Hochschule
München
University of
Applied Sciences

Department for Computer Science and Mathematics

Insights into Cyber Defense: How Security Teams leverage Cyber Threat IntelligenceÜberschrift

2023-06-08

Cyber Defense

- Effective cyber defense involves a multi-layered approach to protect digital assets.
- Layers include:
  - **Perimeter Defense**: Firewalls, intrusion prevention systems (IPS), and network monitoring.
  - **Endpoint Security**: Antivirus software, endpoint detection and response (EDR), and mobile device management (MDM).
  - **Identity and Access Management (IAM)**: Authentication, authorization, and user access controls.
  - **Data Protection**: Encryption, data loss prevention (DLP), and backup systems.
  - **Security Monitoring and Incident Response**: Security operations centers (SOCs) and incident response teams.

Service Framework

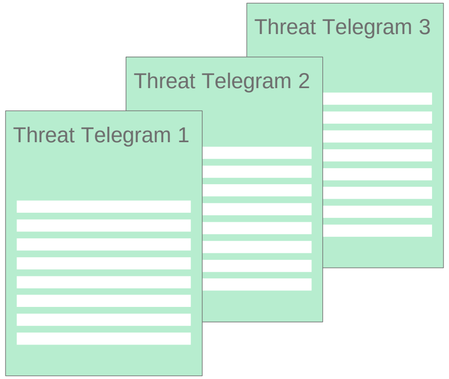
https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

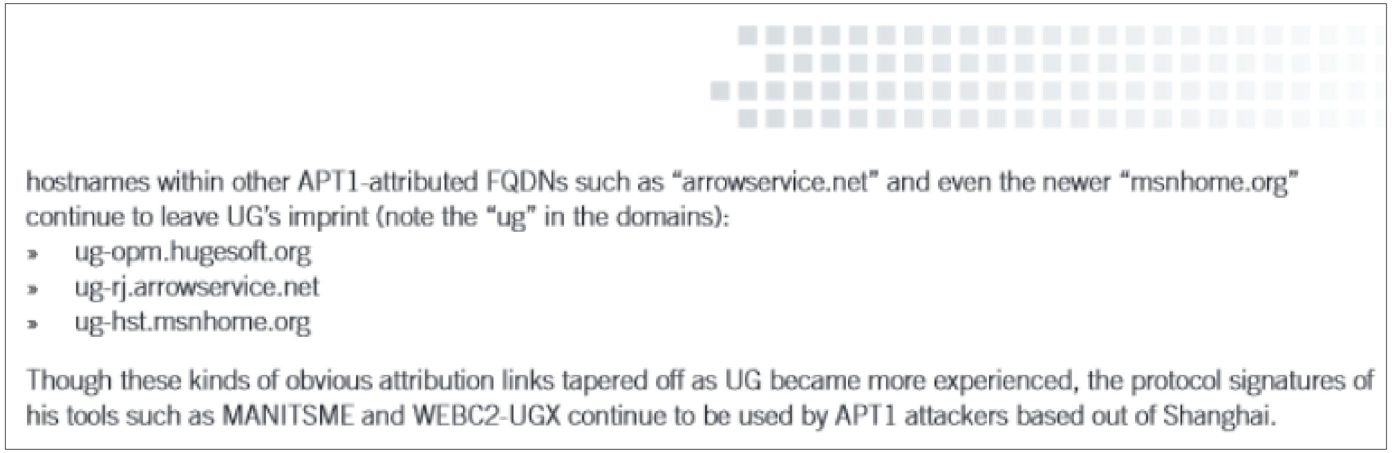
- Incident Management
- Knowledge and Information Management
- Collaboration and Coordination
- Training and Education
- Tools and Technologies
- Continuous Improvement
- Legal and Ethical Considerations

2596.59

… and here is the reality!

PDF Reports





hostnames within other APT1-attributed FQDNs such as “arrowservice.net” and even the newer “msnhome.org” continue to leave UG's imprint (note the “ug” in the domains):

- ug-opm.hugesoft.org
- ug-rj.arrowservice.net
- ug-hst.msnhome.org

Though these kinds of obvious attribution links tapered off as UG became more experienced, the protocol signatures of his tools such as MANITSME and WEBC2-UGX continue to be used by APT1 attackers based out of Shanghai.

