

Key Security and Compliance Terms and Concepts

Having a solid grasp of key concepts and tools is necessary for protecting your digital assets and ensuring compliance with industry standards. This glossary provides a comprehensive overview of important terms and practices in security and compliance.

Organized into four main sections — Cybersecurity Platforms and Management, Cybersecurity Operations and Processes, Telemetry and Analytics, and Security Monitoring and Compliance — this guide gives you the knowledge you need to secure your digital environments effectively.



Table of Contents



Cybersecurity Platforms and Management	01
Cybersecurity Operations and Processes	04
Telemetry and Analytics	07
Security Monitoring and Compliance	11



Cybersecurity Platforms and Management

This section covers terms related to various platforms and management strategies used to safeguard applications, data, and infrastructure in cloud and hybrid environments. It includes concepts like Cloud-Native Application Protection Platforms (CNAPP), Cloud Workload Protection Platforms (CWPP), and Zero Trust Architecture.

Terms	Description
Application Security Posture Management	Prioritize and remediate risks and misconfigurations across AWS, GCP, and Azure cloud environments with rich context across runtime, identity, network, data and business insights. Start with agentless scanning for quick ROI and optionally extend to deep runtime visibility through eBPF sensor based approach for efficient risk prioritization.
Cloud Detection and Response (CDR)	Uptycs Cloud Detection and Response (CDR) is the first solution that alerts teams when an event is part of a recognized cloud-focused attack technique. That means higher fidelity alerts and faster remediation.
Cloud Infrastructure Entitlement Management (CIEM)	Implement least privilege, visualize identity relationships, and rapidly respond to security incidents and threats from the same platform you use to secure your cloud infrastructure.
Cloud Security Posture Management (CSPM)	Prioritize and remediate risks and misconfigurations across AWS, GCP, and Azure cloud environments with rich context across runtime, identity, network, data and business insights.

Cloud Workload Protection Platform (CWPP)	A cloud workload protection platform (CWPP) has emerged as a solution for securing systems across hybrid and multi-cloud environments.
Cloud-Native Application Protection Platform (CNAPP)	A cloud-native application protection platform (CNAPP) is a unified suite of security solutions designed specifically for cloud-native environments. It provides comprehensive protection across the entire lifecycle of cloud-native applications, from development to deployment and ongoing management.
DevSecOps	The practice of integrating security into every phase of the software development lifecycle, fostering collaboration between development, security, and operations teams.
Endpoint Security	Attackers often target endpoints—especially developer laptops—because they know that's where valuable credentials and data reside. Uptycs offers comprehensive endpoint security and compliance capabilities in a single solution.
Extended Detection and Response (XDR)	Protect the developer laptops that build your applications, to the Linux servers that run them. The Uptycs extended detection and response (XDR) solution gives you powerful visibility and flexibility to secure and query any endpoint in your fleet. Enjoy unified threat detection and response, vulnerability scanning, security hygiene, compliance, remediation, and more.
Hybrid Cloud Security	Measures and solutions implemented to secure applications, data, and infrastructure in a hybrid cloud environment, combining on-premises and cloud-based resources.

Identity Federation	A method for securely sharing identity information across different organizations or systems, enabling users to access multiple services using a single set of credentials. Identity federation simplifies authentication in hybrid and multi-cloud environments while maintaining security and user convenience.
Kubequery	An extension of osquery designed specifically for Kubernetes environments to enhance security and visibility.
Managed Detection and Response Services (MDR)	Experience total peace-of-mind with round-the-clock, fully managed detection and response (MDR) services across your entire attack surface. Seamlessly extend your in-house security with Uptycs Managed Services.
Osquery	Osquery is an operating system instrumentation agent that provides a unique and refreshing approach to security. It delivers a single-agent solution using a universal query language to collect rich datasets for multiple use cases.
Security Automation and Orchestration (SOAR)	Platforms that integrate and automate security operations, incident response, and threat intelligence to streamline workflows and enhance threat detection and remediation capabilities. SOAR enables teams to focus on critical issues by reducing manual effort and improving operational efficiency.
Shift Up Security	A new cybersecurity methodology aimed at eliminating tool, team, and infrastructure silos by adopting a unified approach to security operations and intelligence.

