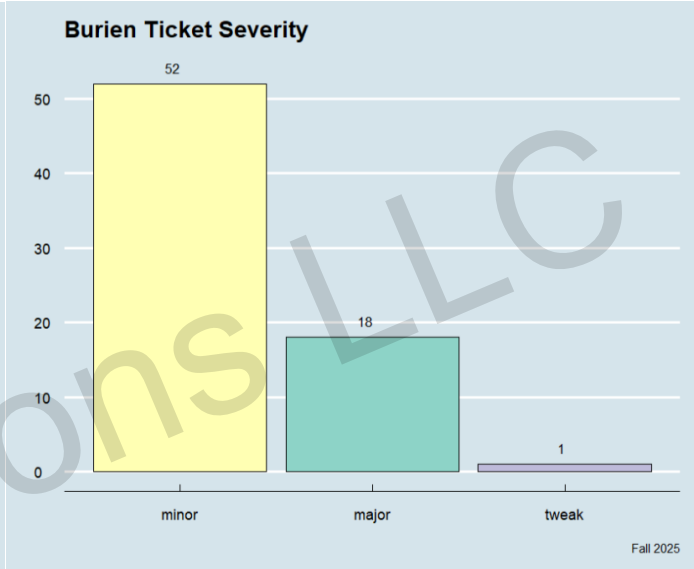
Top Four Colleges 2025 Tickets	open	resolved	closed	total	resolved ratio	ratio
Bellevue College	10	20	6	36	72.20%	0.40%
Central Washington University	11	105	719	835	98.70%	8.70%
Greenriver Community College	7	110	15	132	94.70%	1.40%
Highline College	**4**	**173**	**4**	**181**	**97.80%**	**1.90%**

A# Solutions LLC Website Portfolio

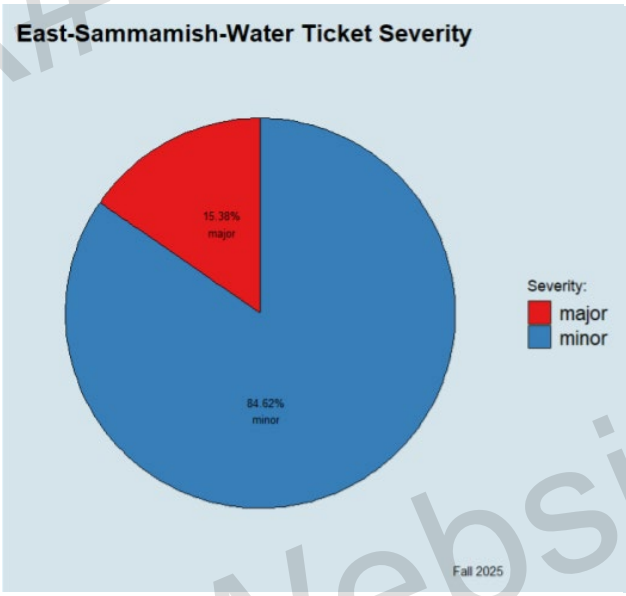
Client Ticket Severity Graphs:

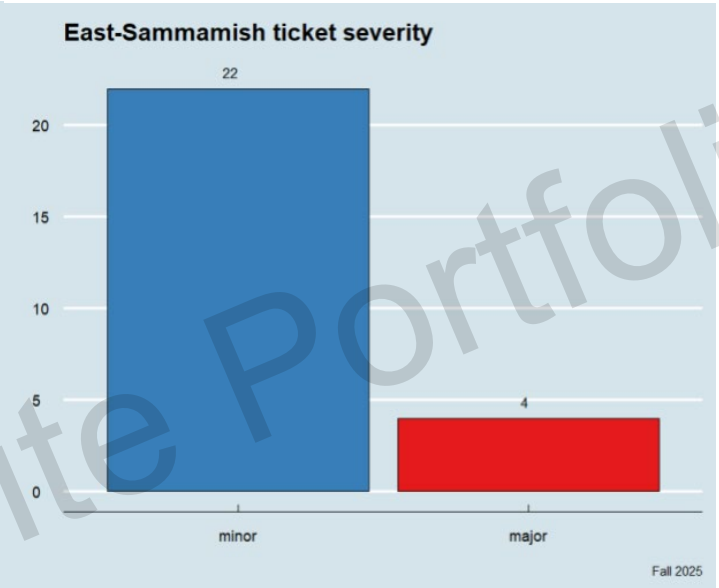
Burien:





