The Real Work of Computer Network Defense Analysts

The Analysis Roles and Processes that Transform Network Data into Security Situation Awareness

A. D'Amico and K. Whitley

Abstract This paper reports on investigations of how computer network defense (CND) analysts conduct their analysis on a day-to-day basis and discusses the implications of these cognitive requirements for designing effective CND visualizations. The supporting data come from a cognitive task analysis (CTA) conducted to baseline the state of the practice in the U.S. Department of Defense CND community. The CTA collected data from CND analysts about their analytic goals, workflow, tasks, types of decisions made, data sources used to make those decisions, cognitive demands, tools used and the biggest challenges that they face. The effort focused on understanding how CND analysts inspect raw data and build their comprehension into a diagnosis or decision, especially in cases requiring data fusion and correlation across multiple data sources. This paper covers three of the findings from the CND CTA: (1) the hierarchy of data created as the analytical process transforms data into security situation awareness; (2) the definition and description of different CND analysis roles; and (3) the workflow that analysts and analytical organizations engage in to produce analytic conclusions.

1 Introduction

As government and business operations increase their reliance on computer networks and the information available on them, defending these valuable networks and information has become a necessary organizational function. Risks have appeared from many sources. The online world is witnessing increasingly sophisticated technical and social attacks from organized criminal operations. Moreover, an estimated

A. D'Amico
Secure Decisions division of Applied Visions, Inc.

K. Whitley
Department of Defense

120 countries are using the Internet for political, military or economic espionage (McAfee, 2007).

The broad area of cyber security encompasses policy and configuration decisions, virus scanning, monitoring strategies, detection and reaction. In the commercial world, the domain of expertise for securing and defending information resources is referred to as information security (InfoSec). U.S. governmental organizations use the synonymous terms computer network defense (CND) and defensive information operations (DIO).

This paper treats the topic of CND analysis from the perspective of the people working as professional CND analysts. We discuss how their user requirements should apply to the design of CND visualization tools. To describe the nature of CND analysis, we draw upon a cognitive task analysis (CTA) that we conducted in the 2004–2005 timeframe using mainly CND analysts working within U.S. Department of Defense (DOD) organizations. D'Amico et al. (2005) provides a preliminary report on that work. The research was designed to gain a full understanding of the daily CND analysis process. Three design considerations were: to understand both the similarities and differences in how network data was analyzed across different organizations; to include analysts whose responsibilities ranged from defending local networks to looking for attacks more broadly across a community (i.e., the notion of enclave, regional and community monitoring); and to include perspectives stemming from both tactical and strategic missions.

The CTA research was undertaken with several goals in mind, including to serve as foundation material for tool developers who do not have easy access to CND analysts and to provide requirements for the design of successful visualization for computer security. These goals also motivate this paper. This paper summarizes three findings from the CTA: (1) the hierarchy of data created as the analytical process transforms data into security situation awareness; (2) the definition and description of different CND analysis roles; and (3) the workflow that analysts and analytical organizations engage in to produce analytic conclusions. We pinpoint cognitive needs of CND analysts, rather than the software and system requirements. The analytic process is a joint (both human and machine) cognitive system, and the pipeline of CND analysis will not be automated in the near future. The needs of human analysts will remain a critical component of successful CND and should be considered when designing CND visualizations.

2 Related Work

The CND mission is succinctly summarized by Sami Saydjari: "Imagine that you lead an organization under computer attack on your critical information systems. What questions are you likely to ask? *Am I under attack; what is its nature and origin? What are the attackers doing; what might they do next? How does it affect my mission? What defenses do I have that will be effective against this attack? What can I do about it; what are my options? How do I choose the best option? How do I prevent such attacks in the future?*" (Saydjari, 2004).

To answer these questions, CND analysts are responsible for tasks such as collecting and filtering computer network traffic, analyzing this traffic for suspicious or unexpected behavior, discovering system misuse and unauthorized system access, reporting to the appropriate parties and working to prevent future attacks. CND analysts consult the output of automated systems that provide them with network data that have been automatically collected and filtered to focus the analyst's attention on data most likely to contain clues regarding attacks. These automated systems (such as firewalls, border gateways, intrusion detection systems (IDSs), anti-virus systems and system administration tools) produce log files and metadata that the analyst can inspect to detect suspicious activities.

To gauge the missions and analytic tasks across the CND community, Carnegie Mellon University (Killcrece et al., 2003) conducted a study of 29 Computer Security Incident Response Teams (CSIRTs), of which 29% were military, and listed the major activities of the teams surveyed. A summary appears in Table 1 along with the percentage of organizations reporting these activities. The bold typeface highlights those activities that were of interest to our CND CTA research. Our research focused on understanding how CND analysts inspect raw data and build their comprehension into a diagnosis or decision, especially in cases requiring data fusion and correlation across multiple data sources. The CTA did not include the work of vulnerability assessments, penetration testing, insider threat or malware analysis.

