

The Vericept Categories

The table below lists the Vericept pre-defined Risk Categories.

Information Privacy and Compliance Categories	
Category Name	Description
Confidential	This Category is designed to detect secretive or encrypted communications that should not be sent across or exchanged using the organization's infrastructure. Such traffic can address a wide range of sensitive matters, including conspiratorial cliques, the leaking or selling of sensitive or proprietary information, hidden power plays, negotiations or covert communications with competitors, cover-ups, and the conduct of an individual's private enterprise hosted on the organization's network.
Credit Card Number	This Category will capture transmission of credit card numbers, in combination with any required expiry date, security code, access code, or password that would permit access to an individual's financial account. Further accuracy is provided by examining the detected CCN numbers for validity. Note that this is a direct requirement of recent state legislation protecting the "Personal Information" of residents and disclosing any security breaches.
Disgruntled Employee	This Category is designed to detect disgruntled employees who may be prone to leaking sensitive company secrets. It monitors suspicious employee language and activity for patterns consistent with antagonistic employees and information exposures. Awareness of such exposure can provide managers the information needed to mitigate the risk.
Encrypted – IM	Detects the use of encrypted AOL Instant Messaging sessions. This category is for detection purposes only and will not decrypt any of the content.
Encrypted – PGP	Detects the use of PGP/MIME: or MIME Type - PGP (PGP encrypted attachments). This category is for detection purposes only and will not decrypt any of the content.
Encrypted - S/MIME	Detects the use of Secure Multi-Purpose Internet Mail Extensions. This category is for detection purposes only and will not decrypt any of the content.
Encrypted – SSL	Detects the use of Secure Socket Layer communication for web services. This category is for detection purposes only and will not decrypt any of the content.
Encrypted – SSH	Detects the use of Secure Shell. This category is for detection purposes only and will not decrypt any of the content.
Encrypted – Other	Detects password protected Zip or Excel spreadsheets. This category is for detection of these types of attachments only and will not perform any analysis on the contents of the password protected attachment.
HL7 – Health Level 7	This category detects transmission of unencrypted HL7 messages. HL7 is a standard in the medical industry used for storing and interchanging clinical and administrative data. HL7 messages contain patient data that is used to indicate/change the patient's status. For example, a patient is admitted or discharged. This category will not capture examples that are listed on web sites (http-response).
Information Hiding Research	This Category will capture research on tools for steganography, digital watermarking, and methods of hiding information.
Mergers & Acquisitions	This Category can alert management to careless or malicious network traffic during negotiations regarding mergers and acquisitions. It can also be useful during the mandatory Quiet Period preceding an Initial Public Offering.

Information Privacy and Compliance Categories (continued)

PHI - Protected Health Information <i>Premium Vericept Category</i>	The HIPAA Privacy Rule requires healthcare organizations implement policies, procedures and technical measures to ensure that only authorized individuals have access to Protected Health Information (PHI). This Category is designed to identify PHI leaks by recognizing such things as Social Security Number, telephone number, address, city, or zip code, Medical Account number, date of birth, and date of Admission or Release.
Personal Information <i>Premium Vericept Category</i>	This Category detects communications of unencrypted personal information such as home addresses, mother's maiden names, bank account information, and so on.
Resignation	This Category fosters awareness of active job searches by an organization's employees. It also captures expressions of staff discontent that may lead to resignations. Awareness of such activities can empower managers to correct adverse conditions or defuse conflict in the workplace as well as to save and retain valued employees. Furthermore, when an employee is known to be seeking work in the same field, employers may want to pay close attention to the handling of proprietary information.
Social Security Number	This Category detects the presence of Social Security Number in communications. The Vericept solution utilizes data obtained from the U.S. Government to identify only those numbers that have been issued. Regular updates to this data are available directly from Vericept as a part of the normal update monitoring process. Note that this is a direct requirement of recent state legislation protecting the "Personal Information" of residents and disclosing any security breaches.
Source Code – C/C++/Java	Captures transmission of C, C++ and Java code. Excludes HTTP response.
Source Code – COBOL	Captures transmission of COBOL code. Excludes HTTP response.
Source Code – Perl	Captures transmission of Perl Code. Excludes HTTP response.
Source Code – Visual Basic	Captures transmission of Visual Basic code. Excludes HTTP response.