East-Sammamish-Water:





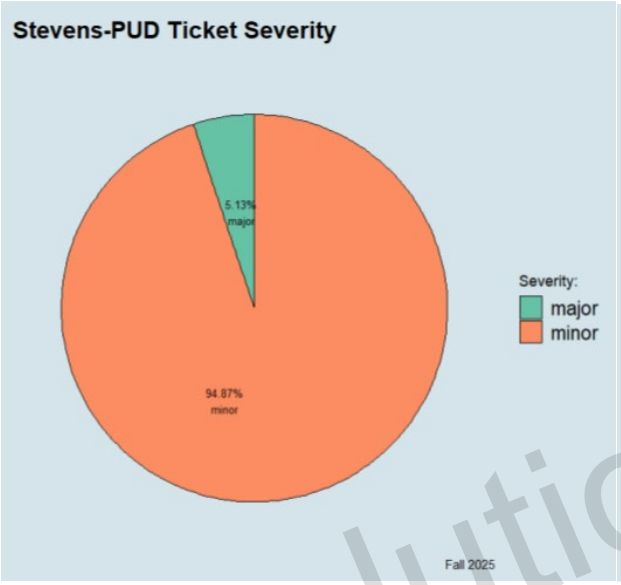
Doesn't take into account the 2 reopened tickets and 2 from May 2025

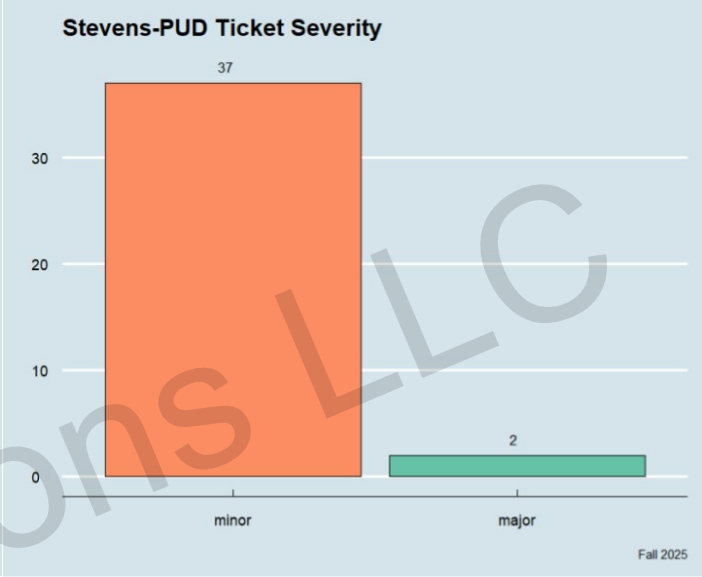
Kittitas:

