USE CASE

Detecting Zero Day Exploits

As technology use proliferates and enterprise IT environments become increasingly complex, the danger of exploits has grown more ominous than ever before. Most organizations are prepared to deal with known threats through the use of specific security tools, such as IDS or IPS devices, vulnerability assessment tools, and anti-malware and antivirus devices. With zero day exploits however, the source is often an unwitting internal user, and manifests in ways that are undetectable by traditional means. Many IT organizations are not adequately equipped to detect and respond to the initial threat.

When an exploit can come from anywhere, prevention and remediation require a true, global window not only into security specific event data, but operations as well. Zero day exploits are best identified by automatically recognizing aberrant behavior, and immediately alerting administrators.

LogRhythm helps administrators identify anomalous behavior patterns, perform rapid root-cause analysis, and extract accurate information needed to help defend against future exploits.

	Automated Anomaly Detection	Real-time Monitoring	Rapid Response
CUSTOMER CHALLENGE	Zero day exploits cannot be detected by conventional means, such as anti-malware or IDS/IPS devices, because signatures have not yet been created. Without specific detection capabilities, security administrators have to rely on behavior-based detection methods.	A sophisticated attack can be very subtle and specific details can go unidentified for days or weeks without the proper tools to identify the cause and impact of an attack.	A zero day exploit can impact any source – frequently an unwitting internal user or system. Locating the source is a near impossible task without the forensics capabilities to identify relevant detail.
LOGRHYTHM SOLUTION	LogRhythm can alert administrators on anomalous behavior, such as any unauthorized outbound internet activity on non white-listed ports.	LogRhythm allows administrators to run a live Tail on outbound internet activity. Administrators can easily pinpoint specific activities, such as significant communication with a single, unknown Destination IP.	LogRhythm provides multiple options for conducting forensic investigations to quickly identify the source of the zero-day exploit. Users have the option to search for focused data points, or to use visual trending and analysis to identify behavior patterns and instantly drill down into specific event details.
ADDITIONAL BENEFITS	Once a general alert is received indicating that an exploit has occurred, alarm rules can be easily modified to incorporate more specific behavior patterns to respond more quickly to similar behavior.	Tail can be quickly configured based on any criteria, using LogRhythm's simple and intuitive wizard-based setup. Any Tail can be saved for future use, providing users with a straightforward and instantaneous method for recognizing and monitoring repeat incidents.	Investigations provide the specific detail required for administrators to contain a zero day exploit, and can be saved for future use to respond to similar breaches or to rapidly discover other points of infection.