Cyber Threat Information Classification and Life Cycle Management using Smart Contracts

Roman Graf and Ross King
AIT Austrian Institute of Technology, Vienna, Austria

Keywords: Cyber Security, Situational Awareness, Access and Usage Control, Content Protection, Smart Contracts, Software Security Assurance.

Abstract: Nowadays, cyber critical infrastructures (CIs) are increasingly targeted by highly sophisticated cyber attacks and should be protected. Advances in cyber situational awareness technology lead to the creation of increasingly complex tools. Human analysts face challenges finding relevant information in large, complex data sets, when exploring data to discover patterns and insights. To be effective in identifying and defeating future cyber-attacks, cyber analysts require novel tools for incident report classification and life cycle management that can automatically analyse and share result in secure way between CI stakeholders to achieve better situation comprehension. Our goal is to provide solutions in realtime that could replace human input for cyber incident classification and management tasks to eliminate irrelevant information and to focus on important information to promptly adopt suitable countermeasures in case of an attack. Another contribution relates to the provided support for document life cycle management that should reduce the number of manual operations and save storage space. In this paper we evaluate the application of so-called "smart contracts" to an incident classification system and assess its accuracy and performance. We demonstrate how the presented techniques can be applied to support incident handling tasks performed by security operation centers (SOCs).

1 INTRODUCTION

The widespread use of cyber security (CS) information technologies is considerably increasing the number of electronic documents. Automated methods for organizing and improving the access to the information contained in these documents become essential to cyber security information management. This paper describes a methodology developed to improve information organization and access in cyber security information systems based on automatic classification of cyber security documents according to their expected threat level.

Cyber Situational Awareness (SA) (Barford et al., 2010) provides and overview of a security and threat situation as well as a current and future impact assessment. Speed of events, data overload, and meaning underload (Kott and Wang, 2014) make real-time situational awareness of cyber operations very difficult to evaluate. Report data are often imprecise, which makes it difficult to find relevant information in large, complex data sets. Novel techniques that can automatically make obvious or predefined decisions by means of smart contracts can help by identifying and defeating of cyberattacks. Smart contract is a piece of software that fixes and verifyies negotiated behavior and can not be manipulated, because it is distributed among multiple nodes on a blockchain. Another value of using "smart contracts" is that once uploaded on blockchain it is working automatically, without the need for interaction with human. We hypothesize that the application of "smart contracts" based on existing blockchain technology (Ethereum (Wood, 2014)) can solve some SA problems. The main purpose of designing smart contracts for SA is to enable rapid and trusted cyber incident classification and management, without the need for a large centralized authority. We propose that smart contracts based on decentralised assets such as Ethereum can reduce effort for securing report transfer, manual analysis costs, and increase speed of severe information sharing. With raising number of advanced CS tools for situational awareness, SOC analysts receive a huge amount of threat reports daily. These experts face challenges finding relevant information in large, complex data sets and following organisation business processes, such as proper acquisition, use, archival and disposal of threat reports. The management system based on smart contracts and blockchain technology is aiming at automatic management of threat reports provided by threat analysis tools, such as

Graf, R. and King, R.
Cyber Threat Information Classification and Life Cycle Management using Smart Contracts.
DOI: 10.5220/0006605203040311
In *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018)*, pages 304-311
ISBN: 978-989-758-282-0

CAESAIR[1], IntelMQ[2] or MISP[3] and should provide effective decision support for SOC operator. Compared to manual classification, automatic classification by threat level can significantly facilitate and accelerate reaction time of a SOC analyst. For example CAESAIR tool (Settanni et al., 2016) supports various security information correlation techniques and provides customizable import capabilities from a multitude of security-relevant sources. These sources include a custom repository, open source intelligence (OSINT) feeds, and IT-security bulletins, as well as a standardized vulnerability library (Common Vulnerabilities and Exposures - CVE). CVEs are especially important for smart contracts with regard to likelihood assessment based on game theory ((Samarji and et al, 2015), (Kanoun and et al, 2009)), which is implementing risk scoring (Reguly, 2013). Employing CAESAIR with CVE scoring (Maghrabi et al., 2016) and extending it by automated tagging can provide valuable inputs for information classification and management life cycle. Such system can be implemented using smart contracts composed for particular organization. The research presented here should support cyber analyst by fast and effective establishing of a cyber situational awareness. Each institution may have multiple classification profile definitions dependent on network, CI, and the role of the cyber analyst.