No real graph due to only 22 minor ticket issues

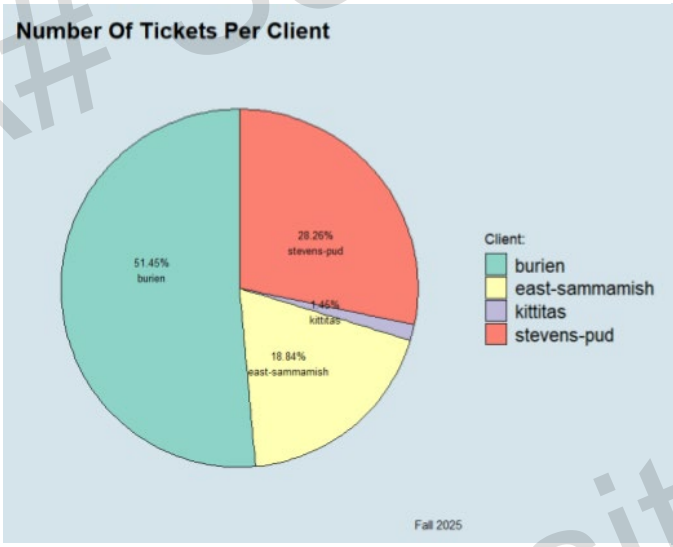
A# Solutions LLC Website Portfolio

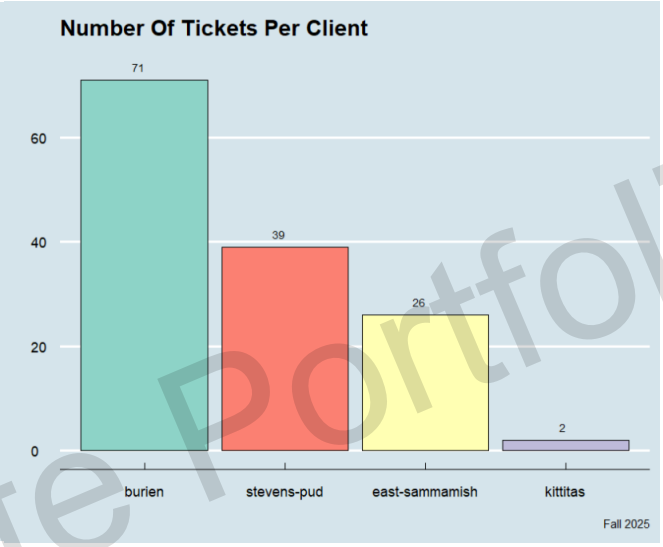
Stevens-PUD:





Overall Client Tickets Comparison:





Wiki Resource Client City Overview:

Burien: Last city tickets reported in 31Jan2022 – all closed. City Network Topology present and with DNS Server information.

Kittitas: Last city tickets reported in 11Nov2021 – one remains open. No City Network Topology of any other current information. Provide one false positive issue from 5 years ago.

East-Sammamish-Water and Stevens-PUD: No data available for PUD or Water districts.

A# Solutions LLC Website Portfolio

Scanning and External Threat Activity Overview:

Summary of external scanning results and threat exposure across all clients.

TICKET / ALERT	SUMMARY	IP ADDRESS	PORT
Blocklisted Source	External IP attempted to contact internal Memcached service	src=64.62.156.91 → dest=[internal]	11211
Blocklisted Source Allowed	External IP on DShield list allowed to connect over HTTPS	src=147.185.132.210 → internal	443
Blocklisted Source	Another malicious source IP observed	src=65.49.1.102	N/A
High-Volume Internal Traffic	Internal system sent >500,000 packets to another internal host	10.21.1.145 → 10.1.14.12	N/A
Script-Based HTTP Traffic	Internal host used Python-urllib/3.10 to perform HTTP GET to Google IP	192.168.2.120 → 142.250.73.132	80
Suricata Stream Alert	"STREAM ESTABLISHED packet out of window"	Internal ↔ Internal	N/A

A# Solutions LLC
Website Portfolio

Notable Findings:

Key vulnerabilities, misconfigurations, and exploit attempts discovered for each client.

1. Blocklisted IP Targeting Memcached (Port 11211)

Traffic from 64.62.156.91, a known malicious source, attempted to communicate with an internal system via port 11211, typically used by Memcached. Attackers commonly scan for misconfigured Memcached instances to exploit for amplification DDoS attacks or to enumerate open services.

