FEATURE

Event Category Catalog for SOC Use Cases

The majority of modern organizations have embarked on the path security operations centers (SOCs) are building. Today, the SOC is not a modern trend; it is a forced restructuring and reorganizing of existing information security or cybersecurity departments. The fact is, the number of incidents is growing continually and the number of threat types is growing year by year, so information security professionals have to orient their information security or cybersecurity services primarily to the detection of incidents, and only then can everything else follow. This situation is well illustrated by these words: "There are two types of companies: those that have been hacked, and those that don't yet know they have been hacked."[1]

SOC and Use Cases

A SOC is a set of staff, processes, technologies and facilities that is primarily focused on identification (detection) and response to cybersecurity incidents that arise as a result of cybersecurity threat realizations. It is widely understood that, unfortunately, it is impossible to cover and resist all types of existing cybersecurity threats since resources are restricted, and, therefore, it is necessary to prioritize actions and projects. The discussion of use cases within SOCs starts here—a mechanism for consistent selection and implementation of cybersecurity incident detection scenario rules, tools and response tasks.
A use case can be considered as a specific condition or event (usually related to a specific threat) to be detected or reported by the security tool. It is an analog of a cybersecurity threat model or cybersecurity risk registry, but oriented in the cybersecurity incident management process within the SOC.

The life cycle of use cases (i.e., the use case process) includes:

1. Design of the use case
2. Development of the use case
3. Implementation of the use case
4. Application of the use case

The main component of use cases is a cybersecurity incident detection scenario rule (i.e., a correlation rule), which includes:

- Syntax of the rule within a specific security information and event management (SIEM) system
- Event source (any software or firmware [tools] that have logging capability and the ability to provide access to log data)
- Event category or accurate recorded event (log data)

Persons involved in the life cycle of use cases include:

- Designer/analyst (sometimes an external consultant)
- SIEM system engineer/administrator

Aleksandr Kuznetcov, CISM
Is head of the information security department at Vulkan R&D and is a postgraduate of Financial University under the Government of the Russian Federation (Moscow, Russia). He has more than 12 years of experience in information security within Russia and the Commonwealth of Independent States (CIS), including security information and event management and security operations center topics. He is the subject matter expert and manager of several hundred projects, and a regular author in his areas of expertise.

- Security tool system engineer/administrator (for every security tool)
- System administrator (for every nonsecurity tool)

> “AN EVENT CATEGORY OR ACCURATE RECORDED EVENT (LOG DATA) CAN PROVIDE COMMON AND CLEAR TERMINOLOGY FOR ALL STAFF.”

In reality, every person from the use case team uses his/her own terminology and understanding of the correlation rule (the cybersecurity incident detection scenario rule). However, there is good news: An event category or accurate recorded event (log data) can provide common and clear terminology for all staff. For example, an event category is “logon, logoff”; accurate recorded events within the Microsoft Windows 2008 R2 and 7, Windows 2012 R2 and 8.1, and Windows 2016 and 10 environments are:

- Event ID 4624, Event message “An account was successfully logged on”
- Event ID 4634, Event message “An account was logged off”

However, there is also bad news: There is no full event category catalog. Therefore, it is necessary to prepare a separate event category or accurate recorded event (log data) list (catalog) for every event source. This is a great challenge within a large IT infrastructure because, on the one hand, this catalog must be focused on cybersecurity (it is clear only for the first two persons from the team listed previously) and, on the other hand, the catalog must be focused on specific event sources (it is clear only for the last two persons from the team listed). Experience has shown that without an event category catalog, it is very difficult and sometimes impossible to carry out the design of a use case and, consequently, next steps.

Figure 1 identifies an existing challenge and provides a suggested catalog.

Figure 1—Event Categorie Catalog

Number	Event Source Type	Event Categories Related to Cybersecurity
1	Operating system	1. Creation, modification and removal of group 2. Addition and removal of group member 3. Creation, modification, removal, locking and unlocking of account 4. Change of authenticator 5. Logon and logoff 6. Creation and completion of process/task 7. Start and stop of service/driver 8. Access (creation, reading/execution, modification/writing, removal) to the object (i.e., directory, file, registry key) 9. Change of access rights related to object 10. Backup and recovery 11. Status of updates 12. Change of system time 13. Turn on, modification of, turn off audit and removal of audit trail

