SOC 3 + C5
Report

Program:
Cisco Webex Teams service
Cisco Webex Control Hub
Cisco Webex for Developers

For the period
May 26, 2018 to October 12, 2018

Accedere Inc. in association with DNV-GL

Accedere Inc.
Certified Public Accountants
info@accedere.us

Table of Contents

Section I

Independent Service Auditor's Report

ACCEDERE

Independent Service Auditor's Report

To: The Management of Cisco Webex Teams
Location: San Jose, CA, USA

Scope

We have examined Cisco Webex Teams service, a product of Cisco's Team Collaboration Group, and Cisco Webex Teams accompanying assertion titled "Cisco Webex Teams Management Assertion of …" that the controls within Cisco Webex Teams service were effective throughout the period May 26, 2018 to October 12, 2018, to provide reasonable assurance that Cisco Webex Teams service commitments and system requirements were achieved based on the trust services principles & criteria (TSPC 2016) relevant to security, availability, confidentiality, and privacy (applicable trust services principles & criteria) set forth in TSPC 2016, Trust Services Principles & Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). The scope also covers Cisco's worldwide applicability of controls of the standard C5 Cloud Controls (Cloud Computing Compliance Controls Catalogue).

Cisco Webex Teams Responsibilities

Cisco Webex Teams is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Cisco Webex Teams service commitments and system requirements were achieved. Cisco Webex Teams has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Cisco Webex Teams is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and Cisco's worldwide applicability of controls of the standard C5 Cloud Controls. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Cisco Webex Teams' service commitments and system requirements based on the applicable trust services criteria

- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Cisco Webex Teams' service commitments and system requirements based on the applicable trust services criteria.
- Cisco Webex Teams ISO 27001:2013 & 27017:2015 audit conducted by DNV GL and the related evidence

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria and Cisco's worldwide applicability of controls of the standard C5 Cloud Controls. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Cisco Webex Teams service were effective throughout the period May 26, 2018 to October 12, 2018 to provide reasonable assurance that Cisco Webex Teams service commitments and system requirements were achieved based on the applicable trust services criteria and Cisco's worldwide applicability of controls of the standard C5 Cloud Controls is fairly stated, in all material respects.

Accedere Inc.
Certified Public Accountants
CPA License No: FRM 5000337
Denver, Colorado, USA
Place of Issue: Denver, CO
Date: October 12, 2018

Stamp & Signature
Ashwin Chaudhary
CPA, CISSP, CISA, CISM, CRISC,
CGEIT, CCSK, ISO 27001LA, PMP.
info@accedere.us

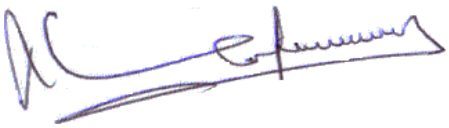
Annexure to Cisco Webex Teams SOC 3 Report

October 12, 2018

DNV GL and Accedere Inc. participated in the SOC 3 attestation and Cisco's worldwide applicability of controls of the standard C5 Cloud Controls of Cisco Webex Teams service, Cisco Webex Control Hub and Cisco Webex for Developers.

The ISO 27001:2013 and ISO 27017:2015 Audit evidences carried out between 13th to 24th of August 2018 were shared and used for the attestation which formed the basis for the SOC 3 type II attestation to support the applicable criteria for the principles in Trust Services Principles & Criteria (TSPC) 2016 for Security, Availability, Confidentiality, Privacy and Cisco's worldwide applicability of controls of the standard C5 Cloud Controls.

Signed,



Shamanna Nandakumar

Lead Auditor, ISMS

DNV GL Business Assurance India Private Limited

DNV GL Business Assurance , Unit No. S2003, 20th Floor, World Trade Center, Brigade Gateway Campus,

No.26/1, Dr. Rajkumar Road, Malleshwaram West, Bengaluru – 560 055 , +91 80 23081100 (B). www.dnvgl.com

Section II

Management Assertion

Cisco Webex Teams Management Assertion for Cisco Webex Teams service, Cisco Webex Control Hub and Cisco Webex for Developers

We are responsible for designing, implementing, operating, and maintaining effective controls within Cisco Webex Teams service system throughout the period May 26, 2018 to October 12, 2018, to provide reasonable assurance that Cisco Webex Teams service commitments and system requirements relevant to security, availability, confidentiality, privacy and the C5 Cloud Controls were achieved. Our description of the boundaries of the system is presented in Section III and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period May 26, 2018 to October 12, 2018, to provide reasonable assurance that Cisco Webex Teams service commitments and system requirements were achieved based on the trust services principles & criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSPC 2016 Trust Services Principles & Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria) and the C5 Cloud Controls. Cisco Webex Teams' objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section III.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period May 26, 2018 to October 12, 2018, to provide reasonable assurance that Cisco Webex Teams service commitments and system requirements were achieved based on the applicable trust services criteria.

Cisco Systems, Inc.