Single Sign-On (SSO)	An authentication technology that allows users to access multiple applications or systems with a single set of login credentials. SSO enhances user experience by eliminating the need for repeated logins while reducing password management risks.
Zero Trust Architecture	Zero-trust is a relatively new approach to enforcing access control for a company's network and internal resources. Traditionally, network security follows a perimeter-based model—like a castle and moat. There's a boundary around all internal resources you want to protect. Anyone who wants to access network resources has to be validated at that boundary.



Cybersecurity Operations and Processes

Understanding operations and processes in cybersecurity is important for effective threat management and incident response. This section introduces terms such as Computer Security Incident Response Teams (CSIRT), Threat Hunting, and Vulnerability Management, along with methodologies like Shift Left Security Controls and Risk Prioritization.

Terms	Description
Attack Path Analysis	Uptycs' Risk Prioritization integrates with the Attack Path data to spotlight the most critical vulnerabilities. This synthesis of real-time data and contextual analysis guides security teams to focus on the highest risks, fostering a proactive rather than reactive, cloud security posture.

Behavioral Detection	Uptycs System Insight, Visibility, and User Behavioral Monitoring offers organizations a unified solution to gain deep visibility, manage assets, and monitor insider risk across hybrid cloud, on-premise, and containerized environments, providing real-time insights and advanced security controls to safeguard critical infrastructure.
Cloud Compliance	Ensuring that cloud environments and operations adhere to relevant regulatory and industry standards and best practices.
Computer Security Incident Response Team (CSIRT)	When determining the scope and severity of an incident, you need quick, accurate answers. Streamline your investigation and reduce the time spent minimizing potential damage with powerfully simple SQL query.
Infrastructure as Code (IaC) Security	Infrastructure as Code (IaC) Scanning: Validates security best practices in cloud setup and deployment.
Internet Exposure	The vulnerabilities that arise from misconfigured cloud resources, such as EC2 instances with overly permissive security settings, which serve as entry points for attackers.
Lateral Movement	The concept of lateral movement stems from the understanding that modern networks typically comprise numerous interconnected devices and systems. Once an attacker manages to breach the perimeter security or gains initial access to one machine, their goal is to stealthily navigate through the network, moving laterally from one device to another and progressively escalating their privileges.

Post-Exploit Detection	Identifying malicious activities that occur after an initial exploit, aimed at detecting further compromise within a network.
Proactive Threat Hunting	Actively searching for signs of malicious activity within an environment, beyond automated alerts.
Risk Prioritization	Unified risk prioritization approach that analyzes security signals, not just agentless posture management and static risk, but through runtime insights and shift-left visibility in order to eliminate blind spots.
Supply Chain Security	The practice of securing the end-to-end software development and delivery pipeline, including dependencies, third-party components, and build systems. Supply chain security aims to prevent tampering, unauthorized code insertion, and vulnerabilities in the software supply chain.
Threat Hunting	Be proactive with Uptycs. Hunt for the most hidden threats across your entire infrastructure, without limits to your hypotheses, and avoid waiting for someone else to discover a breach in your network.
Threat Intelligence Matches	Correlating observed activities within an organization's environment with known threat intelligence data to identify potential threats.
TTPs (Tactics, Techniques, and Procedures)	Patterns of behavior used by cyber adversaries, including methods of attack and tools used.

Uptycs Academy	Uptycs Academy empowers your team with guidance and tools to enhance security knowledge of the Uptycs platform, optimizing posture, boosting productivity, and providing total support at every step.
Uptycs Security Policies	Defined rules and guidelines established by Uptycs to ensure the security and integrity of systems and data.
Vulnerability Management	Full vulnerability lifecycle management from build to runtime across servers, hosts, containers, VMs, and serverless.

Telemetry and Analytics

Telemetry and analytics play a key role in monitoring and analyzing security data to detect and respond to threats. This section provides insights into terms like Security Analytics, Cloud-Based Security Analytics, and Unified Data Models, as well as tools like Flight Recorder and YARA Rule Scanning.

Terms	Description
Bloatware	Refers to pre-installed software that takes up excessive storage and system resources without providing meaningful value. It often slows down device performance and occupies space with unnecessary apps or trial programs.

