ElastAlert: unauthorized_login_outside_business_hours_admin_users

1 message

<rangammabokka46@gmail.com> Fri, May 16, 2025 at 11:18 PM
Reply-to: rangammabokka46@gmail.com
To: rangammabokka46@gmail.com

```
unauthorized_login_outside_business_hours_admin_users

@timestamp: 2025-05-16T17:47:10.724Z
_id: tCg12pYBvjY1DP6yEbjz
_index: .ds-winlogbeat-8.10.2-2025.05.14-000001
agent: {
    "ephemeral_id": "8e853c93-bbea-4fda-b422-6aff76d97f54",
    "id": "e5e3a761-acc3-41a2-88c5-ee2b2b236970",
    "name": "Viticm-SOC",
    "type": "winlogbeat",
    "version": "8.10.2"
}
ecs: {
    "version": "1.12.0"
}
event: {
    "action": "logged-in",
    "category": [
        "authentication"
    ],
    "code": "4624",
    "created": "2025-05-16T17:47:11.797Z",
    "ingested": "2025-05-16T17:47:13.261962600Z",
    "kind": "event",
    "module": "security",
    "outcome": "success",
    "provider": "Microsoft-Windows-Security-Auditing",
    "type": [
        "start"
    ]
}
host: {
    "architecture": "x86_64",
    "hostname": "viticm-soc",
    "id": "7e25c1a1-4745-47c6-abe9-ec7f50bf1d98",
    "ip": [
        "fe80::2674:6aaf:881:b09b",
        "192.168.52.131"
    ],
    "mac": [
        "00-0C-29-C5-7F-10"
    ],
    "name": "viticm-soc",
    "os": {
        "build": "19045.5854",
        "family": "windows",
        "kernel": "10.0.19041.5848 (WinBuild.160101.0800)",
        "name": "Windows 10 Home",
        "platform": "windows",
        "type": "windows",
        "version": "10.0"
    }
}
log: {
    "level": "information"
}
message: An account was successfully logged on.

Subject:
        Security ID:        S-1-5-18
        Account Name:       VITICM-SOC$
```

```
	Account Domain:		WORKGROUP
	Logon ID:		0x3E7

Logon Information:
	Logon Type:		5
	Restricted Admin Mode:	-
	Virtual Account:		No
	Elevated Token:		Yes

Impersonation Level:		Impersonation

New Logon:
	Security ID:		S-1-5-18
	Account Name:		SYSTEM
	Account Domain:		NT AUTHORITY
	Logon ID:		0x3E7
	Linked Logon ID:		0x0
	Network Account Name:	-
	Network Account Domain:	-
	Logon GUID:		{00000000-0000-0000-0000-000000000000}

Process Information:
	Process ID:		0x334
	Process Name:		C:\Windows\System32\services.exe

Network Information:
	Workstation Name:	-
	Source Network Address:	-
	Source Port:		-

Detailed Authentication Information:
	Logon Process:		Advapi  
	Authentication Package:	Negotiate
	Transited Services:	-
	Package Name (NTLM only):	-
	Key Length:		0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).

The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.

The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.

The impersonation level field indicates the extent to which a process in the logon session can impersonate.

The authentication information fields provide detailed information about this specific logon request.
	- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event.
	- Transited services indicate which intermediate services have participated in this logon request.
	- Package name indicates which sub-protocol was used among the NTLM protocols.
	- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
num_hits: 54
num_matches: 4
process: {
  "executable": "C:\\Windows\\System32\\services.exe",
  "name": "services.exe",
  "pid": 820
}
related: {
  "user": [
    "SYSTEM",
    "VITICM-SOC$"
  ]
}
source: {
  "domain": "-"
}
user: {
  "domain": "NT AUTHORITY",
  "id": "S-1-5-18",
  "name": "SYSTEM"
}
winlog: {
  "activity_id": "{0199f395-c689-0000-79f5-990189c6db01}",
  "api": "wineventlog",
  "channel": "Security",
  "computer_name": "Viticm-SOC",
  "event_data": {
    "AuthenticationPackageName": "Negotiate",
    "ElevatedToken": "%%1842",
    "ImpersonationLevel": "%%1833",
    "IpAddress": "-",
    "IpPort": "-",
    "KeyLength": "0",
    "LmPackageName": "-",
    "LogonGuid": "{00000000-0000-0000-0000-000000000000}",
    "LogonProcessName": "Advapi  ",
    "LogonType": "5",
    "RestrictedAdminMode": "-",
    "SubjectDomainName": "WORKGROUP",
    "SubjectLogonId": "0x3e7",
    "SubjectUserName": "VITICM-SOC$",
    "SubjectUserSid": "S-1-5-18",
    "TargetDomainName": "NT AUTHORITY",
    "TargetLinkedLogonId": "0x0",
    "TargetLogonId": "0x3e7",
    "TargetOutboundDomainName": "-",
    "TargetOutboundUserName": "-",
    "TargetUserName": "SYSTEM",
    "TargetUserSid": "S-1-5-18",
    "TransmittedServices": "-",
    "VirtualAccount": "%%1843"
  },
  "event_id": "4624",
  "keywords": [
    "Audit Success"
  ],
  "logon": {
    "id": "0x3e7",
    "type": "Service"
  },
  "opcode": "Info",
  "process": {
    "pid": 828,
    "thread": {
      "id": 5612
    }
  },
  "provider_guid": "{54849625-5478-4994-a5ba-3e3b0328c30d}",
  "provider_name": "Microsoft-Windows-Security-Auditing",
  "record_id": "35056",
  "task": "Logon",
  "version": 2
}
```