The research presented evaluates a system based on blockchain and smart contract technology that will automatically classify and manage cyber incidents that could impact cyber situational awareness reported and analysed by one of the trusted stakeholders. Within our prototype system, smart contracts trigger incident classification for large amounts of data by means of knowledge base employing one of the incident analysis tools. Smart contracts also manage incident life cycle if rules coded in related smart contract are met.

This paper is structured as follows: Section 2 gives an overview of related work and concepts. Section 3 explains the cyber incident classification workflow and also covers report life cycle issues. Section 4 presents the experimental setup and applied methods. Evaluation results are presented in subsection 4.2. Section 5 concludes the paper.

2 RELATED WORK

Multiple researchers are developing an automated technology that will support an information classification system. An attempt to classify the relationships between documents and concepts (Weng et al., 2006) employs principles of ontology. To improve information organization and access in construction management was developed a methodology (Caldas and Soibelman, 2003) based on automatic hierarchical classification of construction project documents according to project components. A survey on various cyber attacks and their classification (M. and Padmavath, 2013) attempts to develop an ontology for cyber security incidents. They classify by characteristics, such as “organized”, “enormous”, “scrupulously designed”, “demanding time and resource”, and by purpose and motivations, such as “obstruction of information”, “retardation of decision making process”, “denial in providing public services”, “reputation of the country will be denigrated”, “smashing up legal interest”. Additionally cyber attacks can be classified based on severity of involvement, scope or network types with multiple sub classification terms. Contrary to this approach, we classify only by threat level that can differ from organisation to organsation. Our goal is to focus human expert resources on the most urgent incidents important for particular organisation.

An information life-cycle model described in (Harris and Maymi, 2016) is applicable also to the cyber security domain. Cyber incident reports are aquired, analysed and become outdated. Effective automatic classification, retention and disposal policies can mitigate risks to data and make information management more effective. Classification of data enables a company or security operational center to focus their resources towards most valuable or urgent incidents and to handle less valuable incidents automatically saving time and costs.

An overview of the blockchain technologies and its potential to facilitate money transactions, smart contracts design, automated banking ledgers and digital assets is provided in (Peters and Panayi, 2016). We suggest that the core technology of this approach can be reused in the cyber security domain by means of suitable smart contracts.

A distributed peer-to-peer network based on blockchain technology where non-trusting members can interact with each other without a trusted intermediary, in a verifiable manner was examined in (Christidis and Devetsikiotis, 2016) for the Internet of Things (IoT) sector. This mechanism should work also for the automation of multi-step processes for cyber incident classification and management.

The performance of Blockchain, which is a probabilistic proof-of-work (PoW) based consensus fabric (Vukolić, 2016) has became an important issue for the modern cryptocurrency platforms. PoW-based

[1] http://caesair.ait.ac.at

[2] https://github.com/certtools/intelmq

[3] https://github.com/MISP/MISP

Blockchains can be replaced by BFT state machine replication, to improve Blockchain scalability limits.

A Blockchain platform comparison (Macdonald et al., 2017) discusses five general-use Blockchain platforms and looks at how Blockchain technology can be used in applications outside of Bitcoin (Nakamoto, 2009) to build custom applications on top of it. This comparison suggests that Ethereum is currently the most suitable platform and well established platform. Therefore, for cyber incident analysis we employ Ethereum Blockchain in its Pyethereum fashion, which supports focused smart contracts testing environment without the need of mining.