Section III

Cisco Systems, Inc.'s Description of its Cisco Webex Teams service, Cisco Webex Control Hub and Cisco Webex for Developers

Company Background

Cisco Webex Teams product is used in this report to refer to: Cisco Webex Teams service, Cisco Webex Control Hub and Cisco Webex for Developers.

Cisco Systems, Inc. ("Cisco" or the "Company") (NASDAQ: CSCO) was incorporated in California in December 1984, and is headquartered in San Jose, California. Cisco is a global leader in information technology (IT). Cisco designs, manufactures, and sells Internet Protocol (IP)-based networking and other products related to the communications and IT industry and provides services associated with these products and their use. Cisco provides a broad line of products, services and solutions for transporting data, voice, and video within buildings, around campuses, and around the world. Cisco products are designed to transform how people connect, communicate, and collaborate. Cisco products are installed at enterprise businesses, public institutions, telecommunications companies and other service providers, commercial businesses, and personal residences.

Collaboration Technology Group

Cisco is organized into business units and corporate functions. The Cisco Webex Teams product is in the business unit called Collaboration Technology Group (CTG). CTG is comprised of a suite of products that make work more intuitive with easy-to-use collaboration technology. The suite of collaboration products enable businesses through Unified Communications, Contact Center, Conferencing, and Collaboration Endpoints solutions.

For more information on Cisco, refer to:

https://www.cisco.com

Cisco CTG Webex Security Organization

Security always comes first for Cisco Webex. Everything you share, say, and type is protected by end-to-end encryption. Authorized administrators can manage and enforce security policies. And thanks to Cisco's high security standards, Cisco Webex Teams products are some of the most secure collaboration tools available.

The Cisco Security and Trust Organization is committed to maintaining strong protections for our customers, products and company by being trustworthy, transparent and accountable. The Cisco CTG Webex security organization is part of the Security and Trust Organization and is also embedded in the Cisco Webex Teams product operation. The organizational independence and intrinsic presence institutionalizes security first for Cisco Webex Teams product.

For more information on Cisco's commitment to security, refer to:

https://www.cisco.com/c/en/us/about/trust-center.html

Controls Common for CTG

CTG uses common and shared controls for cloud products in the CTG portfolio. This report describes these common controls and following Controls Common for CTG is the description of the controls that are specific to the Cisco Webex Teams product.

Compliance and Governance

Management, in conjunction with the groups it creates, is responsible for creating, maintaining, and monitoring the policies, standards, and procedures that constitute the internal controls deemed to provide reasonable assurance of the integrity and reliability of the production systems,

and for the protection of customer information and assets against unauthorized use and disposition. Compliance with Cisco policies and standards is required and verified

Leading the priority and focus on security is the CTG Governance Committee (GC). The GC is comprised of Cisco CTG Webex Security and Cisco Webex Teams product leaders. The GC is accountable for the overall governance framework, planning, directing, and controlling the security and risk aspects of business operations. The GC assigns roles and responsibilities to provide oversight to confirm adequate resourcing, efficiency of operation, and separation of duties. The key roles and responsibilities of the committee are:

- Chief Information Security Officer (CISO) – accountable to information security for Cisco Webex Teams product
- Cisco CTG Webex Security Compliance team – responsible for the governance of Cisco Webex Teams product within the Cisco CTG Webex Security organization. This team is responsible for maintenance of the Information Security Management System (ISMS)
- Security Operations team – responsible for the operations of security compliance such as baseline configuration management and vulnerability management
- Cisco Webex Teams product leadership and team – responsible for the implementation and execution of security processes and procedures

Information Security Management System

Cisco has established and maintains formal policies, standards, and procedures to delineate the standards relevant to the design and operations of controls over the Cisco Webex Teams product. CTG has an Information Security Management System (ISMS) designed to meet ISO/IEC 27001:2013 and 27017:2015 requirements implemented and operating on an annual cycle. Policies are reviewed and approved on a periodic basis, published on the company intranet, and communicated to CTG employees and contractors. Organizational roles, responsibilities, and competency requirements affecting the security, confidentiality, and privacy of the services are defined and assigned by CTG management and communicated to the CTG organization.

The Information Security Policy defines the management commitment to Information Security and the information security program. The policy requires developing processes and procedures to protect security, confidentiality, and privacy of customer data, and to ensure compliance to applicable legal requirements, contractual obligations, and any security requirements. Management is responsible for periodic assessment of the level of compliance to legal requirements, operational controls, and overall risk posture. Assessment reports are presented to the ISMS GC and other appropriate levels of management which include:

- The importance/criticality of information resources
- The effectiveness of present information security arrangements
- Special circumstances that increase the probability of incidents occurring
- New threats and vulnerabilities
- Recommendations for ongoing improvements
- The status of current improvement activities

Information technology is governed by ISMS processes and procedures including the following:

- Access Management
- Asset Management
- Personnel Management
- Change Management
- Configuration Management

- Cisco Secure Development Lifecycle
- Incident Management
- Vulnerability Management
- Business Continuity Management

CTG evaluates its organizational structure, reporting lines, authorities, and responsibilities for appropriate scope, competence, and position within the organization on an annual basis as part of its business planning process. CTG monitors global regulatory requirements to ensure relevant statutory, regulatory, and contractual requirements are identified, documented, and kept up to date through regular interaction with legal, operations, and compliance business units.