2. Blocklisted IP Allowed Communication Over Port 443

A second blocklisted source, 147.185.132.210, attempted to reach internal systems via HTTPS.

The traffic was permitted through, suggesting:

- Firewall rules allow broader external access than necessary
- DShield blocklists are not consistently enforced
- A "default allow" outbound policy may be in place

While the Suricata alert for this event appears to be a false positive, allowing traffic from known malicious IPs is a policy concern.

3. Repeated Malicious IP Activity from 65.49.1.102

Additional communication attempts from a third DShield-flagged IP confirm that the organization is exposed to continuous global scanning, consistent with normal background internet noise, but still valuable for tuning rules.

4. High Internal Traffic Volume Between 10.21.1.145 → 10.1.14.12

Over 500,000 packets were transmitted between two internal hosts within ~22 minutes. This may indicate:

- Backup or replication jobs
- Misconfigured service
- Accidental loop
- Possible internal data movement that should be validated

This traffic is not necessarily malicious but warrants verification.

A# Solutions LLC Website Portfolio

5. Suricata STREAM ESTABLISHED "Packet Out of Window"

This alert is generally associated with:

- Packet retransmission
- Reordering
- Asymmetric routing

Most cases are **false positives**, but repeated occurrences may indicate a network configuration issue.

6. Internal Python Script Making Outbound HTTP Requests

Host 192.168.2.120 made an HTTP GET request to a Google-owned IP using: Python-urllib/3.10

Possible explanations:

- Scheduled automation
- Administrative script
- Misconfigured testing script
- Unauthorized or unintended internal scripting
- Early-stage malware beacon (if unexpected)

Verification with internal IT is recommended.

Stevens-PUD:

1. Attempted phishing/credential theft

Traffic from two internal devices shows connections to an IP address (199.36.158.100) that has been previously reported for phishing activity and hosting a credential stealing website. As Alexis Cole suggested in their ticket (#0010711), blocking the following malicious URLs can help mitigate threats from this source:

- scotiabank-chat[.]web[.]app[.]
- clone-c2da3[.]web[.]app[.]
- feedinfo-check-do-sys[.]web[.]app[.]
- cancaquiaj47pago8[.]web[.]app[.]
- ect-rollout-maps[.]web[.]app[.]
- annoter-812f6[.]web[.]app[.]

A# Solutions LLC Website Portfolio

2. **Telemetry traffic is triggering Suricata alerts**

   Network traffic from the iHeartRadio mobile app (Android) triggered Suricata alerts for a JA3 fingerprint associated with a known signature (Trojan.AndroidOS.jocker.snt). This activity is benign telemetry traffic that only resembles known threat patterns, however, refining Suricata rules to avoid triggering alerts for known or trusted IP's/services can reduce false positives. (#0010919)

Other Unresolved/Outstanding Tickets:

- Several Suricata alerts require additional validation to determine whether they represent benign retransmissions or misconfigured routing.
- Multiple Burien tickets labeled as 'Won't Fix': Ticket #'s 0011278, 0011294, 0011304. Additional eyes may allow further fix implementation assistance in completing full system resolution.
- High-volume internal traffic has not yet been confirmed as expected behavior from system administrators.
- Blocklisted external IP traffic continues to be allowed in some cases, suggesting firewall or rule tuning gaps.

Open Ticket per Clients:

Burien:

Ticket 0010969 - Suspicious outbound DNS activity – submitted 18Nov25 19:39

East-Sammamish-Water:

Ticket 0010243 – Fraud Risk – submitted 28May25
Ticket 0010243 – Malware – Malicious – submitted 13May25

Kittitas:

Ticket 0009977 - ET JA3 Hash - Trojan.AndroidOS.Jocker.snt 1 – submitted 06May25
Ticket 0009992 - URICATA UDPv4 invalid checksum/possible malware injection attempt – submitted 08May25

Stevens-PUD:

Ticket 0009977 - SURICATA UDPv4 invalid checksum – submitted 13May25
Ticket 0009977 - Self-signed SSL Certificate Flagged as Malicious – submitted 17May25
Ticket 0010029 - ET INFO Splashtop Domain in DNS Lookup (splashtop .com) – submitted 21May25

A# Solutions LLC Website Portfolio

Advisories on Issues Outside Organizational Control:

Items such as probing, spam, and external threat activity that cannot be remediated internally.