A basis for smart contracts development in cyber security realm is a solid threat intelligence that is provided by a number of cyber incident analysis tools. The CAESAIR tool (Settanni et al., 2016) introduces the concept of a cyber intelligence analysis system, called Collaborative Analysis Engine for Situational Awareness and Incident Response. CAESAIR provides analytical support for security experts carrying out cyber incident handling tasks on a national and international level, and facilitates the identification of implicit relations between available pieces of information. It provides powerful correlation capabilities, which support the tasks carried out by the analysts of a Security Operation Center (SOC) during the incident handling process. CAESAIR evaluates how the collected documents are connected to one another, and allows the analyst to select the most appropriate correlation method and to flexibly adjust relevance metrics.

The research on risk management in SA increasingly gains in importance. The SA framework (Morita et al., 2011) describes how a person perceives elements of the environment, comprehends and projects its actions into the future. This framework employs the situation awareness model that can be used in the assessment of risk awareness focusing on the adverse event notification system. Our expert system takes a similar approach, but focuses on classification of essential information, rather than events. The review of existing situation awareness measurement techniques for their suitability for use in the assessment of SA in different environments (Salmon et al., 2006) demonstrates that current SA measurement techniques are inadequate by themselves for use in the assessment of SA, and a multiple-measure approach utilising different approaches is recommended. To address this gap, we employ specific metrics employing outputs from the threat analysis tools. In security planning, it is necessary to analyse data that are often vague and imprecise. In (Barford et al., 2010) authors survey existing technologies in handling uncertainty and risk management in cyber situational awareness, but the focus is on looking for vulnerabilities in a system, whereby our approach is focused on secure classification of the raw data at a lower level that creates a basis for further SA aspects, such as situation recognition, situation comprehension and situation projection (Barford et al., 2010).

In the proposed system we intend to apply smart contracts for cyber incident classification and life cycle management, which is unique for the given domain.

3 CYBER INCIDENT CLASSIFICATION AND MANAGEMENT USING SMART CONTRACTS

We evaluate the application of smart contracts to classify and manage incident reports sended between CIs experts in order to improve SA. For instance, smart contracts can be used to estimate that reported cyber incident is of high relevance, to remove it after some predefined time, to tag it by acquisition, to search by tag, to assign access rights (confidential, private, sensitive, public), to periodic check data integrity (preventing manual or hardware corruption) or to determine data provenance. Using GUI this approach can also provide visualisation support - show storage content of smart contract. One smart contract can call other smart contract to read from his storage. Our goal is to save storage place, improve performance and to keep information up-to-date in a trusted way leveraging distributed nodes nature of the blockchain technology. Another goal is to minimize calculations number and to make secure smart contracts.

Once a smart contract is triggered, the analysis result is automatically propagated among all participants through inherent blockchain mechanisms. One of the advantages of this approach is that smart contracts cannot be changed or compromised without being detected (through hashed transactions) and that the messages can be verified to originate from a trusted source (through public key encryption).

The state of smart contracts is stored on the blockchain and is transparent and accessible to all registered community members (see Figure 1). The smart contract code is executed in parallel by a network of miners under consensus regarding outcome of the execution. The execution of the smart contract results in an update of the contract's state on the blockchain that is synchronized with every participating node through standard peer-to-peer mechanisms.

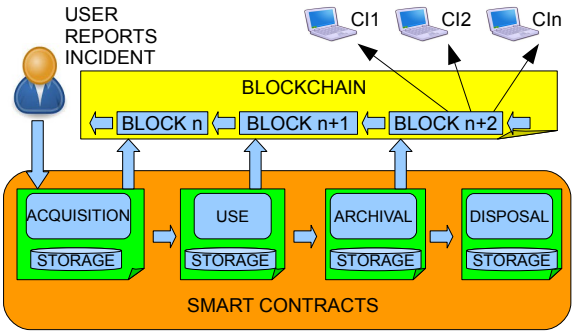

Figure 1: The overview of establishing the Cyber Situational Awareness using Smart Contracts for information classification and life-cycle management.

By incident acquisition an acquisition smart contract performes classification of a report by threat level, stores obtained threat level on a blockchain and initiates life-cycle management process for given incident. In the next steps this report will be used, archived and disposed.

