A COMPREHENSIVE GUIDE TO CENTRALIZED LOG MANAGEMENT

for SOC Trust Services Criteria (TSC) Compliance

graylog

Most companies in the business-to-business space need to provide customers with assurance over their security controls. Organizations working outside highly regulated industries often engage in System and Organization Controls (SOC) audits to comply with customer third-party risk management requirements. The Association of International Certified Public Accountants (AICPA) sets the audit requirements and processes for SOC audits. Organizations may only engage certified public accountants (CPAs) for these audits, and the reports must follow the AICPA's Statement on Standards for Attestation (SSAE) 18.

When engaging in a SOC audit, auditors use the Trust Services Criteria (TSC) to evaluate an organization's controls. Understanding what the TSC controls are and how centralized log monitoring can help achieve audit objectives can accelerate an organization's compliance readiness.

WHAT ARE THE TRUST SERVICES CRITERIA (TSC)?

Developed by the AICPA's Assurance Services Executive Committee (ASEC), the Trust Services Criteria (TSC) establish the control criteria that auditors use during SOC attestation and consulting engagements. The controls define how auditors evaluate and report on how organizations manage information and system:

- Availability
- Processing integrity
- Confidentiality
- Privacy

In 2022, ASEC updated the 2017 TSC to refocus audits in alignment with evolving digital transformation strategies. While the primary controls remained the same, the revised points of focus intended to support evolving:

- Technology, threat, vulnerability, and risk landscapes
- Privacy cultural expectations and government compliance requirements
- Data management and confidentiality concerns

Additionally, these revisions addressed different privacy compliance requirements for data controllers and data processors.

HOW TSC IS ORGANIZED

TSC aligns with the Committee of Sponsoring Organizations (COSO) Framework's 17 principles, then supplementing COSO principle 12 with additional criteria that address how the entity deploys control activities through policies and procedures that put policies into action.

- These supplemental criteria focus on:
- Logical and physical access controls
- System operations
- Change management
- Risk mitigation

TSC places the 17 COSO principles into the following five buckets known as Trust Services Categories:

- Security
- Availability
- Processing integrity
- Confidentiality
- Privacy

As if that wasn't enough dissection, it also establishes two sets of criteria:

- **Common criteria:** applicable to all five trust services categories
- **Additional criteria:** specific things that apply only within Availability (A), Processing Integrity (PI), Confidentiality (C), and Privacy (P)

WHAT ARE THE COMMON CRITERIA WITHIN THE 17 TSC?

When preparing for a SOC audit, organizations should have basic understanding of the different Common Criteria so that they can begin collecting the appropriate documentation.

CONTROL ENVIRONMENT

This TSC contains five common controls:

- **CC1.1:** The entity demonstrates commitment to integrity and ethical values.
- **CC1.2:** Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
- **CC1.3:** Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives
- **CC1.4:** The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
- **CC1.5:** The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Embedded within these five common controls and their additional points of focus, the TSC establishes requirements around management:

- Setting clear expectations by setting standards of behavior
- Ensuring internal and external workforce members adhere to these
- Assigning responsibilities and reporting structures
- Implementing processes and technologies to achieve compliance
- Providing the financial, staffing, and technologies resources to support compliance
- Communicating performance expectations and incorporating them into performance reviews
- Supplementing board of director expertise on key issues through the use of a subcommittee or consultants
- Considering legal and contractual privacy requirements and objectives
- Ensuring staff have the appropriate skills, including technical competency, to do thi obs and providing training to maintain the skills
- Defining disciplinary actions for workforce members who violate privacy policies or negligently cause a privacy incident

INFORMATION AND COMMUNICATION

This TSC contains three common controls:

- **CC2.1:** The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
- **CC2.2:** The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
- **CC2.3:** The entity communicates with external parties regarding matters affecting the functioning of internal control.

Embedded within these two common controls and their additional points of focus, the TSC establishes requirements around the organization:

- Identifying and capturing relevant internal and external data from information systems
- Documenting internal and external data flows
- Identifying, documenting, and maintaining system components' records across hardware, software, and infrastructure
- Classifying data types
- Collecting and using complete, accurate, current, and valid data
- Identify, documenting, and maintaining physical location records for all assets
- Communicating all objectives, changes to objectives, and internal controls across workforce members and directors so that they can fulfill responsibilities
- Implementing safe communication channels for anonymous or confidential communications, like whistle-blower hotlines
- Ensuring all people responsible for any aspect of system control understand their responsibilities and know how to report failures, incidents, concerns, or other matters
- Implementing employee security and privacy awareness training, including how to report suspected privacy incidents
- Providing and receiving communication with external parties, like customers, shareholders, regulators, and financial analysts
- Communicating relevant third-party assessment information with directors

RISK ASSESSMENT

This TSC contains four common controls:

- **CC3.1:** The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
- **CC3.2:** The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed
- **CC3.3:** The entity considers the potential for fraud in assessing risks to the achievement of objectives.
- **CC3.4:** The entity identifies and assesses changes that could significantly impact the system of internal control.