Probing and Reconnaissance

- Regular port scanning observed from global botnets
- Credential stuffing attempts using previously leaked credentials
- Web application reconnaissance activity
  Recommendation: Enable rate limiting, MFA, and geo-blocking as appropriate.

Email Spam and Phishing Campaigns

- Increase in spoofed email attempts

PISCES Client-Wide Threat Advisories

(Ticket – Description)

0011265 - Timestamp was november,1,11:57. The host IP is ipv4 and ipv6.At the moment the alert was just logged.
0010405 - Dashboard Armory and other useful searches you want to share
0010050 - Suspicious: ET INFO PE EXE or DLL Windows file download HTTP (Potential Corporate Privacy Violation)
0010004 - Likely Malicious Reconnaissance: ET SCAN Zmap User-Agent (Inbound) (Detection of a Network Scan)
0009957 - ET EXPLOIT Apache HTTP Server 2.4.49 - Path Traversal Attempt (CVE-2021-41773) M2 (Attempted Administrator Privilege Gain)

0010139 - ET SCAN MS Terminal Server Traffic on Non-standard Port (Attempted Information Leak)

0009756 - Scanner/Malware - attempting from multiple IPs
0009979 - ET SCAN JAWS Webserver Unauthenticated Shell Command Execution (Web Application Attack)
0010297 - ET SCAN Zmap User-Agent (Inbound) (Detection of a Network Scan)

0010085 - GPL WEB_SERVER printenv access (access to a potentially vulnerable web application)

Threat Environment Overview:

Summary of broad threat trends observed across all organizations.

Current Regional Threat Trends:

- Increased activity from financially motivated threat groups
- High ransomware activity targeting SMEs
- Localized phishing campaigns using regional branding

AF Solutions LLC Website Portfolio

- Repeated communication attempts from blocklisted malicious IPs
- Possible reconnaissance or scanning activity
- Phishing and state-sponsored reconnaissance
- False positives from Suricata stream-based signatures
- Unusual internal traffic behavior and script-based outbound connections

Observed Threat Actor Behavior:

- Automated scanners probing exposed services
- Botnets attempting brute-force login and Botnet-origin traffic probing internal hosts
- Opportunistic exploitation of old vulnerabilities
- Attempts to connect to web-facing services on HTTPS (Port 443
- Regular inbound scanning activity (Zmap, reconnaissance sweeps)

Client Specific Stevens-PUD and East-Sammamish-Water:

CyberArmyofRussia_Reborn (CARR) and Sandworm (APT44) are two groups known to have targeted water districts in the United States. Here are some links showing this:

- Rural Texas towns report cyberattacks that caused one water system to overflow | AP News
- Hackers Linked to Russia's Military Claim Credit for Sabotaging US Water Utilities | WIRED
- Sanctioning Members of the Cyber Army of Russia Reborn - United States Department of State

Sandworm/APT44 is known to use third party email management software to run their phishing attacks (T1583). Furthermore, they have previously registered domain names and created URLs made to appear as legitimate websites (T1583.001) and leased servers from resellers instead of going through a hosting company (T1583.004) to set up infrastructure for their phishing campaigns.

Recommendations for Remediation and Best Practices:

General Best Practices for All Clients:

- Maintain a 30-day patching cycle.
- Require MFA for email and VPN.
- Implement strong password policies and continuous monitoring.

A# Solutions LLC Website Portfolio

- Maintain offline backups and test them regularly.
- Deploy endpoint detection and response (EDR).
- Maintain current Firewalls, IDS, VPN endpoints.
- Provide critical SCADA/monitoring systems.
- Maintain full logging and submit to SIEM for correlation.