The CMU study also categorized CND activities or functions into three groups: reactive, proactive, and security quality management. Reactive activities are triggered by a preceding event or request such as a report of wide-spreading malicious

Table 1 The major activities performed by CND analysts and percentages of organizations reporting these activities (Killcrece et al., 2003)

Activities of Computer Security Incident Response Teams	
Incident handling	**97%**
Perform security policy development	72%
Publish advisories or alerts	72%
Perform artifact analysis	**66%**
Perform virus handling	66%
Monitor IDS	**62%**
Produce technical documents	**62%**
Provide and answer a hotline	62%
Do training and security awareness	59%
Perform forensic evidence collection	**55%**
Perform a technology watch or monitoring service	55%
Track and trace intruders	**52%**
Pursue legal investigations	44%
Vulnerability handling	41%
Monitoring network and system logs	**38%**
Security product development	34%
Vulnerability scanning	31%
Vulnerability assessments	28%
Security configuration administration	24%
Penetration testing	17%

code or an alert identified by an IDS or network logging system. Looking to the past, reactive tasks include reviewing log files, correlating alerts in search of patterns, forensic investigation following an attack and identification of an attacker who has already penetrated the network. Looking to the future, proactive activities are undertaken in anticipation of attacks or events that have not yet manifested. Proactive tasks include identifying new exploits before they have been used against the defended network, predicting future hostile actions and tuning sensors to adjust for predicted attacks. Security quality management activities are information technology (IT) services that support information security but that are not directly related to a specific security event; these include security training, product evaluation, and disaster recovery planning. Killcrece et al. reported, and our CTA results support, the fact that most CND analysis work is reactive, not proactive. In the CND CTA, we looked for examples of proactive work; however, the majority of the analytic activity was reactive. In describing the analysis roles below, we note instances in which proactive tasks can occur.

Alberts et al. (2004) extended the work of Killcrece et al. in a report that advocates best-practice workflows for effective incident management. Their models represent what incident response should or could be and do not necessarily represent the actual experiences of most CND analysts. By comparison, our CTA studied the state of the practice, sought to understand the existing factors that impede successful analysis and identified opportunities to improve situation awareness. Biros and Eppich (2001) conducted a CTA of rapid intrusion detection analysts (which include triage and aspects of escalation analysis, as defined below) in the U.S. Air Force and identified four requisite cognitive abilities: recognizing non-local Internet Protocol (IP) addresses, identifying source IP addresses, developing a mental model of normal, and sharing knowledge. We used their work as a starting point, but studied the larger range of CND analysis beyond triage analysis and beyond the Air Force.

3 Methods

Generally, CTA is the study of an individual's or team's cognitive processes, activities and communications within a specific work context. CTA uses naturalistic observation techniques to elucidate expertise and to understand the actual effect of processes and systems (e.g., software systems) built to automate or assist human decision makers. Ideally, a CTA involves both observing individuals as they go about their work and asking directed questions about the way in which they approach the problems, how they decide what steps to take, their communications with their coworkers and the difficulties of their work. In a CTA, care is taken to distinguish between the inherent work of a domain and the work that may be created by the current working environment and tools; in this way, the CTA can provide insight into how the current working environment helps or hinders the ultimate goals of the work. The output of a CTA is a detailed description of the tasks that an individual or team performs, the data on which they operate, the decisions they make and the

processes and activities (cognitive, communicative and perhaps physical) that they engage in to reach those decisions.

During the CTA described in this paper, 41 CND professionals working in seven different organizations participated. Most were currently active analysts; a few were managers who were not performing analysis on a day-to-day basis. They varied in level of expertise and represented a variety of job titles and work roles, as defined by their organizations. We focused on CND analysts who look at network traffic and related data to determine whether the information assets are under attack and who the attacker is. To collect data, we used a combination of four knowledge capture techniques: semi-structured interviews, observations, review of critical incidents and hypothetical scenario construction. In semi-structured interviews, the researcher guided discussion with an analyst by using a checklist of questions, yet also used wide latitude to encourage the subject to describe the day-to-day work in detail. Observations involved watching analysts at work combined with asking questions to clarify the process. Review of critical incidents involved dissecting past incidents that challenged the analyst's skills. The technique of scenario construction involved working with analysts to flesh out an imaginary analysis case of typical offensive actions taken by a sophisticated attacker and defensive actions taken by the CND analyst. Scenario construction allowed analysts to reveal the kinds of information they seek from available data sources, knowledge of adversary operations and techniques, and types of connections they make between seemingly disparate pieces of information.

4 Findings

While the organizations participating in the CTA differed in their stated mission (such as protecting a single network, identifying trends in computer attacks across the entire DOD, or performing CND services for customers outside one's own organization), they had much in common. This overlap, however, was obscured by the lack of standard terminology. Whereas various members of the community used common terms (e.g., *event* and *alert*), they often used the terms differently or without a specific definition. Also, at times, the analysts used different terms that gave an initial impression that they had different missions or needs. Therefore, a primary task in the CTA data analysis became to analyze the participants' usage of terms in the context of the details of their work. By sifting through the details, we identified similarities across the community. For tool designers, these widespread cognitive processes are valuable to understand, because they are fundamental aspects of CND.

The following sections describe CND analysis from three perspectives, highlighting aspects of human cognition. The first section considers the status of the data as raw data are processed into analytic product. The second section presents a range of analysis roles, based on work performed, not on job title. The third section describes a synthesized workflow that captures the steps in the analytic process. Throughout the discussion, the focus is on the similarities across organizations, not

on exceptional cases. In these findings, we use a standardized vocabulary, not in a prescriptive way, but as a way to illuminate the CND process data for the purpose of the CTA.

4.1 Data Transformation in CND Analysis

As a CND analyst works, data are filtered, sorted, retained or discarded based on the analyst's responsibilities and expertise. Different responsibilities involve different data. For example, some analysts primarily review the newest packet traffic or sensor data; others concentrate on data that have already been identified as suspicious, but require further analysis and correlation with additional data sources. As we discussed this process with the analysts, we ascertained that, as analysis proceeds, data are transformed as an analyst's confidence in an analytic conclusion increases. The cognitive transformation can be seen as a hierarchy of data filters with the levels reflecting the increasing certainty that a reportable security violation has been identified (depicted in Fig. 1). It is worthwhile to note that the volume of data generally decreases from level to level.