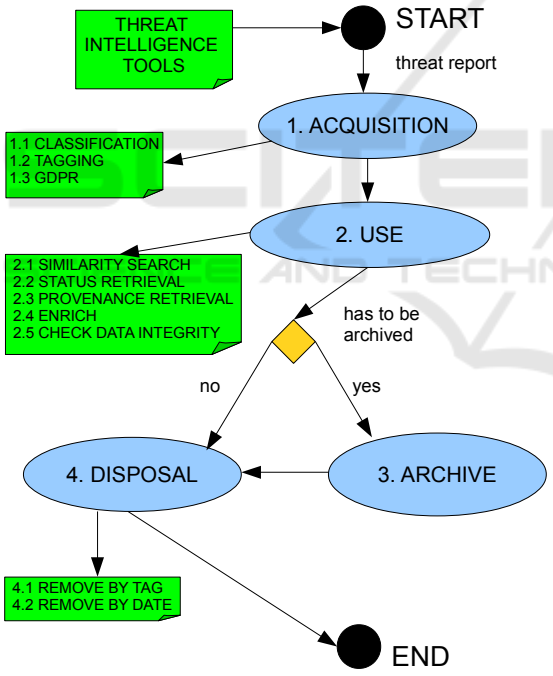

Figure 2: The workflow for classification and life-cycle management of cyber incident using smart contracts.

For cyber incident processing we employ four smart contracts as depicted in Figure 2. The workflow execution begins with the reading of an incident report and parsing of the report content. Input data, along with expert profile settings that are specific for an organisation, are passed to the first smart contract "acquisition". For the acquisition computation we employ one of the threat intelligence tools. By means of threat intelligence tool we obtain cyber incident content. In the next step we merge the incident with institutional settings and using smart contract logic to automatically decide which threat level to assign a given incident to classify it. Classification occures employing incident text, splitted by words or phrases, specific terms separated by low, middle and high threat relevance. The significant terms data provided by domain experts is stored in a text files. In the next step we compute risk points counting how many of threat level terms are included in incident report for each threat level. Finally, we calculate threat level using one of two methods. Either we estimate threat level applying threasholds for each level or we employ weighted method using Formula 1 where we additionally multiply calculated points on each threat level with a constant standing for weight of related threat level.

Domain experts rated the threat level on a scale of 1-3, where 1 is "low threat" and 3 is "high threat." Risk points RP are calculated using Formula 1 and is a sum of high risk points H_{rp} multiplied by high threat weight HT_w, middle risk points M_{rp} multiplied by middle threat weight MT_w and low risk points L_{rp} multiplied by low threat weight LT_w.

$$RP = H_{rp} * HT_w + M_{rp} * MT_w + L_{rp} * LT_w \quad (1)$$

where $HT_w = 3$, $MT_w = 2$ and $LT_w = 1$.

Threat level T_l can be inferred using high threat HT_t and middle threat HT_t thresholds and weighted risk points RP from Formula 1 applying Formula 2

$$T_l = \begin{cases} 3(high) & \text{if } RP > HT_t, \\ 2(middle) & \text{if } RP > MT_t, \\ 1(low) & \text{else } RP \leq MT_t. \end{cases} \quad (2)$$

where $HT_t = 10$ and $MT_t = 3$.

Acquisition step is splitted in different tasks: SC1.1: Automatic classification by threat level defines one of three threat levels. "high" (3) level requires fast reaction and mediation steps, triage process. "medium" (2) level assumes detection of "Indicator of Corruption" (IoC) or metrics that indicate possible vulnerabilities, requires SW update. "low" (1) level addresses regular cyber security information, logs, requires attention but should not necessary be a threat. SC1.2: Tagging means that spcific tags can be assigned to a report to easy find, shift or remove it later. SC1.3: Remove personal information (GDPR). To protect personal data it may be required to remove personal information from incident report and store normalized version of incident.

In the second step the workflow supports incident using. Using employs tasks, such as: SC2.1: Automated similarity search. SC2.2: Status and provenance retrieval. SC2.3: Enrichment with data and metadata. SC2.4: Periodic check for data integrity (using hash of incident report - that saves storage space on blockchain, because instead of storing and validating of the file content we validate only file hashes, which are short strings).