Embedded within these four common controls and their additional points of focus, the TSC establishes requirements around the organization:

- Analyzing risk and determining acceptable risk levels that reflect operational and financial objectives
- Allocating appropriate resources for achieving objectives
- Complying with external financial and nonfinancial reporting objectives that consider materiality and compliance mandates
- Providing internal reports with accurate and complete information to achieve nonfinancial and financial reporting objectives
- Identifying, analyzing, and assessing internal and external risk factors across all business areas to determine risk response
- Identifying, analyzing, and assessing risks arising from malicious and accidental threats, including those arising from system component vulnerabilities and third-parties
- Identifying, analyzing, and assessing fraud risks arising from internal or external entities, like unauthorized access to assets or inappropriate employee actions
- Assessing the risk impact arising from changes in the external environment, business model, leadership, systems/technology, third-party business relationships, threats, and vulnerabilities

MONITORING ACTIVITIES

This TSC contains two common controls:

- **CC4.1:** The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

- **CC4.2:** The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Embedded within these two common controls and their additional points of focus, the TSC establishes requirements around the organization:

- Implementing and integrating a mix of automated, manual, preventive, and detective risk mitigation controls that respond to the organization's environment, complexity, nature, and operations

- Segregating duties to prevent conflicts of interest and fraud

- Establishing baselines to compare evaluation outcomes against

- Balancing ongoing and separate evaluations that are built into the business and respond to changes in the business model and processes

- Engaging in ongoing and separate risk and control evaluations to determine whether they exist and function as intended

- Engaging in management and board of director results assessment

- Communicating deficiencies to responsible parties, senior management, and board of directors

- Tracking deficiency remediation timeliness

CONTROL ACTIVITIES

This TSC contains three common controls:

- **CC5.1:** The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
- **CC5.2:** The entity also selects and develops general control activities over technology to support the achievement of objectives.
- **CC5.3:** The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Embedded within these three common controls and their additional points of focus, the TSC establishes requirements around the organization:

- Ensuring that controls address and mitigate risks as intended within the context of the organization's environment, complexity, nature and operations
- Evaluating whether the mix of automated, manual, preventive, and detective controls mitigate risks across relevant business processes
- Ensuring controls appropriately segregate duties
- Understanding how business processes, automated control activities, and general technology controls are dependent on and linked to each other
- Selecting, developing, and implementing appropriate control activities across:
    - Technology infrastructure
    - User access
    - Technology development, procurement, and maintenance
- Building control activities into daily business processes and employee activities with policies that communicate expectations and procedures defining appropriate actions
- Holding the appropriate business unit workforce member accountable by assigning responsibility for timely performance and investigation of control activities defined in policies and procedures
- Periodically reviewing policies and procedures to update them as needed

LOGICAL AND PHYSICAL ACCESS CONTROLS

This TSC contains eight common controls:

- **CC6.1:** The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives
- **CC6.2:** Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
- **CC6.3:** The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consid-eration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
- **CC6.4:** The entity restricts physical access to facilities and protected information assets (for example, datacenter facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
- **CC6.5:** The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.
- **CC6.6:** The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
- **CC6.7:** The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
- **CC6.8:** The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

Embedded within these eight common controls and their additional points of focus, the TSC establishes requirements around the organization:

- Identifying, inventorying, classifying, and managing information assets
- Assessing the security of new architectures before implementing them
- Restricting logical access to information assets through access control software, rules sets, and system hardening
- Identifying and authenticating users prior to granting access while determining whether the organization's use case requires additional controls, like multi-factor authentication (MFA)
- Using network segmentation, zero trust architectures, and other isolation techniques as part of the network security strategy
- Identifying, inventorying, documenting, and managing external user and system access at the point of access
- Restricting information asset access by establishing access control rules and configurations based on data sensitivity, port restrictions, access controls, user identification, and digital certificates
- Establishing, documenting, and managing user identification and authentication requirements
- Ensuring registration, authorization, and documentation for al infrastructure and software before granting them network access and disabling access when no one is using them
- Encrypting data at rest, during processing, or in transit and protecting cryptographic keys
- Restricting user access to and use of both personal information and confidential information
- Appropriately creating, reviewing, and terminating access credentials across users, systems, and service accounts
- Implementing processes for creating, modifying, removing, and reviewing access to protected information