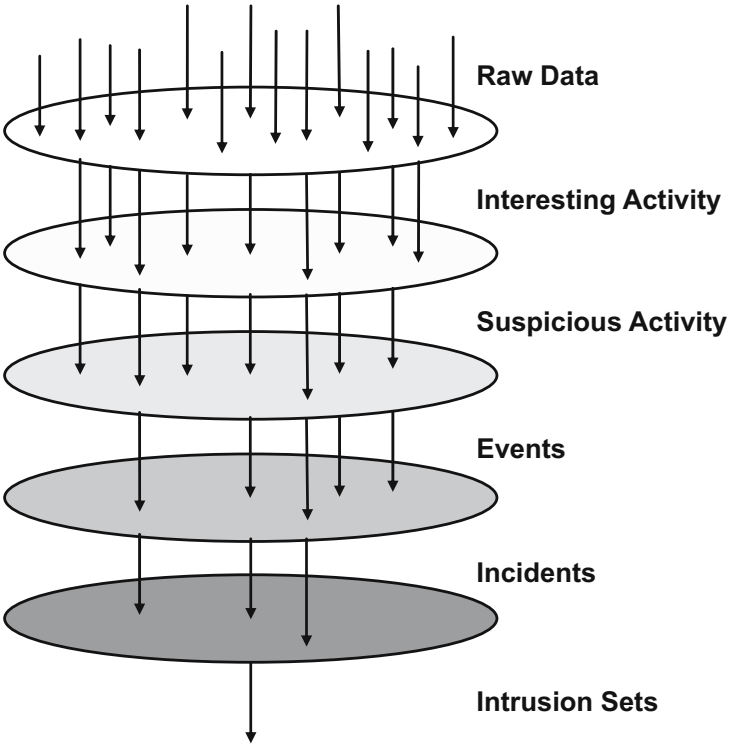

Fig. 1 Data hierarchy as data are transformed into security situation awareness

Raw data are the most elemental data in the hierarchy. At the start of the entire CND analytic workflow, the raw data can be network packet traffic, netflow data or host-based log data. Especially because the amount of raw data is so large, analysts do not generally inspect all raw data. Instead, raw data are passed through an automated process (e.g., an IDS) that makes initial filtering decisions (e.g., based on attack signatures). The automated filtering results in a substantially reduced amount of data requiring human attention.

Interesting activity refers to the data that has been flagged by the initial automated filter and sent to a CND analyst for inspection. We heard it referred to as *activity*, *alerts*, *alarms, data, logs* and *interesting activity*. Some analysts objected to the term *alerts* because they felt strongly that activity is not an alert until a human analyst has inspected and verified that the activity is worthy of further attention. Interesting activity might be presented to the CND analyst in the form of packet header data from TCPDUMP or as an IDS alert. Depending on the techniques employed by the automated filter, the interesting activity may be largely composed of false positives. Analysts perform triage on interesting activity, examining the alert details and related data, throwing out false positives and retaining the remainder for closer inspection.

Suspicious activity remains after the triage process because the CND analyst believes that the activity is anomalous for the monitored network or because it adheres to a signature or attack pattern associated with malicious intent. Some CTA participants called this type of activity an *event, anomaly* or *suspicious activity*. Examples of suspicious activity include a series of scans from the same source IP address; an unusual increase in traffic to or from a server inside the network; virus infections on several workstations in a short time period; and misuse of the monitored network by employees downloading inappropriate content.

Event refers to suspicious activity that a CND analyst has a responsibility to report, based on the organization's mission and policies. For example, an organization might be charged to report only on certain types of intrusion attempts and not on employee policy violations (e.g., using unauthorized peer-to-peer software); in this case, a policy violation would not be escalated as an event.

At the level of events, the volume of data has been significantly reduced from that of raw data. It is also the point at which CND analysts begin grouping individual activity based on common characteristics (such as source and destination IP addresses, time, attack characteristics or attacker behavior). Along the analysis workflow, CND analysts are also expanding their understanding of the data by searching for and adding new facts that show the extent of the security violation including the actors, machines, and information that has been compromised. The work for the CND analyst inspecting event data is to confirm that a security violation has occurred and to provide as full an understanding as possible of the violation.

Incident is the point when a CND analyst(s) has confirmed the occurrence and seriousness of one or more events and reports on the collection of relevant data. The incident level is usually a formal, documented point in the analysis process. A CND

analyst prepares a formal report describing the incident. After any required approval, the incident report is released as an official analytic product. Some organizations have more than one type of reports (e.g., a rapid-release distribution mechanism to distribute early information as quickly as possible and a formal reporting mechanism which is the finalized incident description). Within the DOD, official incidents are assigned to the responsible party for incident handling. Incidents may be tagged with a category type or priority ranking. Currently, there is no international consensus on incident categories or how to measure incident severity.

Incident reports are distributed to interested parties based on factors like category type and official reporting chain. The topic of report distribution and data sharing is closely related to the fact that CND analysis is often done collaboratively across organizations. Monitoring often takes place at enclave, regional and community levels with formal or informal collaboration and sharing across levels. For example, in the DOD, CND analysis occurs at individual military bases (i.e., enclave level), at the military service level (i.e., regional level) and across the entire DOD (i.e., community level). Data and reports flow up and down this reporting chain. Currently, the Joint Task Force for Global Network Operations (JTF-GNO) provides DOD community-wide analysis. For state and local governments, US-CERT, operated by the Department of Homeland Security (DHS), provides the community level. In the commercial world, companies have corporate monitoring (i.e., enclave or regional level) and may also report to a community service (e.g., a financial institution may participate in the Financial Services Information Sharing and Analysis Center (FS-ISAC)). In the case of Managed Security Service Providers (MSSPs), incidents are reported to individual customers (i.e., enclave level); an MSSP might also perform trend analysis across its entire customer base.

