ExtraHop

Updated October 2017

Addy Anomaly Detection Categories

The ExtraHop platform gathers thousands of metrics by observing communications on the network. Addy uses unsupervised machine learning to evaluate hundreds of these metrics across dozens of protocols to determine whether there are active performance or securityproblems in a customer's environment.

ADDY DETECTS ANOMALIES IN THE FOLLOWING CATEGORIES:

Authentication, Authorization, and Access Control	Network File System	Database
Email Server	Web Server	Remote Access Servers and Methods
External Communications	Network Infrastructure	Internet Communications and Telephony

Authentication, Authorization, and Access Control

PROTOCOLS: KERBEROS, LDAP, AAA, ACTIVE DIRECTORY

Addy looks for issues with users, clients, and servers attempting to log in and to access resources. Addy looks for: spikes in login or access errors that can indicate brute-force attacks, performance issues with authorization and authentication servers, and large increases in the number of entities attempting to login.

Network File System

PROTOCOLS: FTP, CIFS, NFS

Addy evaluates network file system traffic to determine whether users are having issues accessing specific files and shares, or suspicious patterns that can indicate ransomware activity or insider threats. It identifies issues by finding increases in network file system errors and large increases in requests to access specific resources on network-attached storage and file servers.

Database

PROTOCOLS: IBM DB2, IBM INFORMIX, MICROSOFT SQL SERVER, MONGODB, MYSQL, ORACLE, POSTGRESQL, REDIS, SYBASE, AND SYBASE IQ

Addy evaluates a suite of database protocols to determine whether your applications or users might be experiencing database access problems. Addy can detect if data transfers are being interrupted or when an insider threat exports large amounts of information from a database. It can also identify database login/authentication issues.

Email Server

PROTOCOLS: SMTP, SMTPS

Addy looks for unusual traffic and activity on the SMTP protocol to determine if your internal mail servers might be experiencing performance problems. For example, Addy can detect when a large number of email messages are being sent, indicating a potential malware infection or email server configuration problem.

Web Server

PROTOCOLS: HTTP, HTTPS

Addy analyzes web traffic to find unexpected spikes in various HTTP error and warning codes. These events indicate that there is a problem with a web server and/or web application, often meaning that end users are directly affected by either a slow experience or not able to access an application entirely.

Remote Access Servers and Methods

PROTOCOLS: ICA (CITRIX) AND SSH

Citrix performance is of great importance to many organizations, and Addy can detect when there are long load times or poor quality sessions for end users. Addy also evaluates SSH (secure shell) activity to determine whether an attacker may be attempting to gain access to systems and move laterally within an environment.

External Communications

PROTOCOLS: TCP, IPV4, IPV6

Addy examines communications to external IPs to detect when an attacker is controlling malware remotely or attempting to exfiltrate data out of the environment.

Network Infrastructure

PROTOCOLS: DNS, DHCP, TCP

Network infrastructure anomalies can represent performance or attackers' reconnaissance activity. Addy evaluates whether there are unusual events over the TCP protocol and in DNS servers, such as TCP SYN scans and DNS hostname lookup scans. Addy also looks for anomalous ICMP and UDP scans as well as rogue DHCP servers.

Internet Communications and Telephony

PROTOCOLS: SIP, RTP, RTCP

Addy analyzes key protocols used in Voice over IP (VoIP) communications within a network in order to detect VoIP service issues.