CLAIMS

1. A computer-implemented method for dynamically identifying security threats comprising a cyber-attack chain composed of a sequence of partial cyber-attacks represented by attack patterns, the method comprising:

– receiving (102) a sequence of security events (302, 306, 308, 318);

– identifying (104), in the received sequence of security events, a first cyber-attack pattern using a correlation engine (518) by applying a set of predefined rules (400) for a detection of an indicator of compromise of a first partial cyber-attack of the cyber-attack chain, thereby identifying a specific cyber-attack chain;

– determining (106) a type and an attribute in the pattern of the first partial cyber-attack of the identified specific cyber-attack chain;

– configuring (108) at least one configured rule for a downstream partial cyber-attack in the specific cyber-attack chain based on the type and the attribute in the attack pattern of the first partial cyber-attack;

– adding (110) the at least one configured rule to the set of predefined rules (400) to be used by the correlation engine (518) for dynamically identifying security threats to information technology systems; the method characterized by

– the set of predefined rules (400) comprising of a set of identifying rules (402), a set of campaign specific rules (404), and a set of generic rules (406);

– the identifying step (104) using the set of identifying rules (402) to identify (608) a tactic-technique-procedure;

– the configuring step (108) using the identified tactic-technique-procedure to generate the at least one configured rule; and

– the adding step (110) adding (620) the at least one configured rule to the set of campaign specific rules (404).

2. The method of claim 1, further comprising:

– determining (610, 622), in the received sequence of security events, a second cyber-attack pattern using the correlation engine (518) by applying the configured at least one rule for a detection of a second indicator of compromise in the second cyber-attack of the cyber-attack chain.

3. The method of claim 1 or 2, wherein the set of campaign specific rules (404) is using information about malware attribute enumeration and characterization and structured threat information expressions.

4. The method of claim 3, further comprising:

– updating the set of campaign specific rules (404) continuously by adding new indicators of compromise.

5. The method of any of the preceding claims, wherein the adding the at least one configured rule to the set of campaign specific rules (404) is performed by:

– selectively configuring and/or activating correlation rules;

– grouping of rules; and/or

– prioritizing the configured and added at least one rule against generic rules.

6. The method of any of the preceding claims, wherein the configuring the at least one rule for a downstream partial cyber-attack comprises:

– using data about tactic-technique-procedure identifying rules, malware attribute enumeration and characterization and structured threat information expressions from a repository.

7. The method of any of the preceding claims, the configuring the at least one rule for a downstream partial cyber-attack further comprising:

– configuring additional rules relating to typical downstream partial cyber-attacks of a cyber-attack chain relating to the determined type and attribute in the pattern of the first partial cyber-attack of the identified specific cyber-attack chain.

8. The method of any of the preceding claims, further comprising:

– triggering an alarm signal after a predefined number of subsequent partial security attacks corresponding to one cyber-attack chain has been determined.

9. The method of any of the preceding claims, further comprising:

– removing the at least one configured rule for a downstream partial cyber-attack in the specific cyber-attack chain in the set of campaign specific rules (404) if it is determined that a

risk value for the specific cyber-attack chain is reduced to below a predetermined risk threshold value.

10. The method of claim 9, further comprising:

– removing the at least one configured rule for a downstream partial cyber-attack in the specific cyber-attack chain if the correlation engine (518) using the at least one configured rule did not determine a downstream cyber-attack pattern for a predefined time.

11. The method of claim 9, further comprising:

– removing a rule relating to at least one configured rule for a downstream partial cyber-attack in the specific cyber-attack chain in the set of campaign specific rules (404) from the repository (516) of malware attribute enumeration and characterization and structure threat information expressions.

12. A security information and event monitoring system (700) for dynamically identifying security threats comprising: a cyber-attack chain composed of a sequence of partial cyber-attacks represented by attack patterns, the system comprising:

– a receiving unit (702) adapted for: receiving a sequence of security events (302, 306, 308, 318);

– a determination unit (704) adapted for determining, in the received sequence of security events, a first cyber-attack pattern using a correlation engine (518) by applying a set of predefined rules (400) for a detection of an indicator of compromise of a first partial cyber-attack of the cyber-attack chain, thereby identifying a specific cyber-attack chain;

– wherein the determination unit (704) is also adapted for determining a type and an attribute in the pattern of the first partial cyber-attack of the identified specific cyber-attack chain;

– a configuration unit (706) adapted for configuring at least one configured rule for a downstream partial cyber-attack in the specific cyber-attack chain based on the type and the attribute in the attack pattern of the first partial cyber-attack;

– an adding module (708) adapted for adding the at least one configured rule to the set of predefined rules (400) to be used by the correlation engine (518) for dynamically identifying security threats to information technology systems; the system characterized by

– the set of predefined rules (400) comprising of a set of identifying rules (402), a set of campaign specific rules (404), and a set of generic rules (406);

– the determination unit (704) adapted for using the set of identifying rules (402) to identify (608) a tactic-technique-procedure;

– the configuration unit (706) adapted for using the identified tactic-technique-procedure to generate the at least one configured rule; and

– the adding module (708) adapted for adding the at least one configured rule to the set of campaign specific rules (404).

13. The system of claim 12, wherein the determination unit (704) is also adapted for:

– determining (610, 622), in the received sequence of security events, a second cyber-attack pattern using the correlation engine (518) by applying the configured at least one rule for a detection of a second indicator of compromise in the second cyber-attack of the cyber-attack.

14. The system of claim 12 or 13, wherein the set of campaign specific rules (404) is adapted for:

– using information about malware attribute enumeration and characterization and structured threat information expressions.

15. The system of claim 14, further comprising:

– an updating unit adapted for: updating the set of campaign specific rules (404) continuously by adding new indicators of compromise.

16. The system of any of the claims 12 to 15, wherein the adding module (708) is also adapted for:

– selectively configuring and/or activating correlations rules;

– grouping of rules; and/or

– prioritizing the configured and added at least one rule against generic rules.

17. The system of any of the preceding claims 12 to 16, further comprising:

– a repository (516) for storing data about tactic-technique-procedure identifying rules, malware attribute enumeration and characterization and structured threat information expressions to be used by the configuration unit (706).

18. The system of any of the preceding claims 12 to 17, wherein the configuration unit (706) when configuring the at least one configured rule for a downstream partial cyber-attack is also adapted for:

– configuring additional rules relating to typical downstream cyber-attacks of a cyber-attack chain relating to the determined type and attribute in the pattern of the first partial cyber-attack of the identified specific cyber-attack chain.

19. The system of any of the preceding claims 12 to 18, further comprising:

– an alarm unit (522) adapted for triggering an alarm signal after a predefined number of subsequent partial security attacks corresponding to one cyber-attack chain has been determined.

20. The system of any of the preceding claims 12 to 19, further comprising:

– a removal module adapted for removing the at least one configured rule for a downstream partial cyber-attack in the specific cyber-attack chain in the set of campaign specific rules (404) if it is determined that a risk value for the specific cyber-attack chain is reduced to below a predetermined risk threshold value.

21. The system of claim 20, wherein the removal module is also adapted for:

– removing the at least one configured rule for a downstream partial cyber-attack in the specific cyber-attack chain if the correlation engine (518) using the at least one configured rule did not determine a downstream cyber-attack pattern for a predefined time.

22. A computer program comprising instructions which, when the program is executed by a computer (800), cause the computer (800) to carry out the steps of one of the methods of claims 1 to 11.