The benefit of wider analysis at the community level is indisputable. Aside from individual enclave concerns about the sensitivity of their data, the value of grouping CND data stems from the fact that certain incidents cannot be fully understood within a single enclave. When protecting national interests, it is important to detect related activity and larger trends occurring across individual enclaves.

Intrusion sets are sets of related incidents. In the organizations we visited, *intrusion sets* and *problem sets* were essentially synonymous terms. Intrusion sets commonly arise at the community level when CND analysts can review incidents from different reporting organizations and group these incidents based upon shared features such as source and destination IP addresses, time, attack characteristics or attacker behavior. When a CND community suspects that separately reported incidents emanate from the same source or sponsor, the community groups the incidents into an intrusion set. Just as incidents are almost universally a formal analytic product, the designation of an intrusion set is an official decision point for the organizations in our CND CTA. The community then increases attention and resources to detecting, understanding and responding to relevant activity. This process can include decisions about tuning data collection and IDS signatures to catch all new related data.

4.2 CND Analysis Roles

We wanted to understand whether and how analysis duties are divided across analysts and organizations. However, we were initially confronted with the lack of any functional descriptions of jobs performed by the analysts. Job titles, such as *level 1 analyst* or *lead analyst*, varied considerably across organizations. Furthermore, an analyst with a single job title, such as *lead analyst*, often performed many roles, such as rapid intrusion detection, consultation with other analysts and even training of junior analysts. In considering how to address this lack of common descriptions, we decided to categorize analytical function based on the actual tasks performed. The result of this exercise was a set of six broad analysis roles that accounted for all of the cognitive work observed: triage analysis, escalation analysis, correlation analysis, threat analysis, incident response and forensic analysis.

These roles represent categories of analysis; the roles do not directly map to job titles. An analyst with a single job title may perform work across more than one of the analysis roles. The roles illuminate the amount and types of data that the analyst is integrating and the goal of the analysis. The roles also reflect authority boundaries imposed by law and policy (e.g., relating to privacy). Some of the roles align closely with reactive analysis; some include aspects of proactive analysis.

Triage analysis is the first look at the raw data and interesting activity. The triage decision is a relatively fast decision about whether the data warrants further analysis. Triage encompasses weeding out false positives and escalating interesting activity for further analysis, all within a few minutes of viewing the data. Commonly, an analyst inspects IDS alerts and the immediate associated traffic/flow metadata and/or packet contents.

The majority of analysts in the CND CTA performed triage analysis. It is also very common that novice CND analysts are first assigned the job of triage analysis and work under the guidance of more senior analysts. The triage cases that novices encounter provide on-the-job training that increases the range of security violations that they can easily recognize.

Triage analysis is reactive in nature, since it is based on reviewing and sorting activity that has already occurred. Within the CTA, we encountered the following relevant CND job titles: *level 1 analyst*, *first responder* and *real-time analyst*. For the organizations in the CTA, analysts with these job titles spent the majority of their time performing triage analysis. In a small organization or at a remote site within a large organization (e.g., Air Force base), triage analysis may be performed, albeit in a limited way, by the system administrator or network manager.

Escalation analysis refers to the steps taken to investigate suspicious activity received from triage analysis. Escalation analysis requires increasing situation awareness of the suspicious activity. The process may take hours or even weeks from start to finish, during which the CND analyst marshals more data, usually from multiple data sources and from inside and outside the organization, resulting in greater comprehension of the attack methods, targets, goal and severity. The CND analyst may also make an initial assessment of attacker identity and the mission impact of an attack.

A main goal of escalation analysis is to produce incident reports. Compared to triage analysis, escalation looks at related data over longer periods of time (e.g., over the last several months of collected data) and from multiple data sources (e.g., including information from threat reports). The time needed to process these data queries and to interpret and assemble the results accounts for the fact that escalation analysis takes longer than triage analysis. In triage analysis, emphasis is on speed; correspondingly, the analysis usually involves limited queries on a single data source. In the current practice of CND analysis, the combination of triage and escalation analysis is what is often referred to as a real-time monitoring capability (although it does not actually occur in real time).

Sometimes, escalation analysis is based on tip-offs received from colleagues in other analysis groups and from cooperating organizations. This situation occurs particularly for senior analysts who have good contacts throughout the CND community.

Escalation analysis is largely reactive. Less commonly, escalation analysis involves proactive actions such as tuning sensors to look for predicted attacks or activity related to a current investigation. Within the CTA, we encountered the following relevant CND job titles: *level 2 analyst* and *lead analyst*.

Correlation analysis is the search for patterns and trends in current and historical data. At the community level, correlation analysis includes grouping data into intrusion sets; these investigations can take days to months. When conducted at the community level, correlation analysis is closely related to threat analysis.

Correlation tasks include retrospectively reviewing packet data, alert data or incident reports collected over weeks or months of CND monitoring, looking for unexplained patterns. Patterns may arise from different data attributes such as specific source or destination IP addresses, ports used, hostnames, timing characteristics, attack details and attacker behavior. By discovering patterns, CND analysts can uncover suspicious activity that was previously unnoticed. An analyst might not know what patterns they are looking for in advance; instead, the analyst might "know it when they see it." When they encounter a pattern that they cannot explain, they form hypotheses about potential malicious intent, which they try to confirm or contradict via additional investigation.

In the CND CTA, we encountered few analysts whose primary role was correlation analysis. Only 5% of the CTA participants were primarily responsible for community-wide correlation; another 5% were primarily responsible for the *post hoc* review, at the regional level, to search for anomalies or patterns not found during triage and escalation analysis.

