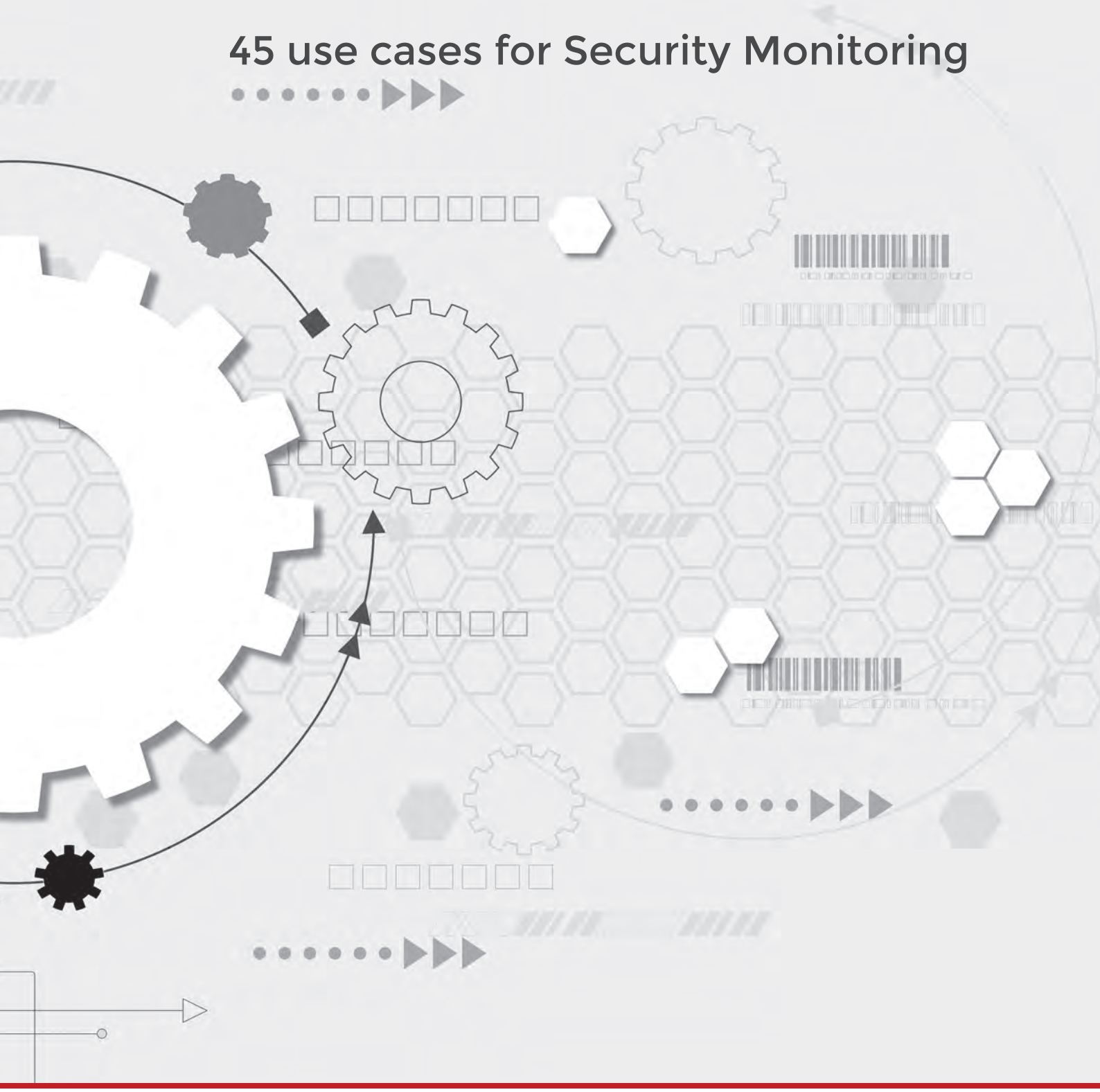
PALADION
HIGH SPEED CYBER DEFENSE

www.paladion.net

SIEM Use Cases

45 use cases for Security Monitoring



Use Case	Description
DMZ Jumping	This rule will fire when connections seemed to be bridged across the network's DMZ.
DMZ Reverse Tunnel	This rule will fire when connections seemed to be bridged across the network's DMZ through a reverse tunnel.
Excessive Database Connections	Rule detects an excessive number of successful database connections.
Excessive Firewall Accepts Across Multiple Hosts	Reports excessive Firewall Accepts across multiple hosts. More than 100 events were detected across at least 100 unique destination IP addresses in 5 minutes.
Excessive Firewall Accepts From Multiple Sources to a Single Destination	Reports excessive Firewall Accepts to the same destination from at least 100 unique source IP addresses in 5 minutes.
Excessive Firewall Denies from Single Source	Reports excessive firewall denies from a single host. Detects more than 400 firewall deny attempts from a single source to a single destination within 5 minutes.
Long Duration Flow Involving a Remote Host	Reports a flow for communicating to or from the Internet with a sustained duration of more than 48 hours. This is not typical behavior for most applications. We recommend that you investigate the host for potential malware infections.
Long Duration ICMP Flows	Detection of ICMP packets between hosts that last a long time. This is rare and shouldn't ever occur.
Outbound Connection to a Foreign Country	Reports successful logins or access from an IP address known to be in a country that does not have remote access right. Before you enable this rule, we recommend that you configure the activelist: Countries with no Remote Access building block.
Potential Honeypot Access	Reports an event that was targeting or sourced from a honeypot or tarpit defined address. Before enabling this rule, you must configure the Activelist: Honeypot like addresses building block and create the appropriate sentry from the Network Surveillance interface.
Remote Access from Foreign Country	Reports successful logins or access from an IP address known to be in a country that does not have remote access right. Before you enable this rule, we recommend that you configure the Activelist: Countries with no Remote Access building block.