Figure 1—Event Category Catalog *(cont.)*		
Number	**Event Source Type**	**Event Categories Related to Cybersecurity**
2	Database management system	1. Creation, modification and removal of role 2. Creation, modification and removal of user 3. Change of authenticator 4. Logon and logoff 5. Connect and disconnect 6. Change of database object owner/database owner 7. Creation, modification and removal of database object/database 8. Access (i.e., SELECT, UPDATE, REFERENCES, INSERT, DELETE, EXECUTE) to the object (i.e., database, table) 9. Statement execution (i.e., GRANT, REVOKE, DENY, CREATE, ALTER, DROP) to the user or role 10. Start and stop of service 11. Backup and recovery 12. Turn on, modification of, turn off audit and removal of audit trail
3	Web server	1. Start and stop of service 2. Logon to virtual hosts 3. Access (i.e., GET, POST to the object [virtual host])
4	Mail server	1. Start and stop of service 2. Logon to administrative console 3. Access (i.e., receiving, sending) to the object (i.e., mailbox, email)
5	Application software	1. Creating, modification and removal of group (if applicable) 2. Addition and removal of group member (if applicable) 3. Creation, modification, removal, locking and unlocking of account (if applicable) 4. Change of authenticator (if applicable) 5. Logon and logoff (if applicable) 6. Start and stop of service 7. Access (i.e., creation, reading/execution, modification/writing, removal) to the object (if related to application software) 8. Change of access rights related to object 9. Turn on, modification of, turn off audit and removal of audit trail (if applicable)
6	Router and switch	1. Creation, modification and removal of group 2. Addition and removal of group member 3. Creation, modification, removal, locking and unlocking of account 4. Change of authenticator 5. Logon to administrative console and logoff 6. Access (i.e., creation, reading, modification, removal) to the object (i.e., ACL, route) 7. Change of access rights related to object (setting) 8. Access (i.e., PERMIT, DENY) to the network object (i.e., IP address, port, protocol) 9. Start and stop of service 10. Backup and recovery 11. Status of updates 12. Change of system time 13. Turn on, modification of, turn off audit and removal of audit trail
7	Firewall (next generation firewall [NGFW], unified threat management [UTM]) and proxy server	1. Creation, modification and removal of group 2. Addition and removal of group member 3. Creation, modification, removal, locking and unlocking of account 4. Change of authenticator 5. Logon to administrative console and logoff 6. Access (i.e., creation, reading, modification, removal) to the object (i.e., ACL, route) 7. Change of access rights related to object 8. Authentication of subject (i.e., use name) within access to network (successful or unsuccessful) 9. Access (i.e., PERMIT, DENY) to the network object (i.e., IP address, port, protocol) 10. Start and stop of service 11. Backup and recovery 12. Status of updates 13. Change of system time 14. Turn on, modification of, turn off audit and removal of audit trail

Figure 1—Event Category Catalog *(cont.)*		
Number	**Event Source Type**	**Event Categories Related to Cybersecurity**
8	Virtual private network (VPN) tool	1. Creation, modification and removal of group 2. Addition and removal of group member 3. Creation, modification, removal, locking and unlocking of account 4. Change of authenticator 5. Logon to administrative console and logoff 6. Access (i.e., creation, reading, modification, removal) to the object (i.e., VPN, router, private key) 7. Change of access rights related to object 8. Authentication of subject (VPN client) within access to VPN (successful or unsuccessful) 9. Connection between VPN tools 10. Change of private key 11. Start and stop of device 12. Change of service status 13. Backup and recovery 14. Status of updates 15. Change of system time 16. Turn on, modification of, turn off audit and removal of audit trail
9	Intrusion detection system (IDS)/ intrusion prevention system (IPS), web application firewall	1. Creation, modification and removal of group 2. Addition and removal of group member 3. Creation, modification, removal, locking and unlocking of account 4. Change of authenticator 5. Logon to administrative console and logoff 6. Access (i.e., creation, reading, modification, removal) to the object (i.e., ACL, signature) 7. Change of access rights related to object 8. Detection and blocking of malicious activity 9. Start and stop of device 10. Change of service status 11. Backup and recovery 12. Status of updates 13. Change of system time 14. Turn on, modification of, turn off audit and removal of audit trail
10	Antivirus tool	1. Creation, modification and removal of group 2. Addition and removal of group object 3. Creation, modification, removal, locking and unlocking of account (if applicable) 4. Logon to administrative console and logoff 5. Change of antivirus policy 6. Start and stop of service 7. Backup and recovery 8. Status of updates of software and signature database 9. Change of status of antivirus tool 10. Detection, quarantine, healing and removal of malicious object 11. Turn on, modification of, turn off audit and removal of audit trail
11	Vulnerability scanner	1. Creation, modification and removal of group 2. Addition and removal of group object 3. Creation, modification, removal, locking and unlocking of account (if applicable) 4. Logon to administrative console and logoff 5. Change of scanner policy 6. Start and stop of service/task 7. Status of updates software and vulnerability database 8. Detection of vulnerability 9. Turn on, modification of, turn off audit and removal of audit trail

Figure 1—Event Category Catalog *(cont.)*		
Number	**Event Source Type**	**Event Categories Related to Cybersecurity**
12	Data leak prevention system	1. Creation, modification and removal of group 2. Addition and removal of group member 3. Creation, modification, removal, locking and unlocking of account 4. Change of authenticator 5. Logon to administrative console and logoff 6. Start and stop of service 7. Access (i.e., creation, movement, coping, removal, modification) to the object (i.e., policy, rule) 8. Action (i.e., sending via network, copy to external storage, printing) on data (i.e., file, email) 9. Backup and recovery 10. Import, export, saving, applying and rollback of configuration 11. Turn on, modification of, turn off audit and removal of audit trail 12. Event interception with the verdicts "block" and "quarantine"
13	Hypervisor	1. Creation, modification and removal of group 2. Addition and removal of group member 3. Creation, modification, removal, locking and unlocking of account 4. Change of authenticator 5. Logon to administrative console, logoff 6. Start and stop process/task (i.e., migration, cloning) 7. Start and stop of service 8. Access (i.e., creation, execution, modification, removal) to the object (i.e., virtual machine, virtual switch) 9. Change of access rights related to object 10. Backup and recovery 11. Status of updates 12. Change of system time 13. Turn on, modification of, turn off audit and removal of audit trail

Conclusion

The suggested catalog uses terminology oriented for every event source type and associated staff (e.g., "role" is clear for a database administrator, "ACL" is clear for a network specialist), so cybersecurity staff does not have to translate key terms, thus saving precious time. Moreover, this list is related to cybersecurity issues and does not include extra information; therefore, cybersecurity resources can be used responsibly within the SOC use case process and remain focused on identification (detection) and response to cybersecurity incidents.

Endnotes

1 Chambers, J.; "What Does the Internet of Everything Mean for Security? Cisco Chief John Chambers Explains," *The Straits Times*, 28 January 2015, *www.straitstimes.com/opinion/what-does-the-internet-of-everything-mean-for-security-cisco-chief-john-chambers-explains*