Correlation analysis is reactive when it focuses on discovery within existing data. It has the potential to be proactive if discovered patterns are used to make predictions about next likely actions. Within the CTA, we encountered the following relevant CND job titles: *level 2 analyst, correlation analyst and site-specific analyst*. We choose the term correlation analysis, not out of a technically correct use of the concept of correlation, but rather due to the prevalent use of the term in the CND community to refer to grouping related data.

Threat analysis is intelligence analysis in support of CND. Threat analysis uses data sources beyond the monitored traffic (e.g., information published on hacker websites) to gain additional insight into the identity, motives and sponsorship of attackers and to forecast upcoming CND attacks. The additional data sources provide a higher-level perspective than is possible by examining computer network traffic and host-based activity. The additional data sources are essential for understanding an attacker's true identity and intent; One of CTA participants explained, "Intelligence is the most important factor in doing prediction and attribution."

Threat analysis may proceed in reaction to a specific attack. However, threat analysis is the most proactive of the analysis categories, since threat analysis can precede and uncover facts before a CND attack occurs. In the CTA, we found that threat analysis was primarily linked with the job title of *threat analyst*.

Incident response analysis recommends and/or implements a course of action in reaction to a confirmed incident. Responses may be as straightforward as blocking a source IP address, or as complex as "caging" or "fish bowling" an attacker inside the network to observe the attacker in action. Incident response involves assessing the tradeoffs of potential responses and how the responses will impact organizational mission. Incident response analysis is, by definition, a reactive activity. Within the CTA, we encountered the following relevant CND job titles: *incident handler* and *incident responder*.

Incident response, as well as forensic analysis, involves the issue of authority. Because of legal ramifications, only certain CND analysts are authorized to implement a response. In the CTA, the majority of analysts was responsible for analysis and reporting and not authorized to take response actions.

Forensic analysis consists of gathering evidence in support of a law enforcement investigation instigated by an incident. Forensic analysis is especially concerned with evidence preservation and has increased need for host-based evidence collection. Forensic analysis takes weeks to months to complete. Forensic analysis is, by definition, a reactive function.

In the DOD, forensic analysis is separated from the other aspects of CND analysis due to the issue of authority. Only certain analysts are authorized to collect and review cases involving U.S. citizens and to prepare this data for legal action. Forensic analysis is performed by members of a law enforcement organization, who may be assisted by incident handlers.

4.3 CND Analysis Workflow Across Organizations

Each organization that participated in the CTA had its own workflow for analyzing CND data, which differed from the other organizations' workflows. Nonetheless, after capturing each process in a workflow diagram and comparing them, we found many commonalities. Figures 2 and 3 depict a synthesized workflow that encapsulates and abstracts observations from all seven organizations.

The entire workflow operates to transform data from interesting activity to incidents and intrusion sets, with the goal of enhancing the situation awareness of

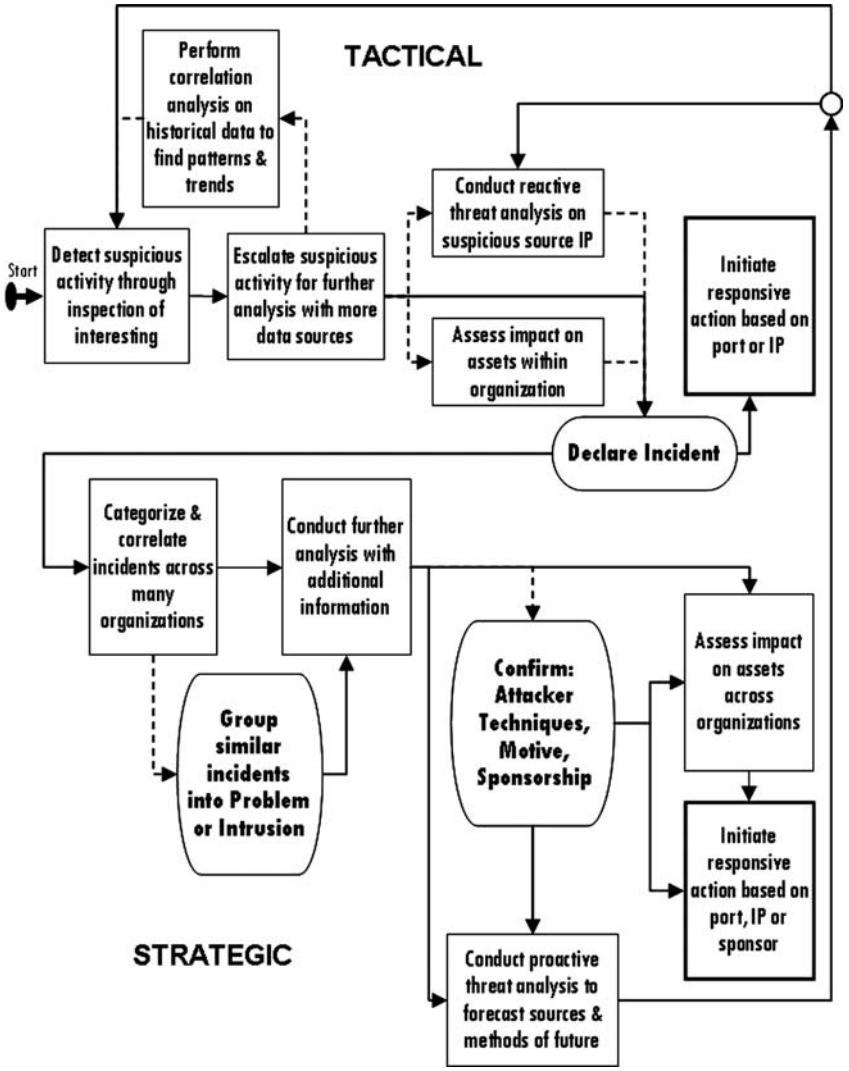

Fig. 2 Generalized CND workflow

individual analysts, organizations and the community of related organizations. All of the analysis roles play a part in this workflow. Some roles operate sequentially (e.g., triage precedes escalation) while others recur through the workflow (e.g., correlation and threat analysis). Feedback loops in the workflow illustrate the interdependence of the analysis roles and the importance of analyst communication in the data transformation process. The workflow contains both tactical and strategic goals (highlighted in Fig. 2 and described below). The workflow also contains three stages that align with principles of situation awareness and sensor data fusion (highlighted in Fig. 3 and described below).