Observed Network Recommendations for All Clients:

1. Harden Firewall and Blocklist Enforcement
    a. Enforce strict blocking of all DShield-listed and other reputation-based threat IPs.
    b. Implement a default-deny inbound policy with explicit allow rules.
    c. Review HTTPS inbound access rules and reduce them to only necessary public-facing services.
    d. Restrict Port 443 access to only necessary endpoints.
    e. Implement default-deny inbound and default-allow outbound with logging.

2. Investigate the Single Block-Level Incidents - Identify
    a. Which internal host received the traffic
    b. Whether the attempted connection targeted a sensitive service
    c. Whether service should be exposed at all
    d. If scanning or exploitation attempts targeted deprecated services, disable them immediately.

3. Review Internal High-Volume Traffic
    a. Verify whether 10.21.1.145 → 10.1.14.12 traffic corresponds to backup or replication tasks.
    b. If not expected, investigate for misconfigured services or possible data exfiltration attempts.
    c. Add rate and anomaly alerting for large internal transfers.

4. Validate Internal Script Usage
    a. Confirm whether Python-based HTTP traffic is legitimate automation.
    b. If not authorized, disable the script and scan host 192.168.2.120 for malware or unauthorized tools.
    c. Require internal scripting tools to use identifiable user-agents.

5. Tune Suricata and Logging Rules

A# Solutions LLC Website Portfolio

a. Reduce noise from recurring stream-based false positives.
b. Enhance signatures for scanning activity to better distinguish benign vs. malicious behavior.
c. Ensure proper packet capture and retention for at least 30–90 days.

6. Improve Monitoring of Exposed Services
    a. Confirm that no Memcached services are exposed externally.
    b. Regularly scan internal network ranges to identify open services on sensitive ports.
    c. Segment traffic where possible to limit reconnaissance from compromised internal hosts.
7. Strengthen Email and Administrative Security
    a. Enable MFA for admin logins.
    b. Email authentication (DMARC, DKIM, SPF)
    c. Apply conditional access policies for remote administrative access.
    d. Provide phishing reporting training, as utilities are common targets.
8. Advisory Items (Cannot Be Fully Prevented)
    a. Inbound internet scanning from global botnets
    b. Credential-stuffing attempts using leaked credentials
    c. Randomized probing of HTTPS and SSH ports
    d. Spoofed email phishing attempts

- Recommended mitigations:
    - Rate limiting
    - MFA everywhere possible
    - Geo-blocking for unused regions

9. Migrate Resolved fixes
    a. Continue to implement known ticket fixes keeping a resolution database to assist in future issues resolution.
    b. Resolving all completed fixes removes potential exposer and known system issues.
    c. Revisit any open or on resolved ticket they be over looked or forgotten.

10. Close Open Tickets
    a. Unresolve tickets may equate to ticking time bombs. Due diligence can be the easiest form of cybersecurity and network protection.

A# Solutions LLC Website Portfolio

b. Completing ticket issues in the most effective and time sensitive manor will server each client with stronger form of overall security and peace of mind.

11. Reduce Ticket System Complacency Factor
    a. Ensure all tickets are properly review and action taken with full attention and resolve.
    b. Avoid allowing the overwhelming ticket flow from pushing for quick resolutions that may not fully resolve ticket issues.
    c. Look for tickets using camouflage measure to avoid detection.
    d. Not all simple tickets should be dismissed.
    e. Not all outside scans may be from CISA approved scans.

12. Better Network Topology Information
    a. The lack of network topology allows for additional and uncertain tickets that could be removed with basic system information.
    b. This would allow for better overall ticket submission and recommendation
    c. The more information a student has to diagnose a problem the more experience can be gained on all ends of the spectrum.
    d. Without current topology information, it is difficult to validate whether exposed ports, services, or IPs are intentional.
    e. This may allow more misconfigured firewall rules, unknown or forgotten services still reachable externally, and inconsistent IDS alert tuning.