Finally, depending on threat level after some period of time, incident can be archived (step 3) or removed e.g. by date or by tag (step 4).

We believe that this automatic smart-contracts-based approach would significantly facilitate incident classification and management and could be used by analysts for the defence of critical infrastructure. The suggested method would make SA analysis less costintensive and would perform with higher throughput. However, as is typical in this area, a human-based approach performs with higher accuracy.

4 EVALUATION

In this section we report on measurements of the automated cyber incident classification, how long it takes for smart contracts to be executed and validated. We carried out measurements for varying incident report categories and different volumes of data in the knowledge base. The goal of this evaluation was to leverage the domain expert knowledge base for cyber incident classification and management as described in the workflow (see Fig. 2), pointing out threat level relevant for Situation Awareness.

4.1 Evaluation Data Set

One responsibility of the cyber analyst is to prioritise a received cyber incident and to mitigate it or to carry out a selected cyber incident response. For this evaluation, we differentiate between high, middle and low priority. High priority means that the incident has high severity and mitigation steps should be carried out. These types of incidents are tagged with a number 3. Low priority incidents are tagged with a number 1.

This evaluation took place on an Intel Core i7-3520M 2.66GHz computer using Python on Ubuntu OS. We evaluate 5850 cyber incident reports from the "seclists" feed [4] from the last three years addressing four report categories: "fulldisclosure", "bugtraq", "pen-test" and "nmap-dev". The "fulldisclosure" category contains messages from public, vendor-neutral forum for detailed discussion of vulnerabilities and exploitation techniques, as well as tools, papers, news, and events of interest to the community. The "bugtraq" category is a general security mailing list. The "pen-test" category discloses techniques and strategies that would be useful to anyone with a practical interest in security and network auditing. The "nmap-dev" category comprises an unmoderated technical development forum for debating ideas, patches, and suggestions regarding proposed changes to Nmap [5] and related projects.

The specific cyber security terms were obtained from the cyber security glossary [6].

We assume that employing of described smart contracts approach should classify cyber incidents among a very large number of incident reports facilitating further cyber analysis and incident management in the future. We also expect that smart contracts written in Serpent language [7], supported by Python 2.7 workflow and subsequent analysis will demonstrate both good performance and sufficient accuracy.

4.2 Experimental Results and Interpretation

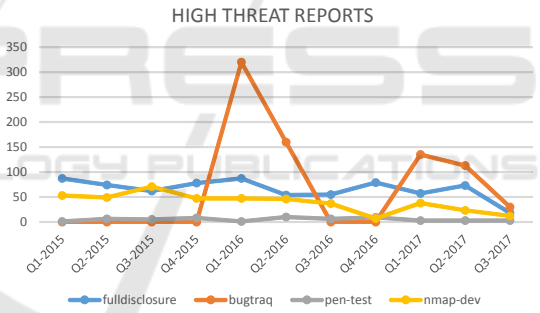

Figure 3: Plot for distribution of high threat incident reports over last three years shared quarterly.

In the test scenario we investigate incident reports from "seclists" feed to classify them by threat level and to automatically manage them from acquisition to disposal without involvement of human analyst (see Table 1). Due to huge number of results in this table we describe only selected classification results, which demonstrate typical cases. The first column contains categories of the incidents. "FD" is "fulldisclosure", "BT" is "bugtraq", "ND" is "nmap-dev" and "PT" means "pen-test". Next three columns show incident timestamp splittet in year, month and quarter. Graphical results for the whole dataset in Figures 3, 4 and 5

[4] http://seclists.org/

[5] https://nmap.org/

[6] https://scottschober.com/glossary-of-cybersecurity-terms/

[7] https://github.com/ethereum/wiki/wiki/Serpent

Table 1: Excerpt of classification results for cyber incident reports by their acquisition using smart contracts.