- Restricting access to protected information to limit privileges and segregate duties, such as though role-based access controls (RBAC)
- Implementing processes for creating, modifying, removing, and reviewing physical access to protected information
- Implementing processes to recover devices when users no longer need access
- Restricting the activity types allowed through a communication channel
- Protecting credentials during transmission
- Requiring additional authentication for access request from outside the organization's network
- Configuring, implementing, and maintaining protections like firewalls, demilitarized zones, intrusion detection or prevention systems, endpoint detection and response systems
- Implementing processes and technologies that reduce data loss by restricting data transmission, movement, and removal
- Implementing encryption and physical asset protections for removable media
- Implementing endpoint protection processes and controls across mobile devices, laptops, desktops, and sensors
- Ensuring only authorized users can install and modify applications and software while monitoring for any unauthorized software or configuration changes
- Defining change control processes for software implementation
- Configuring, implementing, and maintaining antivirus and anti-malware software across servers and endpoint devices

SYSTEM OPERATIONS

This TSC contains five common controls:

- **CC7.1:** To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
- **CC7.2:** The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
- **CC7.3:** The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.
- **CC7.4**: The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.
- **CC7.5:** The entity identifies, develops, and implements activities to recover from identified security incidents.

Embedded within these five common controls and their additional points of focus, the TSC establishes requirements around the organization:

- Defining configuration standards and baselines
- Monitoring that infrastructure and software complies with baselines, including identifying unknown or unauthorized components and vulnerability scanning
- Implementing alerts that identify unauthorized modifications to critical system, configuration, or content files

- Implementing policies, procedures, and technologies to identify anomalous infrastructure, software, and system activity
- Designing detections to identify and implementing processes for analyzing anomalies to identify security incidents arising from:
    - Physical barrier compromise
    - Unauthorized actions of authorized personnel
    - Use of compromised credentials
    - External unauthorized access
    - Compromised, authorized external parties
    - Unauthorized hardware/software implemented or connected
- Monitoring detection tools' effectiveness
- Developing and implementing procedures for responding to, communicating, and analyzing security incidents
- Assigning roles and responsibilities for incident response plan's design, implementation, maintenance, and execution

- Implementing procedures for:
  - Containing security incidents
  - Mitigating ongoing security incident's effect
  - Ending threats through vulnerability closure, unauthorized access removal, or other actions
  - Data and business operations restoration
  - Security incident communications, including affected party notifications and management reports documenting the incident, recovery actions, and future prevention steps
  - Restoring the affected environment through system rebuilding, software updates, patch installation, or configuration changes
  - Determining root cause
  - Changing preventive and detective controls as necessary
  - Analyzing incident response plan and procedures to identify areas of improvement
  - Periodic management incident reviews
- Determining appropriate response time-frame and containment approach execution based on the incident's nature and severity
- Implementing and documenting vulnerability remediation activities
- Testing and revising the incident recovery plan with scenarios that consider system criticality and key personnel unavailability

CHANGE MANAGEMENT

This TSC contains one common control:

- **CC8.1:** The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

Embedded within this common control and its additional points of focus, the TSC establishes requirements around the organization:

- Creating and maintaining baselines configurations
- Implementing a change management process across system and component life cycles that includes change:
    - Authorization before development
    - Design and development
    - Documentation, including maintenance and user support
    - Tracking before implementation
    - Approved configurations
    - Testing before implementation
    - Approval before implementation
    - Deployment
- Identifying incident remediation changes to infrastructure, data, software, and procedures and initiating the change process along with them
- Implementing an emergency change management process

RISK MITIGATION

This TSC contains two common controls:

- **CC9.1:** The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
- **CC9.2:** The entity assesses and manages risks associated with vendors and business partners.

Embedded within these five common controls and their additional points of focus, the TSC establishes requirements around the organization:

- Developing and implementing policies, procedures, communications, and alternative processing solutions to mitigate business disruption arising from security incidents
- Considering insurance as a way to offset financial impact
- Implementing vendor and business partner risk management policies, procedures, and monitoring that include:
    - Assessing risks
    - Assigning responsibility and accountability for risk management
    - Communicating and resolving issues
    - Handling exceptions
    - Assessing performance
    - Addressing issues
    - Terminating relationships

CENTRALIZED LOG MANAGEMENT FOR TSC COMPLIANCE

When you use a centralized log management solution that incorporates security analytics, you can develop, design, and monitor your TSC controls and compliance across various common controls, including:

- CC4.1
- CC4.2
- CC5.1
- CC5.2
- CC6.2
- CC6.3
- CC6.6
- CC6.7
- CC6.8
- CC7.1
- CC7.2
- CC7.3

Further, your logging and monitoring can support additional common criteria by acting as supporting documentation. For example, you can use reports derived from dashboards to support risk assessment decisions or management reporting requirements.