A# Solutions LLC
Website Portfolio

Conclusion:

This multi-client cybersecurity review highlights common vulnerabilities, unique threats to each organization, and opportunities to strengthen overall defenses practices. While some external threats (probing, spam, widespread scanning) cannot be eliminated, proactive security measures will significantly reduce each client's risk and ultimate exposure.

Overall, the region experienced a consistent pattern of low-severity external scanning, minor false positives, many known Malware – Malicious threat actors, and a few internal events that require validation. No critical threats appear to have gained access to any of the client systems. However, the repeated presence of blocklisted IPs and the existence of unintended internal script traffic highlight areas in need of improvement.

Continued attention should focus on:

- Firewall hardening
- Reviewing internal anomalous traffic
- Tuning IDS noise
- Verifying that internal tools and scripts are authorized and documented

Like many PISCES regions, recurring scans and attempts from malicious IPs are normal and expected, but internal visibility and proper filtering remain essential for maintaining security posture.

Continuing regular vulnerability assessments, patching, user training, and monitoring will maintain a strong security posture and help mitigate future threats.

A# Solutions LLC
Website Portfolio

Glossary of Cybersecurity Terms:

APT44 / Sandworm: A Russia-linked cyber threat group tracked by MITRE ATT&CK as Sandworm Team. It is associated with Russia's military intelligence organization, the GRU.

Blocklisted IP: An IP address identified by a threat-intelligence or reputation service as associated with suspicious or malicious activity.

CARR: Cyber Army of Russia Reborn, a pro-Russia hacktivist group associated in reporting with attacks against critical infrastructure, including water utilities.

Credential Stuffing: An automated attack that tests previously exposed username and password combinations against other services.

CVE: Common Vulnerabilities and Exposures; a standardized identifier used for publicly known cybersecurity vulnerabilities.

DShield: A SANS Internet Storm Center threat-intelligence service that collects attack reports and provides reputation/blocklist information.

DMARC: Domain-based Message Authentication, Reporting, and Conformance; an email-authentication policy that builds on SPF and DKIM.

DKIM: DomainKeys Identified Mail; an email-authentication mechanism that uses cryptographic signatures to help verify message authorization.

EDR: Endpoint Detection and Response; technology that monitors endpoints and supports detection, investigation, and response.

False Positive: A security alert that identifies legitimate activity as suspicious or malicious.

Firewall: A security control that permits or denies network traffic according to configured security rules.

HTTPS: Hypertext Transfer Protocol Secure; encrypted web communication using TLS.

ICS: Industrial Control System; hardware and software used to monitor or control industrial processes.

IDS: Intrusion Detection System; technology that monitors activity and generates alerts when traffic or behavior matches detection rules.

IPS: Intrusion Prevention System; a security control capable of detecting and actively blocking malicious network activity.

JA3: A TLS client fingerprinting technique used to characterize clients based on properties of their TLS handshake.

Mantis: The ticket-management system referenced in the report for tracking client security issues, severity, status, and resolution.

Memcached: A distributed in-memory caching system commonly associated with network port 11211; exposed or misconfigured instances can create security risks.

MFA: Multi-Factor Authentication; authentication requiring two or more distinct authentication factors.

Network Reconnaissance: The process of discovering hosts, services, ports, vulnerabilities, or other information about a target network.

A# Solutions LLC Website Portfolio

OT: Operational Technology; hardware and software that monitors or controls physical processes and equipment.

PISCES: Public Infrastructure Security Cyber Education System; a program that provides supervised cybersecurity analysis experience using live network metadata from public-sector partners.

SCADA: Supervisory Control and Data Acquisition; systems used to monitor and control geographically distributed processes and equipment.

SIEM: Security Information and Event Management; technology that collects, correlates, analyzes, and retains security logs and events.