Cat	Year	M	Q	Source	ID	Time	L	LT Terms	M	MT Terms	H	HT Terms	SUM	TL	WTL	SC ID
FD	2017	Jan	q1	Wolfgang feedyourhead at	75	0.371	1	subject	1	bug	3	attacker firewall password	5	3	3	68
FD	2015	Feb	q1	Scott Arciszewski	53	0.370	1	key	2	bug spam	0		3	2	2	1304
FD	2015	Feb	q1	Praveen D	90	0.451	1	response	0		0		1	1	1	1314
BT	2017	Jan	q1	Vulnerability Lab	18	0.677	2	capability investigation	4	access authen-tication author-ization encode	7	alert attack attacker hack phishing risk vulne-rability	13	3	3	3419
BT	2017	Jun	q2	SEC Consult Vulnerability Lab	56	0.532	3	investigation penetration work	5	cipher crypt-analysis decrypt decryption encryption	5	attack attacker risk signature vulne-rability	13	3	3	3829
BT	2016	Jan	q1	Slackware Security Team	75	0.332	1	key	1	authen-tication	0		2	1	1	4009
BT	2016	Apr	q2	Salvatore Bonaccorso	158	0.432	0		1	bug	0		1	1	1	4215
ND	2017	Mar	q1	Henri Doreau	226	0.533	2	event work	1	bug	0		3	2	2	4831
ND	2015	Nov	q4	Peter Houppermans	107	0.600	2	interoperability penetration	3	authen-tication decryption interope-rability	3	attack password signature	8	3	3	6849
ND	2015	Oct	q4	Mark Scrano	63	0.496	1	bitcoin	0		0		1	1	1	6853
PT	2017	Jul	q3	Hafez Kamal	1	0.252	2	NFC penetration	1	access	0		3	2	2	7994
PT	2016	Feb	q1	Francisco Amato	2	0.357	1	penetration	1	bug	0		2	1	1	8071
PT	2016	Dec	q4	ERPScan inc	0	0.521	2	penetration work	1	cyber security	6	attack attacker exploit impact threat vulne-rability	9	3	3	8072

also splitted in quaters on X axis. Column “Source” depicts an incident source that can be a person or an organisation. Incident ID in “seclists” terms is presented in column “ID”. The columns “L”, “M” and “H” to the right of the “ID” column present how many risk points were detected for given incident respectivly. And columns “LT Terms”, “MT Terms” and “HT Terms” show detected significant threat terms for low, middle and high threat level. The total number of risk points for each incident can be found in the column “SUM”. Resulting threat level and weighted threat level are shown in columns “TL” and “WTL” respectively. Finally, column “SC ID” contains smart contract id of incident on the blockchain.

As a use case scenario assume that Security Operational Team has received an incident report from Vulnerability Lab in January 2017. On receiving of this report our smart contract triggers automati-

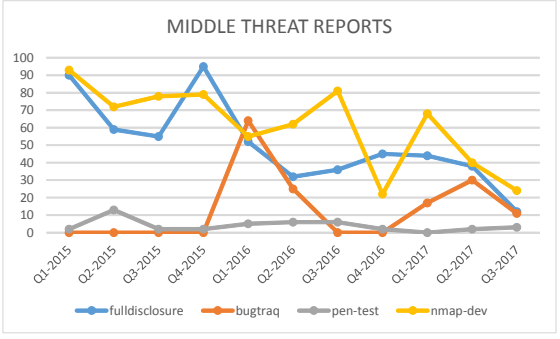

Figure 4: Plot for distribution of middle threat incident reports over last three years shared quarterly.