ACCESS MONITORING

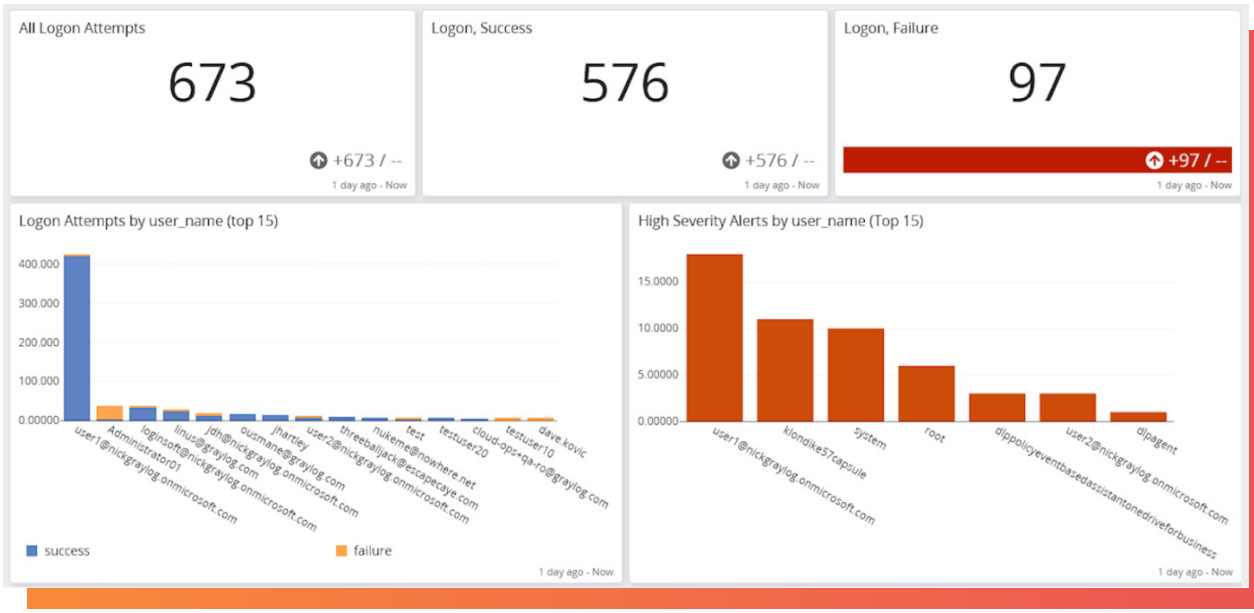
Access monitoring is critical to the eight common controls under "Logical and Physical Access Controls." A centralized log management solution with built-in user and entity behavior analytics (UEBA) provides a robust access monitoring solution that can help detect and investigate anomalous behavior in complex environments.

Some security functions that centralized log management paired with security analytics can enable include:

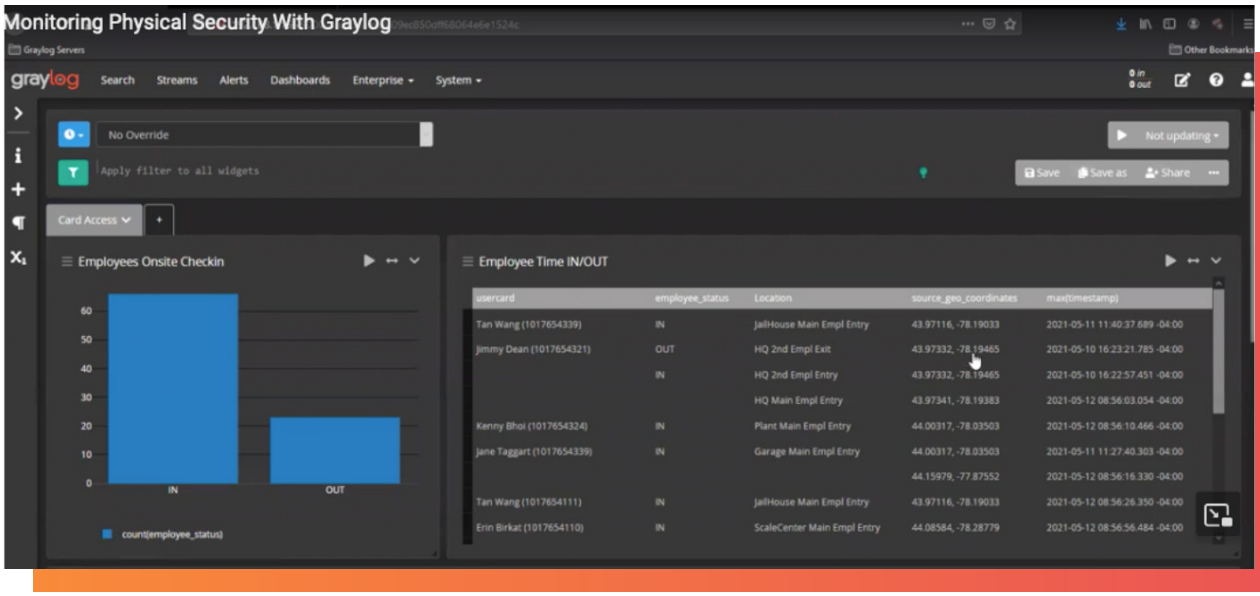
- Privileged access management (PAM)
- Password policy compliance
- Abnormal privilege escalation
- Time spent accessing a resource
- Brute force attack detection