SPF: Sender Policy Framework; an email-authentication mechanism identifying authorized mail servers for a domain.

Suricata: An open-source network IDS, IPS, and network-security-monitoring engine. In the PISCES environment, Suricata is used in network collectors to generate intrusion-detection alerts.

Telemetry: Data generated by an application, device, or service for monitoring, analytics, diagnostics, or operational purposes.

Threat Intelligence: Information about threats, threat actors, indicators, tactics, techniques, and procedures used to support security decisions.

UDP: User Datagram Protocol; a connectionless transport protocol that does not provide TCP's delivery and sequencing guarantees.

Vulnerability: A weakness in software, hardware, configuration, process, or architecture that could be exploited to affect confidentiality, integrity, or availability.

Water/Wastewater Sector: Critical infrastructure organizations responsible for producing, treating, distributing, or managing drinking water and wastewater services.

A# Solutions LLC
Website Portfolio

Works Cited:

MITRE. *Common vulnerabilities and Exposures (CVE)*. n.d. The MITRE Corporation. Website. 2025. <www.cve.org>.

The MITRE Corporation. *MITRE ATT&CK Framework*. Vers. V19. n.d. MITRE. Electronic. 2025. <https://attack.mitre.org/>.

MITRE. "Sandworm Team (G0034)." MITRE ATT&CK, https://attack.mitre.org/groups/G0034/. Accessed 25 Aug. 2026.

Associated Press. "Rural Texas Towns Report Cyberattacks That Caused One Water System to Overflow." AP News, 18 Apr. 2024, https://apnews.com/article/texas-muleshoe-water-systems-cyberattacks-russia-5f388bf0d581fc8eb94b1190a7f29c3a. Accessed 5 Dec. 2025

Greenberg, Andy. "Hackers Linked to Russia's Military Claim Credit for Sabotaging US Water Utilities." WIRED, 17 Apr. 2024, https://www.wired.com/story/cyber-army-of-russia-reborn-sandworm-us-cyberattacks/. Accessed 5 Dec. 2025

Open Information Security Foundation. "Suricata." Suricata Documentation, https://docs.suricata.io/. Accessed 5 Dec. 2025.

OpenAI. *ChatGPT*, GPT-5.1, 7 Dec. 2025, https://chatgpt.com/. Research organization, source integration, MLA formatting, and glossary development".

Cybersecurity and Infrastructure Security Agency. "Defending OT Operations against Ongoing Pro-Russia Hacktivist Activity." CISA, 1 May 2024, https://www.cisa.gov/news-events/alerts/2024/05/01/cisa-and-partners-release-fact-sheet-defending-ot-operations-against-ongoing-pro-russia-hacktivist. Accessed 3 Dec. 2025.

National Institute of Standards and Technology. "Digital Identity Guidelines: Authentication and Authenticator Management." NIST Special Publication 800-63B, https://pages.nist.gov/800-63-4/sp800-63b.html. Accessed 5 Dec. 2025

SANS Internet Storm Center. "Highly Predictive Blocklist (DShield)." SANS, https://isc.sans.edu/hpbinfo.html. Accessed 3 Dec. 2025.

PISCES Suricata Monitoring Platform — Washington

The Public Infrastructure Security Cyber Education System (PISCES) provides supervised cybersecurity monitoring experience using live network metadata from public-sector community partners. PISCES uses network collectors that include the Suricata intrusion detection system (IDS). The collected data are limited to packet headers and IDS alerts, rather than packet contents. For Washington State, the PISCES monitoring stack is hosted at the Western Washington University Cyber Range in Poulsbo, Washington. PISCES also uses state-level chapters with network isolation and VPN-based access to help protect the monitoring environment. This architecture is directly relevant to the CIS370 report because the group's analysis relied on Suricata alerts and related monitoring data from the PISCES environment.

A# Solutions LLC Website Portfolio