Internal Communication

The CTG ISMS program uses a variety of mechanisms to communicate security requirements and expectations to its employees and contractors. The following assure that employees and contractors are informed and understand our security policies and expectations:

- Acknowledge the Company Code of Business Conduct (COBC)
- Take and pass the annual Security Awareness training course
- Read the Security Policies and Standards
- Take and pass the Cisco Security Ninja Program

During onboarding and annually thereafter, the organization provides mandatory Annual Security Awareness training which reaffirms the location of all policies and standards. Annually, the Organization Business Unit leader will send an email containing:

- The importance of adhering to the Organization Information Systems Policy
- The importance of meeting the Organization Security Objectives
- The importance of the ISMS
- The importance of adhering to the ISMS
- The Organization's responsibilities under the applicable laws & regulations
- The criticality of continual improvement
- Link to CTG ISMS Standard Manual, which contains:
    - The latest version of the CTG Information Systems Policy
    - The latest version of the CTG Security Objectives
    - Link to ISMS Policies and Standards intranet page
    - Link to the CTG ISMS Roles and Responsibilities document containing roles, responsibilities, and authorities

The CTG ISMS program maintains resources to communicate internally all ISMS documentation, policies, and standards. These policies and standards are managed in Cisco's enterprise documentation control system. An ISMS GC representative will send an email quarterly to employees, contractors, consultants, temporaries, and other workers with selected relevant information.

Internal Audit and Risk Management

CTG management is responsible for identifying the risks that threaten the achievement of the control objectives for the Cisco Webex Teams product. The CTG GC meets quarterly to review risks, mitigations, and required actions.

At the direction of CTG GC, an independent group within the Security & Trust Organization performs an Internal Audit at least annually. In addition, the independent group performs a Risk Assessment at least annually. The Internal Audit and Risk Assessment identify risks in the Cisco Webex Teams product. Management then implements appropriate measures to address those risks.

The Internal Audits and Risk Assessments are conducted for the Cisco Webex Teams product production system and operations.

Risk Assessment Methodology

The overall steps of the risk assessment include:

- Plan the risk assessment
- Establish context
- Perform assessment including risk identification, risk analysis, and risk evaluation
- Determine risk treatment options
- Document risk acceptance
- Communicate and consult on risk
- Monitor and review

Risks are analyzed for their possible impact and likelihood, yielding a level of risk determination and corresponding acceptance criteria. Risks are assessed and evaluated both at the global level and the site-specific level. Risk treatment, following the risk assessment, evaluates cost effective controls or measures. Management uses the following risk treatment options to assist in the decision making process of treating residual risks:

- Risk Modification (Mitigate) – The level of risk should be managed by introducing, removing, or altering controls so that the residual risk can be reassessed as being acceptable
- Risk Retention (Accept) – The business unit decides to accept the potential risk and continue operating with the risk. This acceptance is a conscious business decision based on a number of factors such as the organization's culture, risk appetite, and potential opportunity loss
- Risk Avoidance (Terminate) – When the identified risk is considered too high or the cost of implementing treatment options exceeds the benefits, a decision may be made to avoid the risk completely by withdrawing from a planned or existing activity or set of activities or changing the conditions under which the activity is operated
- Risk Sharing (Transfer) – The risk may be treated by transferring the risk using options such as purchasing insurance to compensate for the loss incurred if the risk materializes

Using the above criteria, the risk assessment team combines the evaluated controls with the risk treatment options and provides a risk assessment report to management.

Cisco Secure Development Lifecycle

Cisco Webex Teams product is compliant with the Cisco Secure Development Lifecycle (CSDL).

The combination of tools, processes, and awareness training introduced in all phases of the development lifecycle ensures defense-in-depth, and provides a holistic approach to product resiliency. CSDL is a process to ensure Cisco develops cloud solutions that adhere to the Cisco and industry security standards.

CSDL compliance is calculated based on information provided by the product teams. It is measured based upon compliance to Product Security Baseline (PSB) requirement-level data, and is monitored over time. Compliance with CSDL cannot be waived.

For Cisco cloud products, CSDL for Cloud requires a Cloud Approval to Operate (CATO). The CATO is Cisco's three-phase certification process. First is the discovery phase, where registration and security planning occur. Second is the assessment phase where CSDL PSB requirements are implemented, and attainment of the CATO approval to operate is achieved. The third phase is the governance and maintenance of the CATO on an annual basis.