By monitoring this activity, you can design detections that support identifying security incidents arising from:

- Unauthorized actions of authorized personnel
- Use of compromised credentials



Additionally, your centralized log management solution can support monitoring physical access to help you document potential physical barrier compromise.

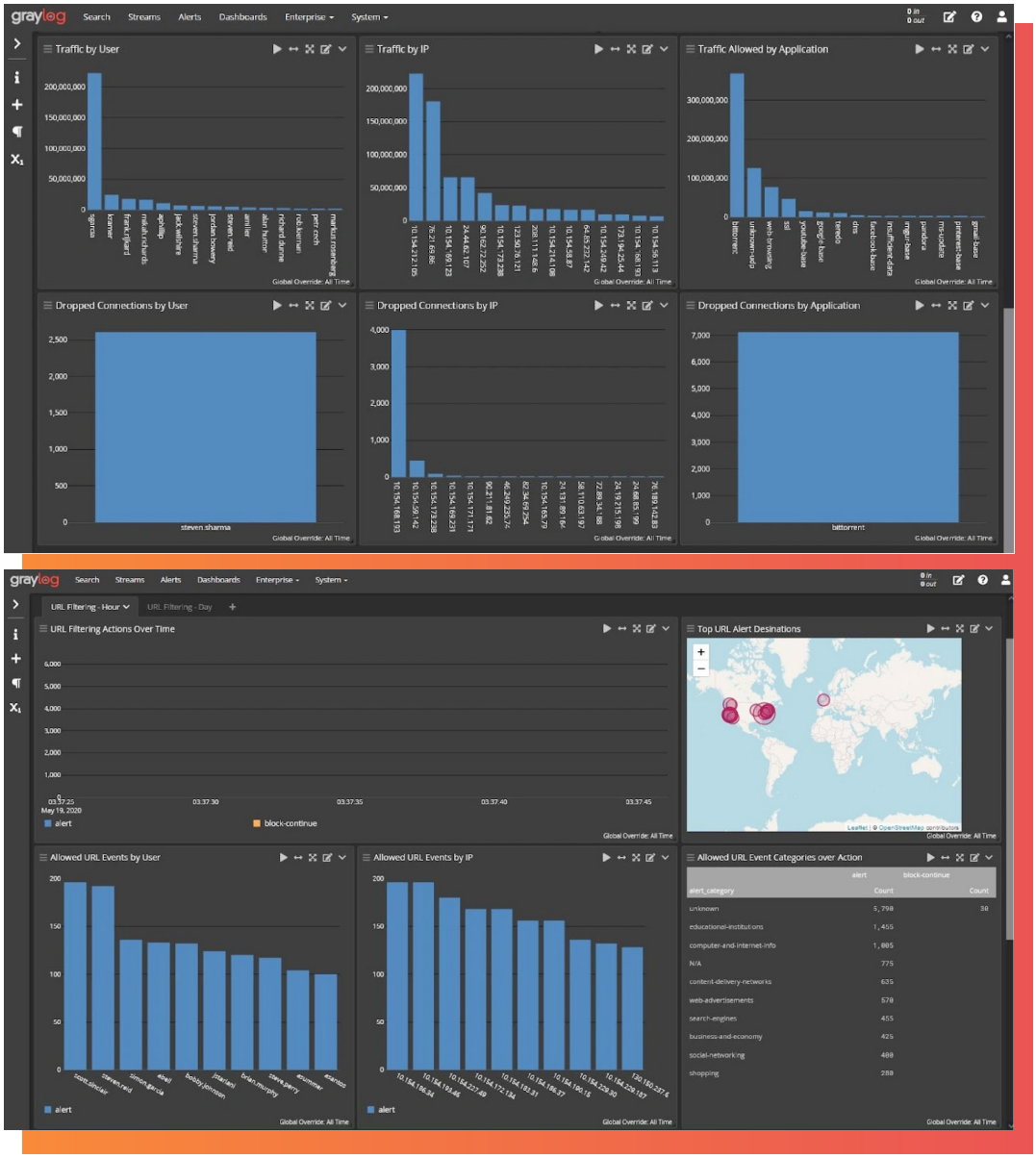


HIGH-FIDELITY ALERTS