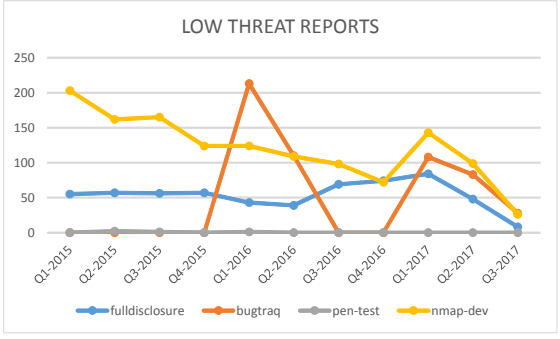

Figure 5: Plot for distribution of low threat incident reports over last three years shared quarterly.

cal analysis and classification of this incident report. According to Table 1 we see that this incident obtains smart contract identifier SCID 3419 and contract identifies 2 “LT Terms” (capability, investigation), 4 “MT Terms” (access, authentication, authorization, encode) and 7 “HT Terms” (alert, attack, attacker, hack, phishing, risk, vulnerability). Going through the contract logic we estimate both the regular threat level and the weighted threat level as a “high threat” (3). Therefore, our smart contract has automatically analyzed and classified this incident report as a “high threat”. That means it should be handled in the first place with high priority. Incident is automatically tagged and enriched with additional data from cyber security feeds and tools like “whois” [8] and “nmap” [9]. Links to similar incidents are established. All this facilitates Triage process for a cyber analyst and performs analysis steps that usually are done manually. Due to employment of blockchain technology aggregated information can not be lost or biased. An expert is able to retrieve incident status or provenance information from blockchain at any time. According to evaluated classification level, smart contract defines timestamps for automated archival and disposal of incident data. Therefore, a cyber analyst does not need to care about incident life cicle and can focus her resources on Triage for urgent cases.

The smallest duration for one smart contract operation 0.252 seconds shows report with SCID 7994 and the longest operation time 0.677 report with SCID 3419. This difference can be explained by different report size (we calculate hash for report content) and different risk points numbers (3 for SCID 7994 vs. 13 for SCID 3419). We can see that reports are coming from persons, such as “Scott Arciszewski” or “Henri Doreau” but also from companies, such as “SEC Consult Vulnerability Lab” or “Slakware Security Team”. This table also gives easy overview over detected significant terms, such as “attack”, “hack”, “phishing” for high threat incidents, “access”, “authentication”, “encode” for middle threat incidents and “key”, “capability”, “investigation” for low level threats. Also cyber analyst can immediately see automatic calculated threat level of incident for different calculation methods. Having smart contract ID analyst is able to retrieve status data of particular incident report from blochchain using smart contract (e.g. hash, provenance, time, tags, owner).

The experimental results regarding category overview are presented in Table 2 that shows distribution of high, middle and low threat level incidents for different incident categories. This table demonstrates that most incident reports (2429) are coming from “nmap-dev” category following by “fulldisclosure” (1872) and “bugtraq” (1447) categories. Most of incident reports belong to the low thrat level (2461) but report number classified as high threat is also high (1967). Most high threat level reports are coming from “fulldisclosure” (724) and “bugtraq” (758) categories. That means that these categories should be addressed first by incident management.

The experimental results are visualized in Figures 3, 4 and 5 and show distribution of threat incident reports over last three years respective for high, middle and low threat levels. Each incident category is flagged by specific color. X axis is range of the number of incidents and Y axis is a time scale splitted in quarters. These figures demonstrate that most productive category for high (up to 325) and low (up to 215) threats is a “bugtraq” category, whereas “nmap-dev” (93) and “fulldisclosure” (97) are dominating for middle thrat reports. For given period of time most active phase for all levels is from “Q4-2015” to “Q3-2016”. Visualization of incident reports provides an analyst with fast and descriptive situational awareness picture. To focus on particular part analyst can perform fine tuning and adjust time scale or select particular category or source.

Table 2: Overview about aggregated threat reports for different threat categories.

Threat category	High Threat	Middle Threat	Low Threat	Total
fulldisclosure	724	558	590	1872
bugtraq	758	147	542	1447
pen-test	55	43	4	102
nmap-dev	430	674	1325	2429
Sum	1967	1422	2461	5850

These results demonstrate that a semi-automatic approach for incident classification and visualisation is very effective and it is a signicant improvement compared with manual analysis for monitoring and validation of design for critical infrastructure. Resulting actions of the presented analysis tool may be mitigation steps, validation, checking or updating of the software.