Empty File Hash

4741a7df46e61985544c647a401e94f7

Being prepared to respond to threats and incidents in a timely manner is key to limit their impact

- Regardless whether dealing with **threats** or **incidents**, having processes and procedures in place to deal with both, is mandatory for timely emergency response.

Time is of the essence.

Capabilities of an CTI program

Intelligence Acquisition

- External sources
  - Public intel
  - Subscriptions
  - Trusted groups
- Internal sources
  - Sandboxes
  - Investigations
  - Sensors

Intelligence Management

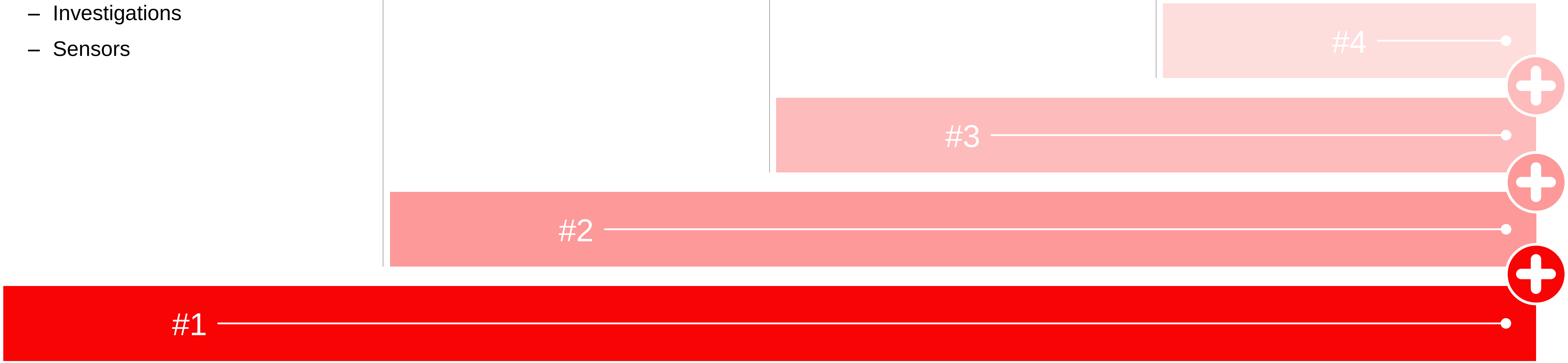
- Assess intel
  - Add context to exclude non-relevant threats
  - Integrate further QA
- Link intel to IoCs
- Integrate intel into IoC Database

Intelligence Use

- Provide CISO community with information details
- Initiate proactive actions (hardening)
- Aggregate strategic intel to build threat landscape

Intelligence Sharing

- Share back own intel with external communities



Leverage CTI - Proactive

- **Proactive Threat Detection**: CTI enables organizations to proactively detect and identify potential cyber threats before they can cause significant damage. By monitoring and analyzing threat intelligence feeds, organizations can stay ahead of emerging threats, identify new attack vectors, and take preventive measures.

- **Proactive Vulnerability Management**: CTI helps identify vulnerabilities and weaknesses in systems, applications, or infrastructure that threat actors may exploit. By integrating CTI into vulnerability management processes, organizations can prioritize and remediate vulnerabilities based on their potential exploitation by known threat actors.

Leverage CTI - Reactive

- **Enhanced Incident Response**: CTI provides valuable insights into the tactics, techniques, and procedures (TTPs) used by threat actors. This information helps organizations understand the nature of the attack, the potential impact, and the necessary response actions. It enables quicker and more effective incident response, reducing the time taken to detect, contain, and remediate security incidents.
- **Understanding Adversary Behavior**: CTI provides valuable insights into the motivations, capabilities, and behavior of threat actors. This knowledge helps organizations understand their adversaries' tactics and adapt their defense strategies accordingly. By understanding the goals and techniques of potential attackers, organizations can better anticipate and counteract threats.