High-fidelity alerts that correlate and analyze events across your environment enable you to design, develop, and monitor events to document activities associated with the common controls under “System Operations.”

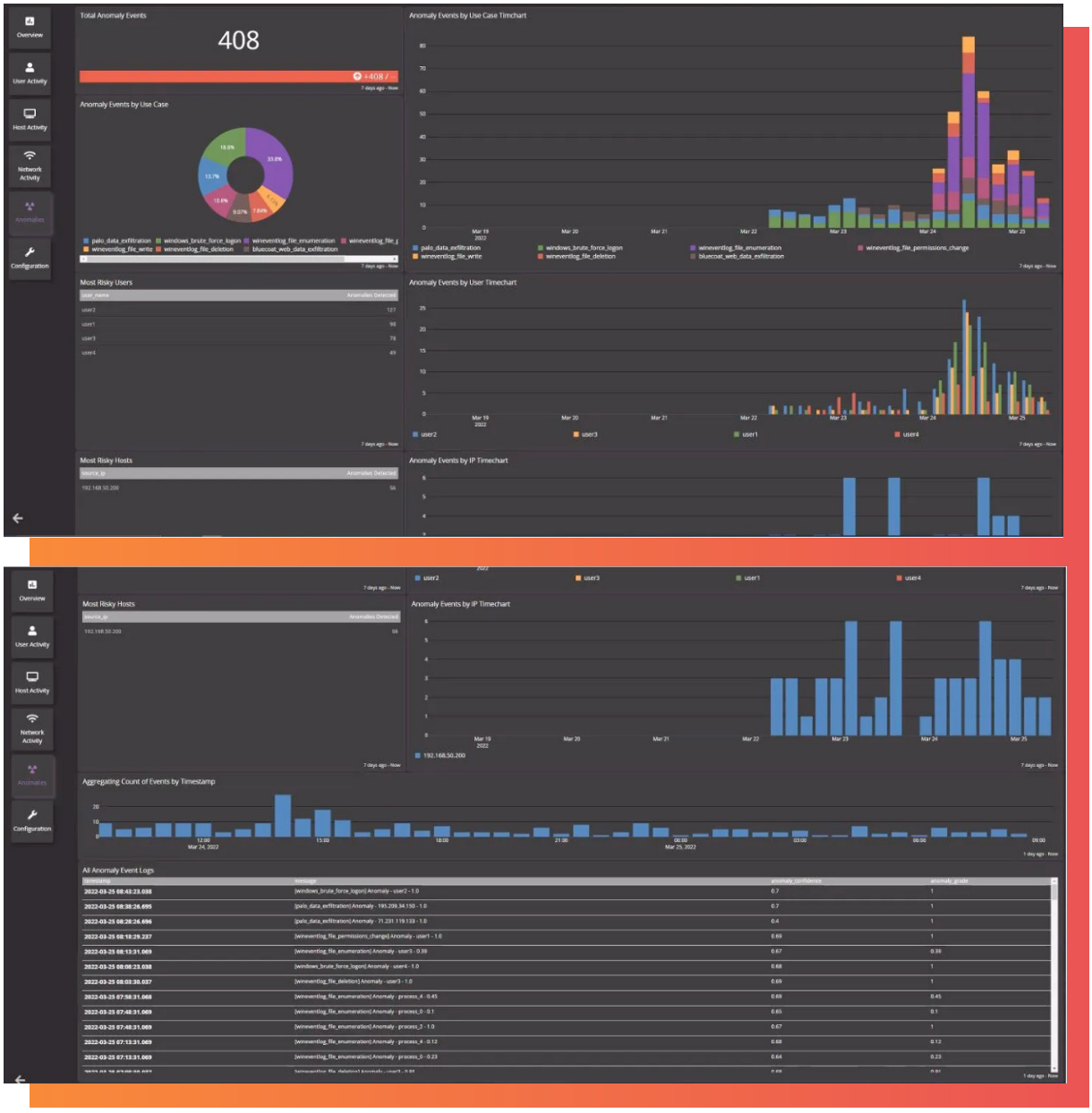
By monitoring network security, you can combine firewall logs with Intrusion Detect System (IDS)/Intrusion Prevention System (IPS) logs to gain visibility into:

- Abnormal inbound and outbound traffic that could signify data traveling to a cybercriminal-controlled server
- Potential evasion techniques

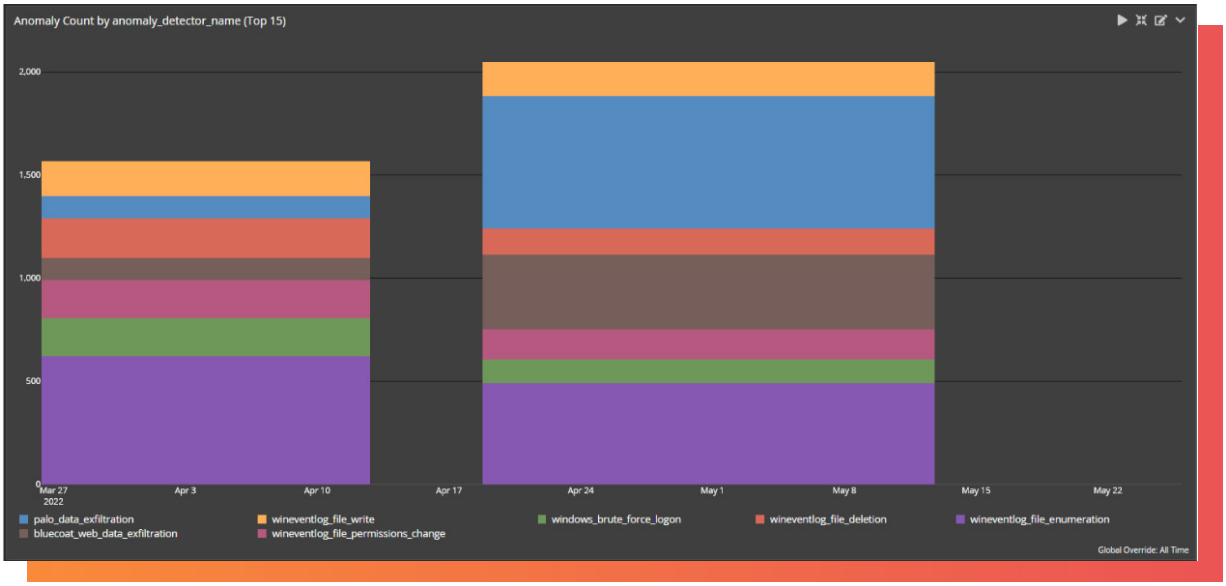


When you integrate security analytics into your network monitoring, you can set baselines and design alerts for anomalies that indicate potential security incidents like:

- Use of compromised credentials
- External unauthorized access
- Compromised, authorized external parties
- Unauthorized hardware/software implemented or connected



To identify potential data exfiltration, your centralized log management solution's high-fidelity alerts should combine security analytics, threat intelligence, and monitoring dashboards. By aggregating, correlating, and analyzing network monitoring logs, antivirus logs, and UEBA enables entities to gain insight into abnormal data downloads.

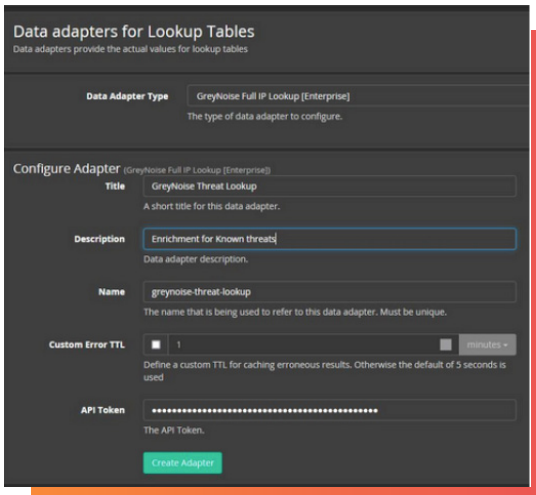


INCIDENT RESPONSE AND AUTOMATED THREAT HUNTING

Your monitoring solution supports your incident response procedures by providing lightning-fast investigation capabilities to determine root cause, documenting remediation activities, and enabling management incident review.