Acceptable Use Categories

Category Name	Description
Adult	This Category is frequently the most dramatic and troublesome for organizations. The volume of pornographic traffic on an organization's network is shocking to most managers and can be challenging to manage. Given the trend in current case law, a simple glimpse of pornography on a coworker's screen may support a legal finding that the organization is tolerating or even promoting a hostile environment.
Conflict	This Category identifies unusual levels of personnel stress, anxiety, and inter-personal hostility through the use of threatening, bullying, or vulgar language. Detection of such conflictive communications is essential to preserving the safety of the workplace.
Gambling	This Category is designed to detect gambling information, including sites and bets where no money is exchanged. Many managers view online gambling as a serious threat as it can place an individual's stability in jeopardy through the loss of time and money. It reduces productivity and can make an employee susceptible to temptation with regard to theft, offers from competitors, and other misuses of organizational assets. In addition, online gambling sites often display pornographic materials, thus exposing the organization to even higher risk.

Acceptable Use Categories (continued)	
Games	This Category is designed to capture discussions of games, sites with advice or tips and tricks for games, newsgroups and chat rooms concerning games, and other game-related content. It will detect communications about fantasy role playing games, video games, and computer games. This category is often considered harmless, but can result in tremendous loss of productivity.
Gangs – Education Only	This Category identifies gang-related activity to help address school safety and violence prevention. It includes web research on gangs, conflictive language used in communications and other indicators of gang activity.
P2P Research	This Category detects searches for Peer-to-Peer applications in web search engines, instant messages, email, Web-based email and chat rooms.
Plagiarism – Education Only	This Category detects attempts at academic dishonesty, such as efforts to purchase term papers or book summaries. In addition, it captures any communications discussing cheating techniques, queries for homework help, requests for copies of tests, and so on.
Racism	This Category alerts managers to racist attitudes and practices that may constitute a threat to the stability of the organization or make the organization legally vulnerable. They range from the improper, illegal, or unfair human resource practices to the behavior of individuals, groups, and cliques who invite and foster subtle intra-organizational strife.
Shopping	This Category captures exceptions that contain shopping information, including items for sale and tips for shopping smarter. Part of the challenge in dealing with shopping is that many people, including some managers, view it as harmless. The amount of captured network traffic can therefore be extensive and difficult to manage.
Sports	This Category looks for information related to sports. Sports sites often include continuous, real-time updates, video clips, and other drains on network resources. In addition, sports-oriented traffic, like pornography, is likely to be flagrant.
Streaming Media	This Category looks for instances of audio or video content that is streamed via a web-browser or media players such as Windows Media® Player, Apple QuickTime®, RealPlayer®, and Winamp. The Streaming Media category will also detect downloads of the media files that use the formats of Real Time Streaming Protocols, Shoutcast/Icecast protocol, and various other audio and video formats.
Substance Abuse	This Category detects information related to illegal or controlled substances as well as recreational substances such as alcohol and tobacco. In addition to specific substance names, this category can identify the sharing of advice on obtaining or using controlled substances, discussions about drug experiences, advice on passing drug tests or screenings, and even discussions about the merits of using controlled substances.
Trading	This Category captures information about investing in the stock market. Day trading and other forms of personal portfolio management are the primary areas of concern addressed by this category. Traders often connect to real-time, online, market-monitoring services and stay connected at all times. The Vericept solution may help identify employees who spend their time running a personal day-trading business while using company time and resources.
Violent Acts	This Category searches for overt and subtle language dealing with violence in school or at work. It is hypersensitive to email messages and message boards. In fact, it is sufficiently sensitive that it often captures intensely violent games and music lyrics.
Weapons	This Category looks at language and items used in the manufacture of homemade explosives, the use of other weapons such as guns and knives, and communications such as bomb threats or the possession of a weapon at school or work.
Insider Hacker Activity Categories	
Category Name	Description
Hacker Research	This Category detects research on exploits, worms, and miscellaneous security information.