For more information regarding Cisco's Secure Development Lifecycle, refer to:

https://www.cisco.com/c/en/us/about/security-center/security-programs/secure-development-lifecycle.html

Data Privacy & Protection

The S&TO Global Data Privacy Office is responsible for data privacy of Cisco assets. The S&TO Data Protection Program team manages the liability of data privacy of Cisco assets. The GDPO and DPP teams are a service to help product teams examine their products and services to remove any privacy or digital friction, including privacy compliance. Privacy engineering requirements defined by the GDPO team are integrated in the CSDL for Cloud CATO process.

The Cisco Webex Teams product team works with the GDPO and DPP teams to fully understand data privacy. In addition, every Cisco worker and partner is continuously accountable to the protection of customer information.

Policies, procedures, standards, guides, and resources available to enable complete understanding and enforcement of Cisco's data lifecycle include:

- Privacy and Data Protection
- Customer Data Protection

- Security Ninja White Belt (Data Privacy and Security Centric Training)
- Enterprise Records Management Policy
- Enterprise Record Retention Schedule
- Corporate Data Protection Standard
- Corporate Backup Data Retention and Media Rotation Policy
- Legal Services (NDA and queries)

To maintain consistency across the company and drive the appropriate protections for specific categories of data, Cisco has an enterprise-wide Common Data Taxonomy:

- Administrative Data
- Customer Data
- Entrusted Data
- Financing Data
- Telemetry Data
- Support Data
- Cisco Operations Data
- Cisco Strategic Data
- Human Resources Data

Consistent categorization of data allows Cisco to develop category-specific data protection requirements that reflect the company's obligations for such data.

Data Impact Analysis

Every product at Cisco undergoes a complete Data Impact Analysis (DIA). This detailed and multiphase process can be summarized by the following mandatory initial questions:

- What data does your organization collect and or use?
- How is your data processed?
- Who accesses your data?
- Where is your data stored?
- What is the sensitivity, classification, and category of the PII data?
- What is the intended use for collecting this PII and are there other usages for it?
- What is the overall volume of this data, both traversing and in storage?
- What is the criticality of the underlying service or functions being performed by this application?

Cisco implements privacy criteria as a part of its Data Impact Assessment (DIA) and its Privacy Impact Assessment (PIA). Elements that are common in the Cisco taxonomy and the Trust Services Privacy Principle include:

- Notice and communication of commitments and system requirements
- Notice to data subjects about privacy practices, commitments, and system requirements
- Choice and consent. Detail choices available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects
- Collection minimization
- Use, retention, and disposal; Cisco limits the use, retention, and enforces disposal of PII
- Access. Cisco provides data subjects with access to their personal information for review and correction (including updates) to meet its privacy commitments

Privacy Assessment

Cisco's offerings (clouds, products) and IT applications must meet customer and regulatory requirements regarding the processing of personal information. Cisco has developed a Privacy Impact Assessment (PIA) process intended to:

- Give relevant privacy guidance to development teams in an efficient and agile way that enables fast, informed decision-making
- Flag potential privacy issues as early as possible in the development cycle

The assessment process applies to all Cisco offerings and IT applications that collect, use, and distribute customer, employee, or 3rd party personal data.

Each assessment contains the following components:

- PIA - General Info - Provides basic information and whether or not personal information is collected, used or distributed
- PIA - Privacy Controls - Section that established what controls the Offering or Application provides to protect privacy data and meet additional regulations
- PIA - Privacy Data Inventory - Inventory of the privacy data elements, including appropriate metadata
- PIA - Supporting Documentation - Area provided to leave more information where necessary
- PIA - Assessment - Final worksheet completed by the Privacy Assessment team

Vulnerability Management

A vulnerability management program, managed by the InfoSec Cloud Security team, is in place to assess vulnerabilities in the Cisco Webex Teams product environment. Assessments are performed on an on-going basis using a vulnerability scanner and penetration testing.

Beginning with an accurate inventory of all assets, the vulnerability management process employs a vulnerability scanning tool to verify the security of the information system and applications. All vulnerabilities found using the scanner and penetration testing are entered into the vulnerability repository where they are evaluated (triaged) and categorized based on severity and their common vulnerability scoring system (CVSS) score. False positives are identified and eliminated. Vulnerabilities are assigned to the responsible team for remediation with a resolution date. After remediation is complete, the environment is scanned to verify that the issue has been resolved.

Penetration Testing

Penetration Testing aims at finding security issues by using the same tools and techniques as an attacker and are used to help secure products and services. A Penetration Test is defined as a legal and authorized attempt to find and successfully exploit systems, products, and services for the purpose of making them secure. Penetration Testing goes a step beyond vulnerability assessment by simulating hacker activity and delivering a live payload. Proof of Concept (PoC) attacks demonstrate that the capability to exploit is real.

Independent third-party Network Penetration Tests are performed annually. The results of this testing are made available upon request. Additionally, component based Penetration Tests of the Cisco Webex Teams product occurs when there are significant changes. All results from Penetration Tests are managed and analyzed for improvements in the Vulnerability Management process.