Leverage CTI - Organisational

- **Risk Mitigation**: By having access to accurate and timely CTI, organizations can better assess their cybersecurity risks. They can identify vulnerabilities, potential attack vectors, and the likelihood of specific threats impacting their systems. With this knowledge, organizations can prioritize and allocate resources to mitigate the most critical risks, strengthening their overall security posture.
- **Informed Decision Making**: CTI provides actionable intelligence that supports informed decision-making processes. It enables organizations to make strategic decisions regarding security investments, threat mitigation strategies, and resource allocation. CTI helps organizations optimize their cyber defense efforts by focusing on the most relevant and high-impact threats.

Leverage CTI – External Factors

- **Collaboration and Information Sharing:** CTI encourages collaboration and information sharing among organizations, sectors, and the broader cybersecurity community. By sharing CTI, organizations can collectively defend against threats and benefit from the experiences and insights of others. Collaborative sharing of CTI helps identify patterns, trends, and indicators that may go unnoticed within individual organizations.
- **Regulatory Compliance**: CTI can assist organizations in meeting regulatory requirements related to cybersecurity. It helps organizations demonstrate due diligence in identifying and mitigating cyber risks, as well as providing evidence of a proactive approach to cybersecurity.

Requirements for good CTI

- **Timely**: CTI should be timely and provide up-to-date information about emerging threats, vulnerabilities, and indicators of compromise. Timeliness allows organizations to respond swiftly and mitigate potential risks.
- **Accurate**: CTI should be accurate and reliable, based on validated data and trusted sources. It is essential to ensure the information is verified and free from false positives or misleading indicators.
- **Relevant**: Indicators should be applicable to a recipient’s operating environment and address threats the organization is likely to face. The unnecessary processing of extraneous indicators creates additional work for analysts and slows down prioritization and categorization actions.
- **Specific:** Indicators should provide clear descriptions of observable events that recipients can use to detect threats while minimizing false positives/negatives
- **Actionable**: CTI should offer actionable insights and recommendations for organizations to implement effective countermeasures. It should guide organizations in making informed decisions regarding threat mitigation, incident response, and risk management.

NIST SP 800-150: Guide to Cyber Threat Information Sharing

Sharing Information

- Enables collective defense by collaborating with trusted partners.
- Provides early warnings and facilitates rapid response to emerging threats.
- Broadens perspectives on the threat landscape, improving situational awareness.
- Optimizes resource allocation and efficiency by leveraging shared intelligence.
- Builds trust and relationships within the cybersecurity community.
- Contributes to public safety and national security efforts.

Some Sharing Communities

Situational Awareness & Best Practice Sharing Communities (International)

FIRST.org

International confederation of trusted computer incident response teams who cooperatively handle computer security incidents and promote incident prevention programs.

TF-CSIRT / Trusted Introducer

Trusted experience and knowledge exchange to improve cooperation and coordination. Maintains a system to register & accredit CSIRTs and certifies service standards.

European Energy – Information Sharing & Analysis Centre (EE-ISAC)

Industry-driven cyber security/resilience information sharing network of private utilities/solution providers and (semi) public institutions.

US Department of Homeland Security CISCP[1]

Sharing of cyber threat, incident, and vulnerability information between the federal government and entities across critical infrastructure sectors.

Situational Awareness & Best Practice Sharing Communities (Domestic)

Deutscher CERT-Verbund

Cooperation to collect and process information related to the protection of national IT networks and including the initiation of joint incident response.