Parameterized search queries not only help with investigations because they provide real-time answers, they also enable proactive threat hunting that can help detect advance threat activities like:

- Abnormal user access to sensitive information
- Abnormal time of day and location of access
- High volumes of files accessed
- Higher than normal CPU, memory, or disk utilization
- Higher than normal network traffic



COMPLIANCE AND POST-INCIDENT REPORTING

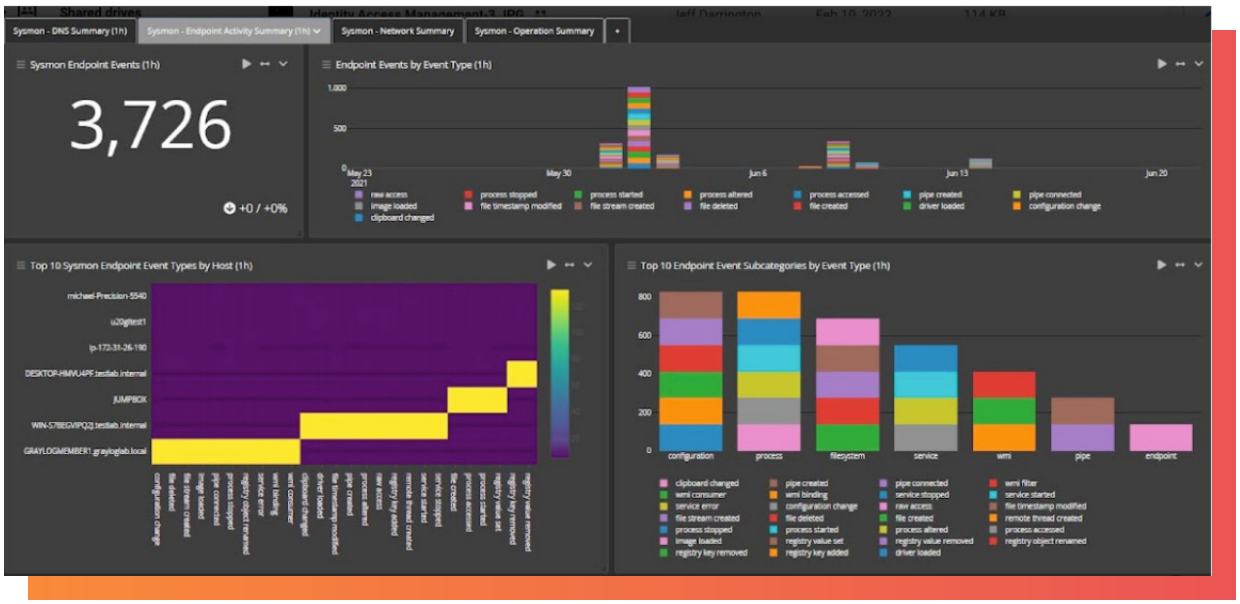
When auditors review TSC controls, they look for documentation that shows you:

- Mitigated the security incident's effect
- Restored business operations, data, and the affected environment
- Changed controls
- Contained the incident within a defined time-frame
- Communicated effectively with management

A centralized log management solution's dashboards provide the high-level visualizations that enable entities to evaluate their security monitoring and cleanup activities.

For example, if trying to prove that the entity eradicated the malicious program, a dashboard can show:

- **Beginning of incident:** when logs documented changes
- **Activities during the incident:** what types of changes the logs documented to highlight what the threat actor tried to do
- **Malicious activity containment/eradication:** when logs stop reporting the activities indicating the threat actor is no longer acting in the system



GRAYLOG SECURITY: DOCUMENTING TSC COMPLIANCE FOR SOC AUDITS

Graylog Security's intuitive user interface enables you to create the high-fidelity detections that prove your information security and data protection processes achieve their objectives. With our analytics, anomaly detection, prebuilt search templates, dashboards, correlated alerts, and dynamic look-up tables, you gain all the value of a security incident and event management (SIEM) technology without the associated costs and complexity.

To see how Graylog Security can help you achieve your SOC objectives, contact us today.

ABOUT GRAYLOG

Graylog is a leader in log management and Security Information Event Management (SIEM), making the world and its data more efficient and secure. Built by practitioners with the practitioner in mind, Graylog unlocks answers from data for thousands of IT and security professionals who solve security, compliance, operational, and DevOps issues every day. Deployed in more than 50,000 installations worldwide, Graylog is an award-winning platform built for speed and scale in capturing, storing, and enabling real-time analysis of terabytes of machine data. Graylog eliminates the noise and delivers an exceptional user experience by making data analysis, threat hunting, detection, and incident investigation fast and efficient using a more cost-effective and flexible architecture.

www.graylog.org
info@graylog.com | 1301 Fannin Street, Suite 2000, Houston, TX 77002

graylog