Insider Hacker Activity Categories (continued)	
Preparation for Attack <i>Includes:</i>	Events in this Class would indicate that immediate action should be taken to prevent what could be an imminent attack. <i>Category includes:</i>
Log Wiping Code	Detects the transfer of log wiping code onto your network. This is usually indicative of an intrusion.
NMAP	Detects the output of an NMAP execution. NMAP is a network scanning utility that identifies vulnerable ports on a target server.
SAM Cracking	Detects the transfer of the Windows Security Accounts Manager database where user passwords are stored
Sniffer Code	Detects the transfer of code used by hackers to collect useful information such as usernames and passwords from the network.
Stack Smashing Code	Detects the transfer of stack-smashing programs, which make up the majority of hacker exploits.
Suspicious VNC Session	Seeks suspicious VNC session activity.
Windows Enumeration SMB	Finds responses back from a system being enumerated through the Microsoft's SMB protocol. Note: The presentation of the data to the end-user is unstructured.
Windows Enumeration Textual	Finds output from enumeration activity that occurred at the DOS shell or equivalent. Typically this output is seen internally if an attacker is enumerating a network from a compromised system inside the customer's network or an employee is attempting to enumerate their internal network.
Impending Threats <i>Includes:</i>	Events in this Class would indicate that the system appears to be compromised. Immediate action should be taken to lock down and patch, or even potentially rebuild, the system and/or affected services. <i>Category includes:</i>
Backdoors	Detects elements on a system that look like a backdoor has been installed.
Keylogger	Catches keyboard logging output. For instance if someone installs keyboard logging software or installs a physical dongle to capture keyboard activity the category captures the transmission of the keylogger file.
Root Activity	Detects the kind of <i>root</i> activity typical of hackers or intruders, rather than legitimate administrator activity.
Suspicious FTP	Detects unusual FTP activity typical of hackers or intruders.
Suspicious HTTP Response	Detects the type of HTTP responses most typical of successful Web server exploits, especially IIS exploits.
Suspicious SUID root	Detects the existence of suspicious SET-UID-ROOT programs.
Suspicious Activity <i>Includes:</i>	Events in this Class can be generated by unusual system administrator activity, non-RFC compliant client software, or hack activity. GoToMyPc activity could be legitimate, but is often disallowed by organizations, as it enables remote access to internal machines, bypassing the firewall. <i>Category includes:</i>
GoToMyPc Client	Detects GoToMyPc client activity.
GoToMyPC Server	Detects GoToMyPc server activity.
Suspicious IMAP	Seeks suspicious IMAP activity.
Suspicious POP	Seeks suspicious POP activity.
Suspicious Shell	Detects suspicious shell activity such as unusual commands often entered by hackers.
Suspicious VNC Session	Seeks suspicious VNC session activity.

Insider Hacker Activity Categories (continued)	
Unauthorized Access Attempts <i>Includes:</i>	Events in this Class are usually the result of an incorrectly entered password. However, an unusually large number of logs from the same address could be indicative of an attack. <i>Category includes:</i>
Unauthorized FTP	Detects unauthorized access attempts on a FTP server.
Unauthorized Web	Detects unauthorized access attempts on a Web server.
Unauthorized General	Looks for unauthorized access attempts other than FTP, Web, IMAP, POP.
Unauthorized IMAP	Finds unauthorized access attempts on an IMAP server.
Unauthorized POP	Finds unauthorized access attempts on a POP server.
All Instance Categories	
Category Name	Description
Instant Messaging & Chat	This Category captures and stores all instances of instant messaging or chat seen by the Vericept solution regardless of content.
Mailing Lists	This Category captures and stores all instances of mailing lists seen by the Vericept solution regardless of content.
P2P File Share	This Category captures requests for files and file transfers using Peer-to-Peer applications.
Web & Blog Postings	This Category captures and stores all instances of bulletin board postings seen by the Vericept solution regardless of content.
Web-mail Receive	This category captures and stores all instances of incoming web-based email, such as hotmail.com or yahoo.com, that are viewed by the end-user. Inappropriate incoming web-based email will also be captured by the applicable monitoring category as well as this one.
Web-mail Send	This category captures and stores all instances of outgoing web-based email, such as hotmail.com or yahoo.com, that are sent by the end-user. Uploading of file attachments to web-based email is also captured and stored by this category. Inappropriate outgoing web-based email will also be captured by the applicable monitoring category as well as this one.