Product Security Incident Management

Cisco has established policy that defines the roles and responsibilities of management for handling suspected data breach, data loss, and computer security incidents at Cisco. This policy defines requirements and procedures for incident detection, reporting, and response. Cisco has response teams that will respond to security incidents 24 hours a day, seven days a week.

The incident management process defines which employees, contractors, and third-parties to contact in case of an incident or awareness of a security weakness. It also defines the systematic steps in which the product security team responds to a security incident including, but not limited to, the identification and validation of an incident, damage control or remediation, service restoration, evidence collection and preservation, contact with authorities, and post-mortem evaluations.

The product security incident management team is responsible for:

- Identifying and reporting suspicious activity
- Monitoring and handling incidents that originate from intrusion detection/prevention systems and other perimeter monitoring devices
- Executing the Security Incident Response Management process
- Performing Incident Response Testing
- Performing Incident Response Training
- Notifying customers

Incident Monitoring

Cisco Webex Teams product employs multiple technologies, procedures, and teams to ensure secure operation. Cisco has implemented key operational metrics and alarms across the production network using a variety of automated monitoring systems to detect outages, service latency, security incidents, and other unusual or unauthorized activities and conditions. Alarms are configured to notify operational and management personnel when warning thresholds indicating potential service latency, server unavailability, or other factors affecting availability and functionality are breached. Personnel are on-call at all times to ensure that alarms are responded to in a timely manner.

Incidents and threshold warnings are logged in the incident tracking system. They are assigned a priority level and ownership and tracked through to appropriate resolution.

A key prerequisite for incident monitoring and response is event logging and centralized logs. Cisco has established a policy that defines the requirements for logging data at Cisco. This policy establishes requirements for event types, time synchronization, content and other key information. Logs are centralized for aggregation, correlation, continuity, and retention.

Incident Response

The Cisco Product Security Incident Response Team (PSIRT) is responsible for responding to Cisco product security incidents. The Computer Security Incident Response Team (CSIRT) provides proactive threat analysis, incident detection, and internally coordinated incident response. In addition, the Cisco Webex Teams product team monitors and responds to security incidents in coordination with PSIRT and CSIRT.

Cisco Product Security Incident Response Team (PSIRT)

The Cisco Product Security Incident Response Team (PSIRT) is responsible for responding to Cisco product security incidents. The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of information about security vulnerabilities and

issues related to Cisco products and networks. Cisco defines a security vulnerability as an unintended weakness in a product that could allow an attacker to compromise the integrity, availability, or confidentiality of the product. The Cisco PSIRT adheres to ISO/IEC 29147:2014

The on-call Cisco PSIRT works 24 hours a day with Cisco customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security vulnerabilities and issues with Cisco products and networks.

The following are the steps in the Cisco Product Security Incident Response Process:

1. Awareness: PSIRT receives notification of security incident.
2. Active Management: PSIRT prioritizes and identifies resources.
3. Fix Determined: PSIRT coordinates fix and impact assessment.
4. Communication Plan: PSIRT sets timeframe and notification format.
5. Integration and Mitigation: PSIRT engages experts and executives.
6. Notification: PSIRT notifies all customers simultaneously.
7. Feedback: PSIRT incorporates feedback from customers and Cisco internal input.

The Cisco PSIRT investigates all reports regardless of the Cisco software code version or product lifecycle status. Issues will be prioritized based on the potential severity of the vulnerability and other environmental factors. Ultimately, the resolution of a reported incident may require upgrades to products that are under active support from Cisco.

Throughout the investigative process, the Cisco PSIRT strives to work collaboratively with the source of the report (incident reporter) to confirm the nature of the vulnerability, gather required technical information, and ascertain appropriate remedial action. When the initial investigation is complete, results will be delivered to the incident reporter along with a plan for resolution and public disclosure. If the incident reporter disagrees with the conclusion, the Cisco PSIRT will make every effort to address those concerns.

Cisco has published a Security Vulnerability Policy that describes:

- How to report or obtain support for a suspected security vulnerability
- Details on the incident response process
- Communications and disclosure plans

For more information on the Security Vulnerability Policy, refer to:

https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html

For more information on Cisco Security Advisories and Alerts, refer to:

https://tools.cisco.com/security/center/publicationListing.x

https://www.cisco.com/c/dam/en_us/about/security/psirt/Cisco-PSIRT-Infographic.pdf

https://tools.cisco.com/security/center/emergency.x?i=56

Cisco Computer Security Incident Response Team (CSIRT)

Cisco CSIRT forms part of the investigative branch of the Cisco Security and Trust Organization (S&TO), and provides proactive threat analysis, incident detection, and coordinated incident response. The primary mission of Cisco CSIRT is to review security architecture, establish incident management procedures for collecting incident data, enable efficient recovery from security incidents, prevent or minimize disruption of critical computing services, and facilitate cooperation and information exchange among cross-functional groups that are responsible for security incident remediation. Cisco CSIRT helps protect Cisco employees, business partners, and Cisco-owned businesses.