Use Case	Description
Remote Inbound Communication from a Foreign Country	Reports traffic from an IP address known to be in a country that does not have remote access right. Before you enable this rule, we recommend that you configure the Activelist: Countries with no Remote Access building block. SMTP and DNS have been removed from this test as you have little control over that activity. You may also have to remove WebServers in the DMZ that are often probed by remote hosts with web scanners
Single IP with Multiple MAC Addresses	This rule will fire when a single IP's MAC address changes multiple times over a period of time.
Systems using many different protocols	Local system connecting to the internet on more than 50 DST ports in one hour. Connections must be successful. This rule can be edited to also detect failed communications which may also be useful.
Authentication: Login Failures Followed By Success to the same Destination IP	Reports multiple log in failures to a single host, followed by a successful log in to the host.
Authentication: Login Failures Followed By Success to the same Source IP	Reports multiple log in failures to a single host, followed by a successful log in to the host.
Authentication: Login Failures Followed By Success to the same Username	Reports multiple log in failure followed by a successful login from the same user.
Authentication: Login Failure to Disabled Account	Reports a host login message from a disabled user account. If the user is no longer a member of the organization, we recommend that you investigate any other received authentication messages from the same user.
Authentication: Login Failure to Expired Account	Reports a host login failure message from an expired user account known. If the user is no longer a member of the organization, we recommend that you investigate any other received authentication messages.
Authentication: Login Successful After Scan Attempt	Reports a successful log in to a host after recon has been performed against the network.
Authentication: Multiple Login Failures for Single Username	Reports authentication failures for the same username.

Use Case	Description
Authentication: Multiple Login Failures from the Same Source	Reports authentication failures on the same source IP address more than three times, across more than three destination IP addresses within 10 minutes.
Authentication: Multiple Login Failures to the Same Destination	Reports authentication failures on the same destination IP address more than ten times, from more than 10 source IP addresses within 10 minutes.
Authentication: Multiple VoIP Login Failures	Reports multiple log in failures to a VoIP PBX.
Authentication: No Activity for 60 Days	This account has not logged in for over 60 days
Authentication: Possible Shared Accounts	Detection of Shared Accounts. You will need to add in additional false positive system accounts to the and NOT when the event username matches the following ...". "
Authentication: Repeat Non-Windows Login Failures	Reports when a source IP address causes an authentication failure event at least 7 times to a single destination within 5 minutes.
Authentication: Repeat Windows Login Failures	Reports when a source IP address causes an authentication failure event at least 9 times to a single Windows host within 1 minute.
VPN Sneak Attack	Check from where remote users are connecting, and what they are accessing. A VPN connection access can be misused to gain access to the intranet.
Anomalous Ports, Services and Unpatched Hosts or Network Devices	Unusual traffic is identified as a potential intrusion; no signatures are involved in the process, so it is more likely to detect new attacks for which signatures are yet to be developed.
Brute Force Attack	Check for attempts to gain access to a system by using multiple accounts with multiple passwords.
Privileged user abuse	Monitor misuse of access of privileged user access such as admin or root access to perform malicious activities.

Advanced Use Cases

01 Unauthorized application access

- Which systems have suspicious access/application activity?
- Are terminated accounts still being used?
- Which accounts are being used from suspicious locations?
- High risk user access monitoring
- Privileged user monitoring

02 Worm/malware propagation monitoring

- Malware beacon monitoring
- CnC access monitoring
- CnC Termination monitoring
- Malware/Worm propagation monitoring
- Anti-virus status/infection trends

03 Hacker detection

- Who is attacking me and where are they attacking from?
- Which of my internal systems are they attacking?

04 VPN Sneak Attack

05 Anomalous Ports, Services and Unpatched Hosts/Network Devices

06 Brute Force Attack

07 Privileged User Abuse

PALADION

HIGH SPEED CYBER DEFENSE

ABOUT PALADION

Paladion is a global cyber defense company that provides Managed Detection and Response Services, DevOps Security, Cyber Forensics, Incident Response, and more by tightly bundling its semi-autonomous cyber platform and managed services with leading security technologies. Paladion is consistently rated and recognized by independent analyst firms and awarded by CRN, Asian Banker, Red Herring, amongst others.

For 17 years, Paladion has been actively managing cyber risk for over 700 customers from its six cyber operations centers placed across the globe. It houses 900+ cyber security professionals including security researchers, threat hunters, ethical hackers, incident responders, solution architects, consultants and more. Paladion is also actively involved in several information security research forums such as OWASP, and has authored several books on security monitoring, application security, and more.

WW Headquarters: 11480 Commerce Park Drive, Suite 210, Reston, VA 20191 USA. Ph: +1-844-507-7668
Bangalore: +91-80-42543444, Mumbai: +91-2233655151, Delhi: +91-9910301180, London: +44(0)2071487475, Dubai: +971-4-2595526, Sharjah: +971-50-8344863, Doha: +97433559018, Riyadh: +966(0)114725163, Muscat: +968 99383575, Kuala Lumpur: +60-3-7660-4988, Bangkok: +66 23093650-51, Jalan Kedoya Raya: +62-8111664399.

sales@paladion.net | www.paladion.net