Correlation Engine Use Cases and Capabilities

Generic Signature-based and Analysis Heuristic and Rule-based Analysis Machine Learning Anomaly-based Analysis Threat Intelligence Cloud and SaaS Solutions Rule-based analysis

Correlation features and Use Cases

Generic Signature-based and Rule-Based Analysis

Automated log analysis and management accelerate threat detection. There are many cases where evidence of an attack can be found in the logs of your devices, systems and applications. UTMStack can be used to automatically aggregate and analyze log data.

1. **Log-based intrusion detection:** Actively monitors and analyzes data from multiple log data points in real time.
2. **Brute-Force attack detection**: Attempts to break user credentials by performing massive requests.
3. **Denial of services:** Deny applications or systems availability by overflowing them with requests.
4. **File integrity monitoring**: For both files and Windows registry settings in real time, detects changes to the system, and maintains a forensic copy of the data as it changes over time.
5. **Rootkit and malware detection**: Process- and file-level analysis detects malicious applications and rootkits.
6. **Unauthorized attempts of privileged access usage**. Suspicious activity and privilege escalation attempts.
7. **Security policy monitoring**: UTMStack leverages SCAP. SCAP is a standardized compliance checking solution for enterprise-level infrastructure. It is a line of

specifications maintained by the National Institute of Standards and Technology (NIST) with the purpose of maintaining enterprise systems security.

8. **Compliance auditing:** Application- and system-level auditing ensures compliance with many common standards, such as PCI-DSS, CIS, HIPAA, and GLBA benchmarks.
9. **System inventory:** Collects system information, such as installed software, hardware, utilization, network services, and listeners.

- **File Classification:** Audits critical or classified files for access, changes or movement.
- **Privileged Identity Monitoring:** Alerts on suspicious activity of privilege accounts and changes on critical groups such as Administrators and Domain Admins.

Heuristic and Rule-based Analysis

1. **Impossible travel:** Logon attempts from uncommon locations or places where physical constrains wouldn’t allow the user to travel to on a reasonable time.
2. **Potentially Bad Traffic:** Potentially Bad Traffic, traffic that is definitely out of the ordinary, and is potentially indicative of a compromised system
3. **Attempted Information Leak:** Attempted information collection (reconnaissance), is a set of processes and techniques (Footprinting, Scanning & Enumeration) used to covertly discover and collect information about a target system. Information leaks or reconnaissance attacks that are classified as Attempted Information Leaks are not proof positive that an information gathering attempt has been successful.
4. **Attempted Denial of Service:** This alert belongs to the group of rules of the category "attempted-dos". A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users.
5. **Attempted User Privilege Gain:** Monitors for attackers trying to elevate privileges to an unauthorized level. An attacker who has access to a user account can make use of various types of system vulnerabilities to elevate the privileges and access data for which is not authorized.
6. **Decode of an RPC Query:** Decode of an RPC Query. Detects RPC related attacks,

vulnerabilities, logging purposes, and protocol detection. Servers running with Portmapper are susceptible to a distributed reflected denial-of-service (DRDoS) attack. Remote Procedure Call (RPC) is a protocol that one program can use to request a service from a program located in another computer on a network without having to understand the network's details.

7. **Executable Code Detection:** Executable code was detected. Detected traffic targeting vulnerabilities that are found in or delivered through executable files, regardless of platform. Remote shellcode is used when an attacker wants to target a vulnerable process running on another machine on a local network, or intranet. If successfully executed, the shellcode can provide the attacker access to the target machine across the network. A shellcode is a code that is injected into the memory of a vulnerable program in the form of a byte string.
8. **Suspicious String Detection:** A suspicious string was detected. It checks whether an individual string is likely an attempt at confusing the reader (spoof detection), such as "paypal" spelled with Cyrillic 'a' characters.
9. **Suspicious Filename Detection:** A suspicious filename was detected. These artifacts are typically associated with malware or intruder activity. The existence of winsrv.exe, svchost.exe, or svchost.dll in specific locations is typically malicious.

- **Attempted Login Using a Suspicious user**. This alert is generated due to the use of a suspicious login attempt, If successful the attacker may have gained superuser access to the host. It notifies if there’s suspicious sign-in activity for one of your users. For example: A user doesn't follow their usual sign-in pattern, such as a signing in from an unusual location, or there was a successful login from a suspended user's account.

11. **System Call Detection:** System calls are usually made when a process in user mode requires access to a resource. Then it requests the kernel to provide the resource via a system call. Most attacks that involve a file require at least two system calls. A first one to open the file and a second one to modify it.

- **Network Trojan Detection:** Discovered software code of a Trojan Network Attack. A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network. A Trojan acts like a bona fide application

or file to trick you.

- **Client Was Using an Unusual Port:** A client was using an unusual port. If an application is using an unusual port which pretends to be a normal application port, then it indicates a sign of compromise.
- **Detection of a Network Scan:** Detection of a Network Scan. They are often harbingers of future attacks.
- **Generic Protocol Command Decode:** A protocol instruction was decode. Protocol decoding is probably the most wanted feature in logic analyzers. Protocol decoding is the (automatic) process of analyzing the logic signals and interpreting it according to a specific protocol.
- **Access to a Potentially Vulnerable Web Application:** A web application is a software application that runs on a remote server. In most cases, Web browsers are used to access Web applications, over a network, such as the Internet
- **Web Application Attack**: Serious weaknesses or vulnerabilities allow criminals to gain direct and public access to databases in order to churn sensitive data . Many of these databases contain valuable information (e.g. personal data and financial details) making them a frequent target of attacks. The majority of web application attacks occur through cross-site scripting (XSS) and SQL injection attacks. TCP port 80 for HTTP supports the web traffic that web browsers receive and is the most used in web based attacks.

