Information Security and Policy (ISP) Monitoring Practices Inventory

Method	Summary	Purpose	Data Examined/Collected; Retention Period	Recommendation*
1. Central Authentication Audit (new)	CalNet login attempts associated with geographic location. Baseline patterns of systems and user authentication behavior	Rule-based alerts for geographically dispersed simultaneous logins and excessive failed logins. Detect anomalies from baseline behavior to identify potential security compromises.	**All** CalNet authentication attempts correlated with geographic location For PL2 (critical) assets and users who access those assets: baseline authentication behavior (patterns) ❖ 1 year retention	Recommend Approval (CISPC, CPO, CISO)
2. Network Flow (Metadata) Reputation Analysis (new)	Which Campus devices communicated with what other devices on or off Campus (like a phone bill).	Traffic addresses correlated with reputational feeds (rapidly changing lists of known sources of cyber attacks).	Metadata on **all** traffic: what computers talk to what computers. Contents of the communication are not inspected or retained. ❖ 1 year retention	Recommend Approval (CISPC, CPO, CISO)
3. Network Intrusion Detection System	Compares traffic content to known malicious patterns	Identify "signatures" of known attack communication patterns.	Only flagged packets (communication fragments triggering malware rules) are collected. ❖ 1 year retention	Recommend Approval (CISPC, CPO, CISO)
4. System/ Application Logs (new correlation)	Collect logs produced by information systems. Logs for PL2 and PL3 (high security impact) systems correlated with other security data.	• Detect compromised devices • Investigate Major Security Incidents	Errors and event logs with user info and possibly application data. ❖ 1 year retention	Recommend Approval (CISPC, CPO, CISO)
5. Network Services and Vulnerabilities (new)	Scan Campus network using a network vulnerability scanning tool such as Nessus, Qualys, etc. Contact	• Identify device vulnerabilities (preventative) • Investigate Major Security Incidents	**Vulnerable device** info and the vulnerability ❖ 1 year retention	Recommend Approval (new use of existing data from patching infrastructure) (CISPC, CPO, CISO)
6. Forensic Data	During breach response memory of the impacted system is copied, and an image of all drives made. If user consent not available, ECP non-consensual access procedures apply.	Breach investigation (determine scope and relevant laws/contractual obligations.)	❖ 1 - 5+ year retention (depending on litigation)	Recommend Approval (long-standing practice) (CISPC, CPO, CISO)
7. Applications/ Versions Used (new source)	Direct feed from patching system of patch status of devices on the Campus network	Breach investigation (determine scope)	IP/mac address, list of software and versions of **systems subscribed to patching infrastructure**. ❖ 1 year retention	Recommend Approval (CISPC, CPO, CISO)
8. DNS query data and DNS RPZ	DNS lookup translates hostnames (typed into the address bar, or	Prevent users from visiting known malicious websites.	Standard ("unfiltered") DNS queries ❖ NOT retained or examined	Recommend Approval as an *alternative choice* to

(Domain Name Service Response Policy Zones) (planned)	clicked web link) into a machine's IP address, which is needed to contact a desired server. An alternative "protected" DNS RPZ (Domain Name Service Response Policy Zones) uses reputational feeds to redirect traffic destined for sites with bad security reputations.		DNS RPZ queries (timestamp, source ip address, requested hostname -- before first single slash) ❖ retained 30 days	unfiltered DNS (CISPC, CPO, CISO)
Method	Summary	Purpose	Data Examined/Collected; Retention Period	Recommendation*
9. Specific protection level 2 data elements in the clear (no plans)	Scan campus traffic for unencrypted social security numbers and credit card numbers.	Detect intentional or unintentional transmission of protected data from campus.	Timestamp, IP header information (protocol, source and destination address and ports), packet and byte count, content monitored as PL2 data. ❖ retained 7 days	Do Not Approve without further specification of procedures (CPO) Recommend Approval (CISPC, CISO)
10. Information about files transmitted on the Campus network (no plans)	Compare hash (algorithmic non-reversible "signature") of files to known malware.	• Incident response • Identifying breach cause	Hash data (not original file) ❖ retained 1 year	Do Not Approve
11. Web browsing data from the Campus network (no plans)	Compare hostnames and URL to reputational feeds.	Determine whether browsers have been exposed to known malware sites, whether browsers are vulnerable to attack, and/or whether browsers have followed links to known phishing sites.	Source and destination info, URL, response code ❖ retained 30 days	Do Not Approve
12. Network traffic feeds to outside commercial partners (no plans)	Provide corporate manufacturer of security appliances with full feed of network border traffic (in exchange for no dollar cost license and hardware to commercial tools).	Facilitate development of effective commercial Intrusion Detection tools		Do Not Approve
13. Email Metadata Collection (no plans)	Collection of email metadata (To/From/Subject Line) when visible traversing the campus network.	Undefined (Possible detection of rudimentary phishing and other basic email hygiene issues)	Email To, From, Subject Line	Do Not Approve

*CISPC: Campus Information Security and Privacy Committee (advisory to IRGC)
CPO: Campus Privacy Officer
CISO: Chief Information Security Officer