CI/CD Process Security	The implementation of security measures within Continuous Integration and Continuous Deployment pipelines to ensure the integrity and security of code throughout the development lifecycle.
CIS Benchmarks	Being certified by the Center for Internet Security (CIS) signifies a robust alignment with high-level compliance benchmarks, embodying trust and excellence in cybersecurity.
Cloud-Based Security Analytics	Security analysis conducted in the cloud, leveraging cloud resources for data processing, threat detection, and response.
Container Runtimes	Stop malicious threats such as container breakouts and privilege escapes with the ability to triage all the way down to malicious code commits via image provenance.
Flight Recorder	A tool that continuously records system activity, allowing for detailed analysis and investigation of security incidents.
Kubernetes Security Posture Management (KSPM)	Tools and practices designed to secure and manage the security posture of Kubernetes environments.
Live and Historical Query Investigations	The ability to perform real-time and retrospective analysis of system data to identify security incidents or performance issues.

Managed Container Orchestration Platforms	Broad support for both cloud and on-prem orchestration planes including Amazon EKS/ECS, Fargate, Microsoft AKS, Google GKE, KOPS, and Red Hat OpenShift across hybrid cloud environments.
Query Packs	Predefined sets of queries in osquery to automate the collection and analysis of security data.
Scalability	The ability to increase or decrease IT resources as needed to meet changing demand, scalability enables organizations to increase workload size within an existing infrastructure without impacting performance.
SDLC Policy Controls	Security measures integrated into the Software Development Life Cycle (SDLC) to ensure compliance with security policies and best practices.
Security Analytics	The use of data collection, aggregation, and analysis tools to detect and respond to security threats in real time.
Security Graph	Uptycs' Security Graph feature to address this challenge head-on. It consolidates and visualizes complex cloud security data, providing a comprehensive view of potential security risks.
Self-managed Kubernetes	Kubernetes clusters that are deployed, managed, and maintained by an organization's internal team rather than by a third-party provider.

Serverless Technologies	Cloud services that allow developers to build and run applications without managing server infrastructure, such as AWS Lambda and Azure Functions.
Service Mesh	A dedicated infrastructure layer that controls service-to-service communication over a network, offering features like load balancing, encryption, and observability.
Structured Telemetry	Organized and systematic collection of data that provides insights into system performance and health.
Telemetry	The automated process of collecting and transmitting data from remote or inaccessible sources to an IT system for monitoring and analysis.
Unified Data Models	Standardized data structures that allow for consistent data integration, analysis, and reporting across different systems.
YARA Scans	YARA memory scans against specific types of files and new processes, and that deploying new rules to the fleet was safe and easy.



Security Monitoring and Compliance

Effective security monitoring and compliance are necessary for maintaining the integrity and security of cloud and container environments. This section includes terms such as Real-time Container Security Visibility, Infrastructure as Code (IaC) Scans, and Compliance Automation, highlighting the importance of continuous monitoring and adherence to security policies.

Terms	Description
Access Request Tracking	Monitoring and logging requests for access to cloud resources to ensure proper authorization and traceability.
Audit Checks	Systematic reviews and evaluations of cloud resources and configurations to ensure compliance with security policies and standards.
Automatic Threat Detection and Response	Use a multi-layered approach to detect cloud threats and apply effective defense techniques through Incident response and automation workflows. Strengthen your cloud threat prevention strategy and safeguard your environments from emerging attack.
Best-Practice Guardrails	Predefined policies and controls designed to enforce industry best practices within cloud environments.
Centralized Visibility and Control	A unified interface for monitoring and managing security across multiple cloud environments and services.
Cloud Anomaly Detection	Identifying unusual or unexpected behaviors within a cloud environment that could indicate security threats.
Cloud IAM Policy Analysis	Uptycs evaluates the identity risk posture of your cloud accounts by analyzing cloud identity and access management (IAM) policies, considering factors such as credential rotation, potential privilege escalation, and credential exposure.