5 CONCLUSIONS

In this work we have presented an automated approach to classify and manage incident reports for establishing cyber situational awareness using smart contracts. We have combined expertise gathered during the development of a cyber intelligence tool with the power of the smart contracts approach. The main contribution of this work is a real-time solution that could replace human input for a large number of cyber

[8] https://www.whois.com/whois/

[9] https://nmap.org/

incident analysis tasks in order to eliminate irrelevant information and to focus on important information to promptly perform mitigation steps. Another contribution is the employment of smart contract techniques to provide an automated trusted system for incident management life-cycle that allows automatic acquisition, classification, use, archiving and disposal. The presented method employs a domain expert knowledge base collected through a cyber intelligence tools to detect Situational Awareness risks. An additional advantage of this approach is a reduction of human analysis costs. Ultimately, our research will lead to the creation of automated security assessment tools with more effective handling of cyber incidents.

REFERENCES

Barford, P., Dacier, M., Dietterich, T., Fredrikson, M., Giffin, J., Jajodia, S., Jha, S., Li, J., Liu, P., Ning, P., Ou, X., Song, D., Strater, L., Swarup, V., Tadda, G., Wang, C., and Yen, J. (2010). Cyber sa: Situational awareness for cyber defense. In Jajodia, S., Liu, P., Swarup, V., and Wang, C., editors, *Cyber Situational Awareness*, volume 46 of *Advances in Information Security*, pages 3–13. Springer US.

Caldas, C. H. and Soibelman, L. (2003). Automating hierarchical document classification for construction management information systems. *Automation in Construction*, 12(4):395 – 406.

Christidis, K. and Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access*, 4:2292–2303.

Harris, S. and Maymi, F. (2016). Cissp all-in-one exam guide. *CISSP book, seventh edition, chapter 2*, pages 189 – 245.

Kanoun, W. and et al (2009). Success likelihood of ongoing attacks for intrusion detection and response systems. volume 3, pages 83–91. IEEE.

Kott, A. and Wang, C. (2014). *Cyber Defense and Situational Awareness*. Springer International Publishing Switzerland.

M., U. and Padmavath, G. (2013). A survey on various cyber attacks and their classification. *nternational Journal of Network Security*, 15(5):390–396.

Macdonald, M., Liu-Thorrold, L., and Julien, R. (2017). The blockchain: A comparison of platforms and their uses beyond bitcoin. The University of Queensland.

Maghrabi, L., Pfluegel, E., and Noorji, S. F. (2016). Designing utility functions for game-theoretic cloud security assessment: a case for using the common vulnerability scoring system. In *2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security)*, pages 1–6.

Morita, P., Burns C.M., H., and He, Q. (2011). Situation awareness and risk management understanding the notification issues. In *Stud Health Technol Inform*. PubMed.

Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system.

Peters, G. W. and Panayi, E. (2016). *Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money*, pages 239–278. Springer International Publishing, Cham.

Reguly, T. (2013). Does anybody really care about vulnerability scoring? [online], Available: https://www.tripwire.com/stateof-security/risk-based-security-for-executives/risk-management/doesanybody- really-care-about-vulnerability-scoring/.

Salmon, P., Stanton, N., Walker, G., and Green, D. (2006). Situation awareness measurement: A review of applicability for {C4i} environments. *Applied Ergonomics*, 37(2):225 – 238.

Samarji, L. and et al (2015). Coordination and concurrency aware likelihood assessment of simultaneous attacks. volume 153, pages 524–529.

Settanni, G., Shovgenya, Y., Skopik, F., Graf, R., Wurzenberger, M., and Fiedler, R. (2016). Correlating cyber incident information to establish situational awareness in critical infrastructures. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, pages 78–81, Auchland, New Zealand. IEEE.

Vukolić, M. (2016). *The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication*, pages 112–125. Springer International Publishing, Cham.

Weng, S.-S., Tsai, H.-J., Liu, S.-C., and Hsu, C.-H. (2006). Ontology construction for information classification. *Expert Systems with Applications*, 31(1):1 – 12.

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger.