Introduction
to
CloudCERT

John Howie

Chief Operating Officer, Cloud Security Alliance, and
Executive Director, CloudCERT

August, 2012

Agenda

- The need for CloudCERT
- History and Goals
- Charter and Organization
- Membership Criteria
- How CloudCERT will work
- Information Sharing
- Research and Policy Development
- Next Steps

The need for CloudCERT

- Cloud computing is very different from traditional IT
  - Characterized by massive scale, hyperconnectivity, interdependency and multi-tenancy
- Cloud providers manage environments that most IT professionals will never get to see or experience
  - No access to customer applications and data
- Incidents in the cloud typically involve more than one provider or customer
  - Requires a different type of incident response

History and Goals

- CloudCERT was conceived of at the same time as the Cloud Security Alliance (CSA)
  - Broad goal is to improve defenses of the cloud ecosystem against attackers
  - Emphasis was placed on developing CSA due to broader scope and potential impact in industry
- CloudCERT initiative was formally announced 2010
  - Working Group has been meeting once a month since January 2011

What is in a name?

- Original name of initiative was CloudCERT
  - In the US and other countries, Carnegie-Mellon University owns the right to the name ‘CERT’
  - We were asked (very politely) to stop using name CloudCERT
- Switched to CloudSIRT and began the process of licensing CloudCERT with CMU
- We now have license and are d.b.a. CloudCERT

Relationship to CSA

- CloudCERT is a CSA initiative
- There are two Memorandums of Understanding in place with the CSA
  - The first defines the relationship with the CSA
    - Similar to MoUs between ISACA, Open Grid Forum, ENISA, etc.
  - The second allows CloudCERT to use CSA services
    - Webmaster, PR, legal, administrative, etc.

Relationship to CSA (continued)

- Relationship with CSA is formally covered in Bye Laws
  - CSA Board of Directors appoints four of the seven seats on the CloudCERT Board of Directors
  - CSA has other powers to protect its interests
- CloudCERT will share research, findings from operations, and other data with CSA WGs
  - Steps will be taken to make PII and CII anonymous
  - No active operational data will be shared

Charter and Organization

- Charter finalized in March 2011 and consists of:
  - Background
  - Mission Statement
  - Principles
  - Goals
  - Membership
  - Governance
  - Resourcing

cloud security alliance

Charter and Organization

Mission Statement

Enhance the capability of the cloud community to prepare for and respond to vulnerabilities, threats, and incidents in order to preserve trust in cloud computing

Charter and Organization

Principles

- Foster an open and collaborative environment between members that supports the goal of safe and secure cloud computing
- Behave professionally and ethically both within the membership and with any external contacts
- Seek to fill gaps in knowledge and capabilities specific to cloud computing security, while avoiding duplication of effort and conflict of ownership

Charter and Organization

Principles (continued)

- Be a responsible and responsive partner to governments, law enforcement and other industry and security organizations
- Provide real value with demonstrable positive effect in achieving our mission and goals
- Strive to build trust with constituent members, third-party security organizations, and with the cloud community at large so that information will flow freely to CloudCERT

Charter and Organization
Organizational structure

- Established as a 501(c)6
- Board of Directors has seven seats
  - Four appointed by the CSA Board of Directors
    - Two of which will be CloudCERT members
  - Three directly elected by CloudCERT members
- CloudCERT members will appoint a Managing Director who reports to the Board for a one-year term

Charter and Organization
Organizational structure (continued)

- The Managing Director will work with member organizations to form three committees
  - Membership committee
  - Ethics committee
  - Research committee
- Additional committees will be formed at the discretion of the CloudCERT Board and Managing Director working together

Membership Criteria

- CloudCERT membership will be limited to qualifying organizations in the following categories only
  - Cloud Providers
  - Telecommunications providers
  - CERTs, CSIRTs and ISACs (and similar)
- Other organizations can join upon approval of a two-thirds majority of the membership
- There is no cost for membership, although cloud providers are expected to be CSA members

Membership Criteria (Cloud providers)

- Must offer Public, Private or Community clouds, with one or more of IaaS, PaaS or SaaS
- Must maintain a permanent, dedicated Incident Response team
- Must hold a direct relationship with their customers
- Must meet or exceed revenue thresholds from cloud services, or a number of unique end-user seats
- Must own and manage the infrastructure used to provide service to customers

Membership Criteria (Telecommunications providers)

- Must provide carrier-class backbone and/or long-haul network connections over which public IP traffic is routed
- Must have established peering relationships with other telecommunications providers
- Must maintain a permanent, dedicated Incident Response team
- Must not route IP traffic solely or in the majority for consumer or small-business oriented ISP line of business

Membership Criteria (CERTs, CSIRTs and ISACs)

- Must be established by statute or regulation, or be recognized or designated as a national or regional CERT/CSIRT by the national or regional government with jurisdiction

Or

- Must be recognized by a national or regional CERT/CSIRT as an industry CERT or ISAC

How CloudCERT works

- Member organizations will exchange operational threat information with other members, including
  - Attacks against infrastructure
  - Malicious activity detected
  - Evidence of compromise of another member
- Members will share information necessary to defend themselves and other members
  - Source of attacks, signatures and patterns, account names, etc.

How CloudCERT works (continued)

- Information sharing is largely done by email and phone
- CloudCERT is participating in IODEF/RID/MILE Working Groups and automation is seen as a key to long-term success
  - Especially as most IR teams at Cloud Providers are Tier 2 or Tier 3 Support

How CloudCERT works (continued)

- Information shared may include sensitive information such as personal data/PII, financial information, etc.
  - CloudCERT continues to study how best to handle this data and share it legally
- All members sign a multi-party NDA that protects the confidentiality of information shared
- Detailed Operations Guide will be developed and maintained by members

Information sharing

- CloudCERT will share information in three ways
  - Between member organizations as part of routine operations
  - With the CSA and its WGs to enable and further research
  - Externally to the public, to governments, and to industry
- Not all information will be shared in all ways, nor simultaneously

Information Sharing

Lexicon

- The WG came up with a lexicon for sharing information and designed to ease member communications
  - Defines the following:
    - Basic terms such as Asset, Attack, Event, Incident, Threat and Vulnerability, etc. (ISO/IEC 27000:2009)
    - Incident categories including DoS, Malicious Code, Unauthorized Access, etc. (NIST SP800-61rev1)
    - Attack types such as Reflector and Flood Attack, Virus, Worm, Trojan, etc. (NIST SP800-61rev1)

Information Sharing
Lexicon (continued)

- Lexicon is open, extensible and will be routinely updated as it makes sense
- Freely available for adoption and use outside of CloudCERT
- Will be contributed to CSA as some of first research from CloudCERT

Information Sharing

Traffic Light Protocol

- CloudCERT uses a Traffic Light Protocol
  - Red: Information is limited to named recipient(s) or members in attendance at meeting when disclosed
  - Yellow/Amber: Information may be shared on a "need to know" basis, and only to those in recipients' organizations or other CloudCERT members
  - Green: Information may be freely shared with others in recipients' organizations or other CloudCERT members
  - White/None: No restriction on redistribution

Information Sharing

Traffic Light Protocol (continued)

- All information shared without a specific traffic light color will be deemed to be Yellow / Amber
- Senders and originators of information should provide the color assigned to the information in the Subject of email addresses, or on every page of a document
- The color assigned to information shall remain in force indefinitely, or until the sender or originator changes it
- Sender or originators of information will not comingle information into a single message or document with different traffic light colors

Information Sharing
External communications

- All information shared externally will be unrestricted information (TLP White), but may be copyrighted
- CloudCERT will publish all information through its website, come from an authorized email address, or via Twitter
  - Details will be posted on the CloudCERT website

    Web: http://www.CloudCERT.org

    Twitter: @CloudCERT

Information Sharing
Third Parties

- During operations CloudCERT members come across data that we would like to share, such as lists of:
    - Usernames and passwords
    - Credit Card numbers
    - Social Security or other National Identifier information
- Statutes and regulations inhibit sharing of this data
- CloudCERT will work to establish protocols to share this information and to define policy to enable it

Research and Policy

- CloudCERT will contribute to CSA WGs
  - Principally the Guidance Domain 9: Incident Response
  - Other domains such as Domain 3: Legal Issues: Contracts and Electronic Discovery will benefit too
- CloudCERT will contribute to external research specific to its focus and consistent with its Charter
  - Industry WGs
  - Academia

Research and Policy (continued)

- CloudCERT will contribute to Policy through
  - Directly and indirectly (as part of a CSA effort) to respond to requests and solicitations for input from Policy Makers
  - Publication of incident reports and other materials developed as part of operations
    - All materials will be scrubbed to remove PII and CII
- CloudCERT's primary focus will be operations and not research and development

Research and Policy (continued)

- CloudCERT is currently contributing to the ENISA Network of Excellence initiative
  - Partners include academia, industry, and organizations such as UNICRI
- CloudCERT has met with UNICRI and will likely contribute long-term to its mission
- CloudCERT will evaluate IETF, ITU-T CYBEX and other standards for use in operations
  - Will provide feedback and contribute to initiatives

Next Steps

- CloudCERT has been accepting membership applications since the beginning of the year
  - Members of the WG have been working together cooperatively on mutual issues and incidents since the early days of CloudCERT
- Members and WG will continue collaborate to develop Operations Guide and other collateral IP
- CloudCERT is talking to several governments about accepting funding and establishing offices to partner with research institutions

More Information

- For more information please visit the website

  http://www.CloudCERT.org

- Sign-up for announcements

  announce@lists.cloudcert.org

- Follow CloudCERT on Twitter

  @CloudCERT

- Contact us: jhowie@cloudsecurityalliance.org

Thank you!