DAX40 Community

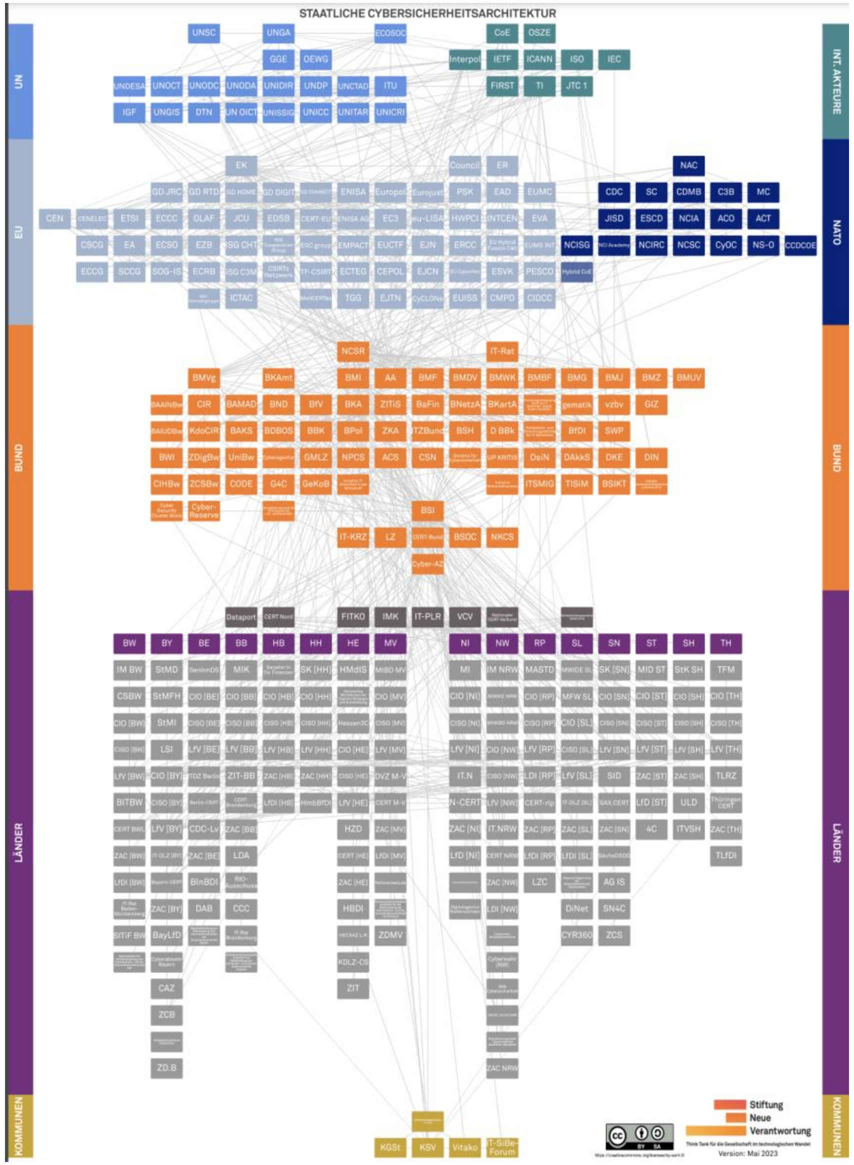
Exchange information about current threats against companies and working groups addressing current topics and developing best practices.

CSSA e.V.

Alliance to jointly share and analyze cyber security challenges in a proactive, fast and effective manner, allowing organizations to benefit from the knowledge of their peers.

...

Speaking about Complexity



https://www.stiftung-nv.de/de/publikation/deutschlands-staatliche-cybersicherheitsarchitektur

Information Sharing in Practise

“MISP (Malware Information Sharing Platform) is an open-source threat intelligence platform used for sharing, storing, and analyzing cyber threat information. It is designed to facilitate the exchange of Indicators of Compromise (IOCs), such as IP addresses, domains, hashes, and other threat data, among trusted organizations and communities.”

Key Features:

- IOCs Management
- Sharing and Collaboration
- Event Analysis and Correlation
- Automated Data Import and Export
- Visualization and Reporting

However we have challenges

- Data Quality and Accuracy
- Standardization
- Trust and Confidentiality
- Timeliness and Speed
- Data Overload and Noise
- Legal and Compliance Considerations
- Contextualization and Interpretation
- Resource Constraints

On-going Research

- Understanding Sharing Communities (study with 24 experts in the field)
- Extracting contextual information from Threat Reports leveraging LLM
- Quality Measurement for CTI Information

Conclusion

- Cyber Threat Intelligence (CTI) is of utmost importance in today's cybersecurity landscape.
- It empowers organizations to proactively detect and respond to threats, mitigate risks, make informed decisions, and collaborate with the cybersecurity community.
- By leveraging CTI, organizations can stay ahead of emerging threats, understand adversary behavior, prioritize resources effectively, and optimize their cyber defense efforts.
- CTI is a vital component of a comprehensive cyber defense strategy, enabling organizations to strengthen their security posture and defend against emerging threats.

Kontakt

Prof. Dr.-Ing. Thomas Schreck
Munich University of Applied Sciences

Email: thomas.schreck@hm.edu