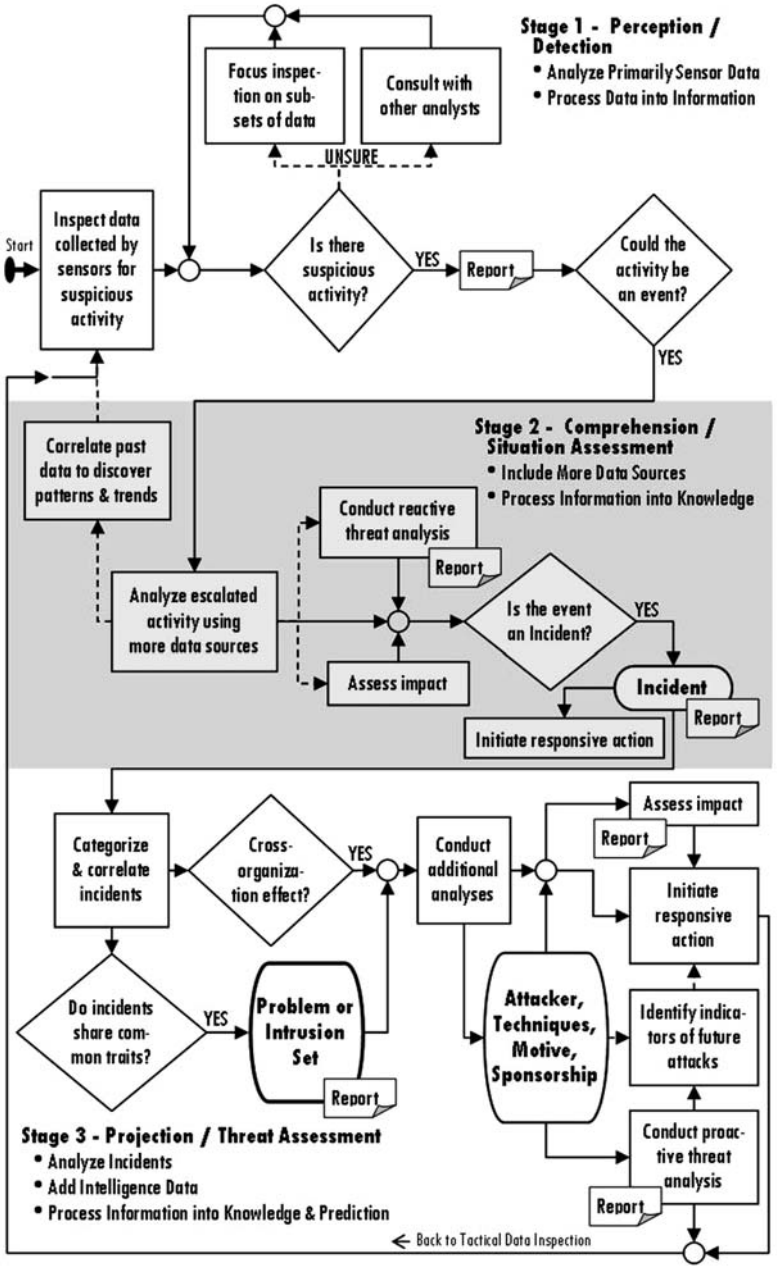

Fig. 3 Stages of CND situation awareness and cognitive data fusion

Tactical analysis. The top half of Fig. 2, ending at the declaration of an incident and initiation of incident response, represents a tactical focus. The goal of tactical analysis is to defend against an immediate, current attack and to maintain the operational status of the monitored networks. Tactical analysis is usually performed at enclave and regional levels. Analysis at the tactical level focuses on inspecting IDS alerts, flow data, firewall logs and TCPDUMP, with additional information drawn from open source and intelligence sources. The declaration of an incident is a definitive point in tactical analysis that initiates a series of incident response tasks. Incident response may be handled by the monitoring organization or by the enclave network administrator.

Strategic analysis. The bottom half of Fig. 2, beginning with the categorization and correlation of confirmed incidents, represents a strategic focus. The goal of strategic analysis is to understand the broader implications of related attacks. Strategic analysis is an important function of the community level (e.g., JTF-GNO and FS-ISAC). Incidents declared across enclaves and regions are collected at the community level. At this strategic level, a community organization examines all constituents' incidents for patterns or trends. Such patterns may indicate a well-resourced, sophisticated attacker with motives beyond nuisance attacks on an individual workstation.

Analysis at the strategic level focuses on confirmed incidents; it may be augmented with data from community sensors, intelligence reports and packet-related data requested from an enclave location. The recognition of an intrusion set is a definitive point in strategic analysis that triggers additional analyses into attack attribution, techniques, motive and sponsorship.