Cloud-Native Security Principles	Foundational strategies designed to secure cloud-native environments by leveraging principles like least privilege, zero trust, and automation.
Compliance Automation	Automating the processes required to meet various compliance standards, such as NSA Kubernetes hardening checks, CIS Benchmarks, SOC 2, PCI-DSS, HIPAA, and ISO 27001.
Configuration and Settings Monitoring	The process of overseeing and verifying cloud configurations and settings to ensure compliance and security.
Credential Escalation	The process by which attackers increase their access privileges within a compromised environment, often by exploiting misconfigurations or vulnerabilities.
Credential Exposure Analysis	Assessing the risk of credentials being exposed to unauthorized entities, potentially leading to security breaches.
Credential Rotation Monitoring	Keeping track of how often and effectively credentials are rotated to minimize the risk of compromise.
Custom Compliance Checks	Tailored assessments that ensure cloud environments meet specific regulatory and organizational compliance requirements.
Data Exfiltration	The unauthorized transfer of data from a compromised system to an external location controlled by the attacker.

Data Privacy	The practice of ensuring that personal and sensitive data is collected, stored, and processed in compliance with legal and regulatory frameworks, such as GDPR and CCPA. Data privacy focuses on protecting individuals' rights and maintaining transparency in how data is used.
Data Security	Measures and technologies implemented to protect data from unauthorized access, alteration, or destruction. Data security encompasses encryption, access controls, and other safeguards to ensure the confidentiality, integrity, and availability of information.
Graphical Kubernetes Overview	A visual representation of a Kubernetes environment, displaying the relationships and status of various components such as nodes, pods, and services.
Historical Trend Data	The analysis of past data to identify patterns and trends in cloud resource usage and security incidents.
Identity Misconfiguration Detection	Identifying incorrect or risky configurations in identity and access management settings that could lead to security breaches.
Identity Relationship Mapping	Visualizing and analyzing the relationships between different identities and their access rights within a cloud environment.
Identity Risk Posture	An assessment of the overall security risk associated with an organization's identity and access management practices.

Incident Response Playbooks	Documented procedures outlining steps to take during a security incident to respond effectively.
Indicators of Compromise (IoC)	Data points or evidence that suggest a system may have been breached or is under attack, used for threat detection and response.
Infrastructure as Code (IaC) Scans	Automated checks of IaC configurations to detect and remediate security vulnerabilities and misconfigurations in infrastructure provisioning scripts.
Insights Dashboards	Visual interfaces that provide real-time analytics and insights into cloud security and performance metrics.
Least Privilege Implementation	Ensuring that users and services have the minimum level of access necessary to perform their functions, reducing the risk of security incidents.
Namespace, Pod, and Image Risk Assessment	The evaluation of security risks associated with Kubernetes namespaces, pods, and container images to identify and mitigate potential vulnerabilities.
OPA Gatekeeper Policy Controls	The use of Open Policy Agent (OPA) Gatekeeper to enforce security and compliance policies within Kubernetes environments.
Privilege Escalation Detection	Identifying attempts to gain unauthorized access to higher privilege levels within a cloud environment.

Real-Time ATT&CK-Mapped Detections	Behavioral detections that are mapped to the MITRE ATT&CK framework, providing real-time alerts and remediation steps.
Real-time Cloud Inventory	Continuous tracking and management of cloud resources to provide up-to-date information about all assets within a cloud environment.
Real-time Container Security Visibility	The capability to monitor and analyze the security status of containers in real time, identifying potential threats and vulnerabilities as they occur.
Resource Relationship Analysis	Examination of how different cloud resources interact and relate to one another to identify potential security risks and dependencies.
Runtime Security	Ensuring that only trusted and verified code is executed within a cloud or container environment, protecting against runtime threats.
Runtime Threat Detection	Identifying and mitigating threats as they occur in real-time within cloud environments.
Shift Left Security Controls	Security practices integrated early into the software development process, enabling the identification and resolution of security issues before deployment.
Software Development Lifecycle (SDLC) Security	Security measures implemented throughout the software development lifecycle to ensure code integrity and compliance with security policies.

Unified API Monitoring	Overseeing and securing API interactions to ensure they are operating correctly and securely across cloud services.
Vulnerability Highlighting	Identifying and emphasizing potential security weaknesses within a cloud environment for remediation.
YARA Rule Scanning	Leverage in-built as well as customized YARA toolkits for incident response.



Uptycs is the leading cloud security platform for large hybrid cloud environments. We extend security visibility from development to runtime, ensuring consistent protection and compliance across the application infrastructure. That's why enterprises like PayPal, Comcast, and Nutanix rely on Uptycs to secure the development ecosystems they use to build their applications and run their workloads.

Secure Everything from Dev to Runtime

[Learn more at Uptycs.com](https://uptycs.com)