Cisco CSIRT is a global team of analysts, investigators, and engineers that serve the IT, business, and engineering organizations within Cisco, and more specifically, the Chief Security Officer (CSO) and the company senior management team, to help protect Cisco information assets. Cisco CSIRT coordinates, investigates, and remediates security incidents, and its investigators provide forensic investigations support at the direction of the Cisco CSO, and within the framework defined by Cisco HR, Cisco Legal, and external entities, including law enforcement.

S&TO has developed an Incident Response Plan which provides a high-level approach for how the incident response capability fits into the overall organization and describes the structure and organization of the incident response capabilities.

The incident handling methodology consists of the following phases:

- Incident Preparation
- Incident Detection and Analysis
- Incident Containment, Eradication, and Recovery
- Post Incident Activity and Evidence Collection

All incidents are considered normal priority unless they are labeled EMERGENCY. All incoming information is handled confidentially by Cisco CSIRT, regardless of its priority. Cisco CSIRT supports the Information Sharing Traffic Light Protocol (ISTLP). Information that arrives with the tags WHITE, GREEN, AMBER, or RED will be handled appropriately.

For more information on ISTLP, refer to:

https://www.first.org/tlp/docs/tlp-v1.pdf

Cisco CSIRT collaborates with FIRST, the National Safety Information Exchange (NSIE), the Defense Security Information Exchange (DSIE), and the DNS Operations Analysis and Research Center (DNS-OARC).

External and internal users can make reports to CSIRT by submitting an incident reporting email notification to Cisco CSIRT management and investigators team email address: csirt-notify@cisco.com.

For more information on the Cisco CSIRT RFC 2350 Profile, refer to:

https://www.cisco.com/c/en/us/about/security-center/computer-security-incident-response-team-csirt.html

Reporting a Data Incident

Cisco has a Data Protection Program Incident Response Team that responds to possible data incidents 24 hours a day, seven days a week. Cisco provides a data incident reporting tool. Once a new incident is submitted, a Data Protection Incident Investigator is assigned and reviews the Incident. The following steps are taken in response to the data incident submitted:

- Investigation: After the new incident is created, CSIRT & DPP incident investigators evaluate the incident to better understand the impact. Once confirmed as a data incident requiring escalation, the DPP Incident Response Team is assembled to:
  - Review the incident
  - Develop a response plan
  - Resolve the incident with the data protection specialists from the impacted organization
- Remediation: The Incident Commander is the leader of the resolution efforts to ensure that both the Root Cause and Corrective Actions are identified. This results in the

Incident Response team working cross company to ensure appropriate actions by the impacted organization. The Cisco Data Protection team responds to data issues promptly, however we are committed to creating a culture of data protection. Mistakes do not result in reprimand and prompt recognition and reporting is advocated. The best chance of minimizing a data handling error is though quick recognition and engagement of the Data Protection team.

- Communication & Awareness: Incident Commander is responsible for ensuring all relevant and interested parties are aware of the situation. They will brief both the Cisco executive and functional staffs as appropriate. Other responsibilities of the Incident Commander include:
  - Document response learnings
  - Create training materials where appropriate
  - Roll out materials and new practices with the Incident Investigator

Supplier Management

Cisco's Supplier Management program begins with the corporate controls governing the procurement organization. Suppliers enter into an agreement which covers supplier duties, services, license and intellectual property rights, confidentiality, integrity, and availability. Suppliers are required to report information security events. Agreements include security requirements and Service Level Agreements.

After complying with the corporate procurement process, products' key suppliers are subject to annual reviews. These cover the handling of non-public information, legal review, budget for the previous and next year, the security of the system, external certifications, as well as pertinent organizational structure reviews if they will affect the stability of the vendor.

If a supplier is a cloud service provider, the product team must ensure that this product is evaluated by Cisco's third party security assessment program. This program is the CASPR/CASPRX process. CASPR/CASPRX assessments evaluate the security risks to Cisco from use of a supplier's product or service, and provide recommendations. The benefits include validation of the supplier's security architecture for compliance with Cisco policies and standards, a proactive and predictable process, and the protection of Cisco data and brand.

Personnel Management

Cisco human resource policies, procedures, and guidelines apply to all Cisco permanent, temporary, and contract personnel. Personnel management requirements include background checks, Code of Business Conduct review, and education and training.

Cisco requires that newly hired employees certify that they have reviewed, understand, and agree to confidentiality and data protection policies and guidelines by signing the Code of Business Conduct (COBC). Contractor companies are required to sign a contract including terms and conditions with confidentiality and non-disclosure restrictions.

The confidentiality policies and restrictions identify and address the following:

- Requirement to protect confidential company, former employer, and third party information and inventions
- Duration of coverage
- Terms for information to be returned or destroyed at contract cessation

- Expected actions to be taken in case of a breach of the contract or policies

Background Checks

Background checks are conducted on anyone who requires badge access to Cisco facilities, electronic access (email, intranet access, etc.), or any access to Cisco's confidential, proprietary or intellectual data. This includes pre-employment background investigations on all Cisco employees, and pre-access background investigations on all non-employees (temporary workers, contractors, consultants, vendors and access-only individuals).

Anyone receiving access to Cisco facilities, systems, or sensitive information must meet Cisco's background check standards. Any applicant who refuses to complete the background check process will not be eligible for Cisco employment or Cisco access. Cisco complies with all applicable federal, state and local laws, including fair employment practices and equal employment opportunity, when conducting background checks. All pre-employment and pre-access background checks are individually assessed.

The below pre-employment screenings are conducted for Regular Cisco hires:

- SSN Trace (US only)
- Criminal Felony & Misdemeanor (7 year history, as local law permits)
- We conduct background checks in all countries but some countries are exempt from the criminal check component. Our exempt countries are listed below:
- Criminal investigations are conducted in all countries except where not permitted by local laws and regulations: EXEMPT from criminal check only - Belgium, Brazil, Canada, Chile, Croatia, Cuba, Finland, France, Germany, Greece, Guyana, Hungary, Iran, Ireland, Italy, Japan, Kazakhstan, Netherlands, Norway, Poland, Russia (CIS), Slovenia, Sudan, Sweden, Syria, Ukraine, Venezuela.
- Federal Criminal (US only)
- Education (highest degree claimed, excludes high school diploma)
- Employment (past 3 employers, up to last 7 years, current employer not verified)
- Prohibited Parties/OFAC

Pre-access background checks for non-employees

Pre-access background checks must be conducted on any non-employee (temporary worker, contractor, consultant, vendor or access-only individual) who requires badge access to Cisco facilities, electronic access (email, intranet access, etc.), or any access to Cisco's confidential, proprietary or intellectual data. The Supplier is responsible for initiating the background check with one of Cisco's preferred background screening vendors and assumes all costs incurred in the background screening process. Cisco does not initiate nor complete background checks for non-employees. Background checks must be completed no earlier than 6 months prior to the non-employee's start date.

The below pre-access screenings are conducted for non-employees:

- Criminal Felony & Misdemeanor (7 year history, as local law permits)

We conduct background checks in all countries but some countries are exempt from the criminal check component. Our exempt countries are listed below:

- Criminal investigations are conducted in all countries except where not permitted by local laws and regulations: EXEMPT from criminal check only - Belgium, Brazil, Canada, Chile, Croatia, Cuba, Finland, France, Germany, Greece, Guyana, Hungary, Iran, Ireland, Italy, Japan, Kazakhstan, Netherlands, Norway, Poland, Russia (CIS), Slovenia, Sudan, Sweden, Syria, Ukraine, Venezuela.

- Federal Criminal (US only)
- Prohibited Parties/OFAC

Nondisclosure Agreement

All Cisco employees, vendors, and contractors who require access to Cisco facilities, systems, or sensitive information are required to sign a confidentiality and a nondisclosure agreement (NDA) before being granted access.

Additionally, the Cisco Acceptable Use Policy describes user responsibilities and establishes expected behavior when using all of Cisco systems, devices, application, and services (including cloud services). All users, including employees, vendors, and contractors are required to follow the rules of behavior. The agreements are put in place to protect trade secrets, sensitive, and business confidential information and assets.

The NDA includes statements regarding information and asset protection responsibilities. They also describe the penalties for the violation of these responsibilities. Additionally communicated is the fact that the user's security responsibilities extend outside of the work site, beyond the standard operating hours of their employment and continue for a defined period after employment ends. Signed confirmation from users indicating understanding and agreement is required prior to their gaining access to Cisco facilities, systems, or sensitive information.

Code of Business Conduct

Cisco requires all employees to certify annually that they have reviewed, understood, and agreed to the confidentiality and data protection policies and guidelines as set forth in the Cisco Code of Business Conduct (COBC). The COBC sets guiding principles governing Cisco personnel behavior with respect to ethics, legal compliance, safeguarding proprietary and confidential information, conflicts of interest and other relevant areas. New hires are required to review and acknowledge the Cisco Code of Business Conduct. Contractors are required to review and agree to a confidentiality agreement with their employer as a condition of working at Cisco.

Education and Training

Cisco requires all permanent, temporary and contract personnel to take the following education and training, as applicable, in support of external security certifications:

- Security Awareness Training – This is annual training prepared by Cisco's Data Protection and Privacy team which features different security topics each year. All applicable personnel are required to take this training annually.
- Cisco Ninja White Belt Training – This is one-time training on security fundamentals. All applicable personnel are required to complete this training.

Controls for Cisco Webex Teams service

Cisco Webex is a cloud collaboration platform that provides messaging, calling and meeting features. The Cisco Webex Teams application is a client app that connects to this platform, and provides a comprehensive tool for teamwork. Users can send messages, share files, and meet with different teams, all in one place.