Stages of situation awareness. The CND workflow (see Fig. 3) moves through the three stages of building situation awareness: perception, comprehension and projection (Endsley, 1995; Endsley et al., 2003). In CND, the three stages of situation awareness also align with levels of data fusion. Specifically, analysts engage in detection, situation assessment and threat assessment, which are levels of data fusion identified by the Joint Directors of Laboratories (JDL) and recognized widely by the sensor data fusion community (Llinas and Hall, 1998, Waltz, 1998).

Stage 1: perception/detection. During the first stage, a CND analyst acquires data about the monitored environment, which is typical of the perceptual stage of situation awareness. As the analyst performs triage on interesting activity, comprehension begins. An analyst assembles and integrates data to form a mental model of how the interesting activity might represent an attacker's action. By testing hypotheses through additional data and input from colleagues, an analyst modifies and clarifies his mental model. By the end of the first stage, when the analyst decides whether to escalate, the focus shifts from perception to comprehension. The first CND stage is primarily concerned with initial data inspection and detection and, thus, aligns with JDL Level 1.

Stage 2: comprehension/situation assessment. During the second stage, analysts focus on escalation and correlation analysis, which represent the comprehension aspect of situation awareness. Analysts combine suspicious data, their own knowledge and expertise, and additional data sources to determine whether the suspicious

activity represents an incident. The analyst refines the mental model of the attacker's identity and threat level by tracking the attack path through the network and time. Analysts performing correlation analysis identify patterns of anomalous behavior, which they share with those performing triage and escalation analysis.

Stage 2 also involves limited projection. Escalation analysis includes some postulating about an attacker's actions if left unblocked. Incident responders, in choosing a course of action, project what actions an attacker might take if he realizes he has been discovered. This stage also aligns with JDL Level 2 because a main activity is to inject more data (perhaps from relevant, additional data sources) to refine the analysis.

Stage 3: projection/threat assessment. During the third stage, analysts performing correlation, incident response, and threat analysis review and categorize confirmed incidents at the community level. By comparing incidents and adding data from intelligence sources, they discern attack patterns. By this point, the analysts at the community level have a shared mental model. As comprehension improves, the analysts refine the shared mental model and project into the future to forecast the types of incidents to expect within the community. Furthermore, proactive threat analysis identifies potentially new exploits and attackers that could become active in the future. Based on these projections, tips are fed back into the start of the analysis pipeline as perceptual cues for detection. This feedback loop forms a perception-action cycle across multiple, distributed actors. This stage aligns with JDL Level 3 because the analysis involves inferences about attacker identity, motive and sponsorship.

5 Implications for Visualization

5.1 Visualization Across the CND Workflow

Along the CND workflow, as analysis tasks transform data into situation awareness, analysts' attention widens from single packets and network flows to communication networks and final conclusions. Fundamental tasks include noticing what data should be investigated, formulating good analysis questions, searching data sources, evidence tracking and synthesizing a conclusion. CND visualization can occur within a single packet/flow, across multiple packets/flows, across incident reports and in situations that require blending data from multiple data sources.

In the triage stage, CND analysts are commonly looking at IDS alerts and the metadata and content contained in individual packets and flows. Usually, an analyst's attention has been guided to a specific packet or flow by an automated filter or colleague's tip-off. The analyst needs fast access to the alerts and rapid drill down to the related raw data. Viewing individual data elements, an analyst is not yet forming connections to other pieces of data. Simple visualizations are appropriate at this stage. An example is color highlighting of the interesting portions of

the data (e.g., the content that matched the IDS signature) to ensure that the analyst sees relevant details. One simple, but effective visual cue observed in the CTA was an alert management system that used color to reflect the status of the alert. Lines were colored according to whether the alert was not yet assigned to an analyst, whether the alert had been assigned and was in triage or whether the triage had completed (either by discarding or escalating the alert). This mechanism can apply to CND offices with centralized, shared raw data in which the office needs to track all incoming interesting data.

In the escalation and correlation stages, CND analysts build patterns that span across packets. The work includes analysis needed to understand whether an attempted attack succeeded and to understand the extent of a successful attack. A common exercise during escalation is to build the communication network of the suspected attacker and victim. The analyst wants the picture of all known hosts that have communicated with either the attacker or the victim, and all alerts associated with any of these hosts. This network is a central part of the analyst's mental model of the attack; it indicates the extent of the attack by showing likely attack origination points, data exfiltration paths and further contamination. Unifying visualizations can facilitate comprehension of the sequence of interconnected events; appropriate visualizations include graphs (i.e., link-node diagrams) and flexible timeline-based visualizations.

Other patterns in the escalation and correlation stages include summaries of, for example, the most active ports and IP addresses, frequency of alert types, the size of data payloads and the relationships between ports and protocols. Visual presentations can be very useful for exposing patterns and supporting data exploration. Even traditional visual techniques such as scatterplots and histograms, combined with easy-to-use filtering capabilities, can be applied effectively to the problem. Analysts will look for something to "pop out at them." In fact, the popping out that occurs is a cognitive event in which an analyst associates several pieces of data and adds a hypothesis explaining how these data are related.

For correlation for intrusion sets and threat analysis, there is increasing need to combine facts from multiple data sources and to present the data as a cohesive analytic conclusion. For intrusion sets, in particular, a visualization solution should be capable of providing a temporal context that emphasizes the sequence of events. In these roles, there is more likelihood that an analyst will be manipulating secondary data sources and textual data (e.g., incident reports in correlation analysis; open source text in threat analysis) and assembling all evidence into a single compendium. The combination of visualization and annotation (a feature mentioned again in Sect. 5.2) would allow analysts to provide the combination of facts and interpretation that completes the analytic product.