- **Misc Activity or Attack:** Some behavior was detected that may be considered a policy warning. Misc activity rules include detections for various traffic patterns which do not easily fit into any other specific class types. This includes detection of DNS requests to less common top level domains like .top, .win, .trade, detection of traffic to domains known to be used by adware and other potentially unwanted applications (PUAs) as well as detection of suspicious HTTP user-agent strings.
- **Generic ICMP Event**: A "ping" packet was detected. An Internet Control Message Protocol (ICMP) flood attack, also known as a Ping flood attack, is a common Denial-of-Service (DoS) attack in which an attacker attempts to overwhelm a targeted device with ICMP echo-requests (pings).
- **Potential Corporate Privacy Violation:** Potential Corporate Privacy Violation, because someone is trying to exfiltrate data over Non-Compliant DNS traffic. Detection of access to Kickass porn and it includes NSFW and porn content. NSFW is an abbreviation for words like Not Suitable For Work, but mostly accepted as Not Safe For Work.

- **Attempt to Login by a Default Username and Password:** Attempt to login by a default username and password. The initial stages of most attacks involve the enumeration of legitimate system and user identities, a process that is necessary to determine vulnerabilities so that an exploit can be attempted
- **Targeted Activity:** Refers to unauthorized changes by software to the operating system, registry entries, other software, or files and folders.
- **Exploit-kit:** An exploit kit is a toolkit which can probe for and run exploit code that takes advantage of vulnerabilities to gain unauthorized access or control of a computer or device.
- **External IP Check:** Device Retrieving External IP Address Detected. Hacked IP addresses can also be used for DDoS attacks (“distributed denial-of-service”)
- **Domain Check:** Domain Observed Used for C2 Detected. C2 is the command and control malware domain. It is used to download payloads, or perform data exfiltration
- **Pup Activity:** A Potentially Unwanted Program, also called in short as PUP, is a software that contains adware, installs toolbars or has other unclear objectives.
- **Credential Theft:** Successful Credential Theft Detected. It is the process of stealing credentials. The first stage of a credential-based attack.
- **Social Engineering:** Possible Social Engineering Attempted. A malicious activity accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.
- **Coin mining:** Crypto Currency Mining Activity Detected. The most common way to mine cryptocurrency on standard hardware is to install Crypto mining client software and leave it running in the background.
- **Command and control:** Malware Command and Control Activity Detected. A command-and-control [C&C] server is a computer controlled by an attacker or cybercriminal which is used to send commands to systems compromised by malware and receive stolen data from a target network. It can be used to disseminate commands that can steal data, spread malware, and disrupt web services.

Machine Learning Anomaly-based Analysis

The Machine learning module creates baselines for metrics such as Network traffic, user behavior, common applications and processes. This baselines allow the engine to define patterns of what can be considered “normal infrastructure and environment activity”.

When a certain process or user behavior falls outside the baseline, then a “rule” violation occurs and the Machine learning algorithm correlates it. If the result of the correlation throws a risk level higher than 1 (informative event), an alert is generated for further investigation.

Machine learning module currently monitors:

- User behavior
- Firewalls behavior
- IPS Logs
- Network Activity
- VPN activity
- Logs from all Systems

Threat Intelligence

Analyses all available security IP Feeds, mainly related to on-line attacks, on-line service abuse, malwares, botnets, command and control servers and other cybercrime activities.

To accomplish this, we include the following IP lists:

Fullbogons: includes IPs that should not be routable in the Internet. It includes bogons which lists private and reserved IPs, but it also includes IPs that are allocated to a local registry, but they are not currently assigned to anyone, ISP, corporation, or end user.

Spamhaus: drop and drop: DROP and EDROP are advisory "drop all traffic" lists, consisting of netblocks that are "hijacked" or leased by professional spam or cyber-crime operations (used for dissemination of malware, trojan downloaders, botnet controllers).

Dshield: summarizes the top 20 attacking class C (/24) subnets over the last three days. The Internet Storm Center of SANS Institute, collects firewall and IDS logs from hundreds of thousands of computers around the globe

Malware lists - the Command and Control IPs: There are several malware lists that are very focused. They only track IPs that are actively used by specific malwares or trojans. We include most the Abuse.ch and Bambenek Consulting lists. Namely: feodo,sslbl, zeus_badips, bambenek_c2 which includes all Bambenek Consulting lists

Cloud and SaaS Solutions Rule-based analysis

All UTMStack modules apply to SaaS and Cloud environments. However, there are specialized rules for monitoring these environments.

1. **API management monitoring:** Detects suspicious activity or attempts to get information from Cloud APIs
2. **Unauthorized Resources access**: Attempts to access resources that are misconfigured or exposed to the Internet.
3. **SaaS and PaaS specific rules:** Rules created to address specific known threats on SaaS applications and PaaS.