Figure: Cisco Webex Teams Messaging

System and Boundary Definition

Cisco Webex Teams is a portfolio of capabilities that provides a collaboration suite. The following are in scope for this report:

- Cisco Webex Teams service (“Platform”)
- Cisco Webex Control Hub (“Control Hub”)
- Cisco Webex for Developers (“API”).

Cisco Webex Teams service

The Platform production and operations systems provide a set of services as a Platform as a Service (PaaS) that are used by applications, integrations and bots. The Platform is a highly-scalable public cloud system that offers data, operations, logging, monitoring and alerting services. The Platform uses global cloud Infrastructure as a Service (IaaS) from several Cloud Service Providers (CSPs.)

Cisco Webex Control Hub

The Control Hub provides functionality for administration of customer companies, partners and users. Control Hub is used to administer users and to configure settings at an organizational level (e.g. domains, SIP addresses, directory synchronization, and authentication). Control Hub

provides status and reports of services, spaces, users, devices, etc. Control Hub is comprised of a user interface and backend services.

Cisco Webex for Developers

Cisco Webex for Developers provides an Application Programming Interface (API) for access to the Platform in order to develop applications, integrations and bots. The API is available through standard secure internet protocols. Cisco internal and external customers can develop applications, integrations and bots that utilize the messaging and file repository capabilities of the Platform.

Infrastructure

The Platform provides data, operations, logging, monitoring & alerting services for the applications, integrations and bots. Platform architecture and operations features are integral to the system and provide secure access to the system components; manage security vulnerabilities; respond to security and operational events; and ensure robust operation.

The Platform architecture is designed as a Platform as a Service for applications, integrations and bots. The architecture is organized in subsystems providing logical and physical separation of capabilities. There are primary and alternate sites for the Platform, Key Management Service and each of the subsystems.

The Platform utilizes secure baseline configurations for operating systems, key components and network devices. These images are hardened and follow the general rule of least functionality where ports and services are only used if required. The systems are patched as part of regular maintenance. Vulnerability scanning and assessments are performed continuously.

The Cloud Service Provider's network segregates and isolates the Platform network from other tenants' networks. Each Platform location creates a trusted environment for the servers. The Platform uses storage provided by the Cloud Service Providers. Customer data is encrypted prior to storing. Direct access to the Platform and storage is by trusted Platform team members only.

Data

End-to-end encryption is used to protect messages and content. Messages are encrypted upon creation and remain encrypted until they are received by other users, where they are decrypted on those users' devices. There is a Key Management Server (KMS) for consumer users. Enterprise users can implement their own KMS if desired.

A custom data retention period for an organization can be set using the Webex Control Hub Pro Pack. Administrators can set the retention period in increments of one month. After the retention period is reached, all the content (messages, activities, files) is purged and becomes irretrievable. Data in the Platform resides in the USA. There is an established incident response procedure for handling suspected and actual data breach, data loss, and computer security incidents at Cisco. Suppliers enter into Agreements, which cover supplier duties, services, intellectual property rights, confidentiality, integrity, and availability.

Procedures

Cisco Webex Teams has a formal procedure for requesting, removing, and reviewing access to system components. The Platform controls access to service instances with local and periphery firewalls. Console access to virtual machine operating systems is secured by asymmetrical key encryption and network security devices.

Cisco Webex Teams has a formal change management process to ensure changes to production are tested, approved, reviewed and function in accordance with platform specifications.

Assets are tracked and managed in order to ensure security processes such as vulnerability scanning are performing properly. The Platform assets are virtual machines, virtual network devices, open source software, third party software and enterprise software.

Availability

The Cisco Webex Teams system is architected for high availability using multiple Platform sites. In the event a site becomes unavailable, the workload will be distributed to the remaining sites. When the site becomes available again, the site will be included in the workload distribution.

Cisco Webex Teams has a formal Business Continuity Plan (BCP) in the event that all production Platform sites becomes unavailable and are expected to remain unavailable. In the event of a disaster, the Business Continuity Plan will be executed to restore service.

Confidentiality and Privacy

Cisco Webex Teams is committed to protecting the customer's Confidential Information as defined in the Cisco Universal Cloud Agreement.

Cisco will use personal data consistent with the Webex Teams Privacy Data Sheet. Note that the Privacy Data Sheet is additional to the Cisco Privacy Statement.

Shared Responsibility

The compliance and controls environment for the Platform, Control Hub and API is based upon the shared responsibility and governance of:

- Cisco Webex Teams
- Cloud Service Providers
- Application, integration and bot owners
- Customers

Cisco Webex Teams has established and maintains an internal control structure that monitors compliance with established policies and procedures. The Cloud Service Providers are responsible for the security, compliance and governance of their service offerings. The owners of the applications, integrations and bots that utilize the Platform are responsible for security, compliance and controls for their applications, integrations and bots, including updates, security patches, and security of data that does not reside within the Platform. Customers are responsible for the security, compliance and governance of their user accounts, account settings and other information within their control.

End of Document