For successful CND visualization, the value of visualization is closely tied to the utility of the data available for viewing and the analysts' ability to search that data. CND analysis is very much an information retrieval problem. Like web searching, CND analysts need to search data repositories and are limited or empowered by the expressivity and usability of the search capability. For example, if analysts can only query their data repository on attributes in the metadata (as opposed

to characteristics of the traffic content), analysts will have difficulty discovering new attack strategies (i.e., for which no IDS signatures exist). Another example concerns whether analysts can easily query the organization's database of incident reports. Incident reports represent the CND organization's collective memory. Often, incident reports are textual documents without delineated fields to enable straightforward searching. The result can be that an analyst is prevented from checking to see if an unusual attack detail has appeared in any prior incident reports.

Expanding on the example of incident reports, the value of CND visualization is strengthened when contextual data are immediately available for viewing. Contextual data are general (e.g., IP registration information) or site-specific (e.g., "Hot IP" lists, prior incident reports) information that speeds situation awareness. In the case of "Hot IP" lists, CND organizations frequently maintain a changing list of IP addresses of particular interest. An analyst may also have a list related to his individual set of investigations. The analyst's perception and comprehension will be improved if data visualizations automatically highlight IP addresses that appear on the organization's list or his individual list.

As a final suggestion, tool designers should consider user groups beyond professional CND analysts. As a whole, the entire Internet population is increasingly concerned with computer security and identity theft. In particular, tool designers could benefit home users by making the current and past behavior of their home computers more transparent and understandable.

5.2 Visualization as Part of a CND Analysis Environment

Visualization components form a part of a larger CND working environment. The success of the visualization pieces depends upon how well the visual tools are integrated with a CND analyst's other tools and how well the combination of tools addresses the CND workflow. These considerations may not be at the forefront of priorities when a visualization designer begins. However, these considerations ultimately determine whether CND analysts are willing to adopt the tool and whether the tool is commercially viable.

Three important criteria are ease of input and output from the tool, support for report building, and management of evidence and analysis. In today's state of the practice, CND analysts spend considerable time on tasks other than analysis. Examples are time spent massaging data formats and spent creating a final report form. Therefore, for a visualization tool to be attractive to analysts, a tool should minimize the effort needed to get data into and out of the tool. A desirable approach is for the tool to support a variety of input and output options, a strategy that also helps interoperability with other tools. For input, it is common for a CND analyst to use a primary data source, but at times to receive data from other sources with differing formats. Similarly, analysts must communicate their analysis to peers; this may mean sharing the data isolated during analysis (i.e., a subset of the actual data) or

sending a copy of the visualization illustrating a communication network or pattern. Thus, the tool should support the output of both data and visualizations.

An extension of this, CND analysts become very enthusiastic at the idea of a tool that automates some or all of the requisite report building. A tool that can directly add relevant data and views into a report for direct distribution to customers will spare analysts the tedious time and potential errors involved in assembling a report using cut-and-paste and transcription. Analysts are not enthusiastic at the idea about investing energy to create a useful visualization, but then having to compose a textual equivalent for their report.

Finally, the category of evidence and analysis management refers to features that assist analysts in gathering and tracking the data that support their current investigations and in documenting the analysts' hypotheses and interpretations. During the CTA, CND analysts were very desirous of tools that would support "an analytic diary" capability. As an analyst isolates data segments relevant to an investigation, it is helpful to be able to save the data subset and its context (i.e., collection information including data source and time range) in a personal analysis space. As a collection of current evidence, the analysis space should support quick access and manipulation of the evidence. Moreover, the analysis space should allow the analyst to annotate investigations with notes about their interpretations of the evidence and recommended next steps.

Acknowledgements The research described in this document was sponsored by the US Department of Defense and the Advanced Research and Development Activity (ARDA) under contract # F30602-03-C-0260, with the Air Force Research Laboratory (AFRL) in Rome, NY as the contracting agency. Mr. Walter Tirenin of AFRL provided opportunities for collaboration with other scientists, careful review of progress, and assistance in making our results available for public distribution. We would also like to thank Daniel Tesone and Brianne O'Brien for their significant work in the CTA data collection and analysis. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of ARDA or the US Government.

References

Alberts C, Dorofee A, Killcrece G et al. (2004) Defining Incident Management Processes for CSIRTS: A Work in Progress, Technical Report CMU/SEI-2004-TR-015, ESC-TR-2004-015. http://www.sei.cmu.edu/publications/documents/04.reports/04tr015.html. Accessed 06 December 2007

Biros D, Eppich T (2001) Human Element Key to Intrusion Detection. Signal, August: 31

D'Amico A, Whitley K, Tesone D et al. (2005) Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts. Proceedings of the Human Factors and Engineering Society Annual Meeting: 229–233

Endsley M (1995) Toward a theory of situation awareness in dynamic systems. Human Factors, 37(1): 32–64

Endsley M, Bolte B, Jones D (2003) Designing for Situation Awareness: An Approach to User-Centered Design. Taylor & Francis, New York: 13–18

Killcrece G, Kossakowski KP, Ruefle R, Zajicek M (2003) State of the Practice of Computer Security Incident Response Teams (CSIRTS), Technical Report CMU/SEI-2003-TR-001, ESC-TR-2003-001

Llinas J, Hall D (1998) An introduction to multi-sensor data fusion. IEEE Report 0-7803-4455-3/98

McAfee Virtual Criminology Report–Cybercrime: The Next Wave (2007). http://www.mcafee.com. Accessed 04 December 2007

Saydjari O (2004) Cyber Defense: Art to Science, Communications of the ACM 47(3): 53–57

Waltz E (1998) Information understanding: integrating data fusion and data mining processes. IEEE Report 0-7803-4455-3/98