CYFORCE

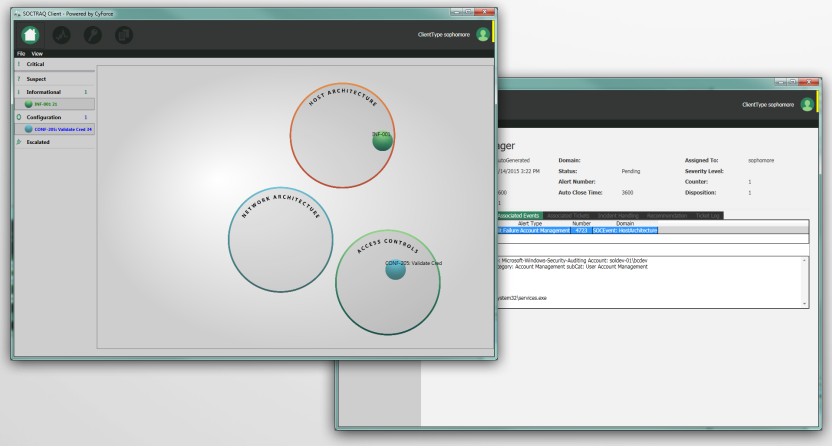
A Paradigm Shift for Incident Response

SOCTRAQ at a Glance

A fundamental shortfall of traditional Cyber Security Incident Response and Case Management systems is the inability to quickly develop threat chains and their impact on "downstream" assets and the challenges associated with analyzing advanced attacks that occur over time, coupled with autonomous actions to allow SOC Analysts to take proactive measures to address threats. SOCTRAQ empowers analysts at any level to perform investigative or proactive mitigation activities appropriate to their experience or responsibility levels.

Leveraging Visualization to Detect and Respond to Next Generation Threats

The approach SOCTRAQ takes to displaying received alerts is similar to that of an air traffic control display interface. Assets within an enterprise, grouped into one of three domain designations, are displayed as alert objects appearing within one of those three domains. Once a "threat chain" has been identified by the system and a threat level to other assets has been determined by the "Threat Guardian™" algorithm, SOCTRAQ will provide appropriate triage and prescribed actions based on "threat indexes" configured by the organization during deployment. SOCTRAQ incorporates a visual element of "movement" to support active identification of advanced threats making threat chains easily discernible and ensure communication of emerging threats does not require extensive investigation.



FEATURES

- Integrated Cyber Security Incident Response and Case Management
- Unique analyst interface provides visual depiction of alerts
- Threat Guardian™ algorithm automates triage and designates alerts
- Threat Chain Compilation graphically depicts related events
- Prescribed Actions and Countermeasures optimizes analyst response
- Autonomous Actions supports orchestrated incident response
- Built-in Case Management provides correlation for related events

BENEFITS

- Visualization and reporting of Incident Response information
- Correlation of incidents across numerous domains
- Prescriptive remediation steps to maximize efficiency
- Better way to harness existing investments in SIEM technology
- Automated threat detection technology provides near real-time detection of incidents across an enterprise
- Enables SOC analyst insight into related historical events
- Supports correlation of related events over time based on trends or multi-incident Indicators of Compromise
- Natively identifies related events tied to a single human actor or group of individuals to support insider threat detection

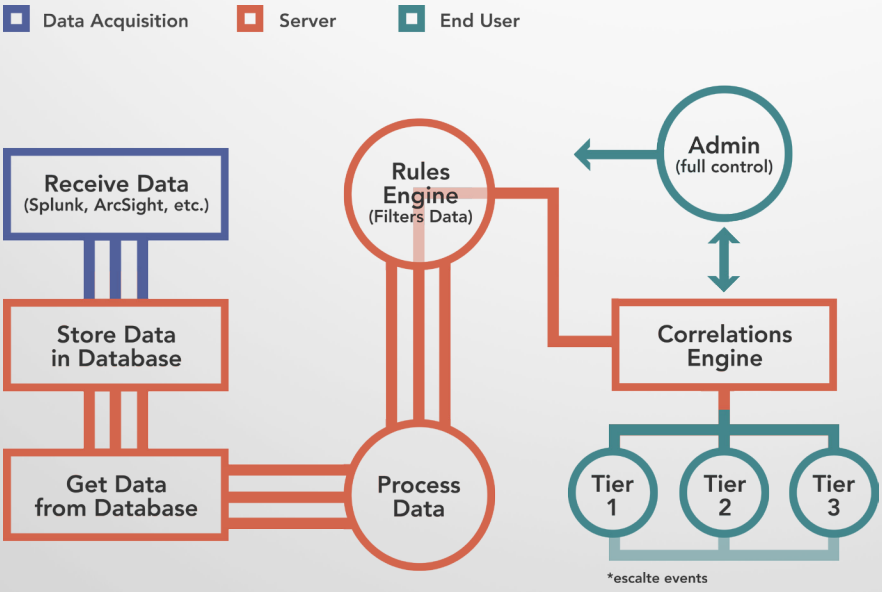
Threat Chain Compliance

Creation of a "threat chain" is dependent on an analysts' ability to collect significant amounts of disjointed information, determine which assets may or may not be involved and perform a threat assessment based solely on what is often a very incomplete picture. SOCTRAQ provides this composite assessment once the "Threat Guardian™" matrix of enclave assets has been completed and will graphically depict the events and how their linkage could result in a compromise or breach.

Actions & Countermeasures

Empowering analysts to do more than basic ticket escalation and updating is one of the strengths of the SOCTRAQ system. Knowing what to do when an alert is received can be a daunting task for engineers of all experience levels. SOCTRAQ allows the SOC manager to prescribe any number of pre-approved actions for alerts received. SOCTRAQ presents the analyst with the ability to take action in response to a received alert/event message. Furthermore, the system can beconfigured to perform the action (or countermeasure) autonomously if no action is taken within a predetermined interval; this ensures that events will be addressed before they can evolve into much larger issues. In most cases, the options available to a tier-1 analyst will be those related to investigation, escalation or research before turning over to help desk or the next tier of analyst.

SOCTRAQ Data Flow



ACTIVE INCIDENT VISUAL

- A visual representation of real-time alerts/threats logically grouped by one of three domain designations; User/ Community, Network, and Application
- Designation of alerts are seperated into one of four categories: Informational, Suspect, Configuration Management and Critical
- Logical depiction of threat chains and the impacts they might have on "downstream" architecture assets

THREAT DETECTION

- Compilation of disparate alerts/events into an identifiable threat chain, via the proprietary Blue Canopy "Threat Guardian™" algorithm
- Enables SOC analyst insight into related historical events
- Allows the correlation of related events over time based on trends or multi-incident Indicators of Compromise
- Provides advanced "backward plot" correlation of related events tied to a single or group of individuals
- Supports correlation of related events tied to an evolvable threat model

INCIDENT RESPONSE AUTOMATION

- Predetermined "Recommended Actions" and "Countermeasures" appropriate to level or tier of the analyst
- Auto escalation and application of countermeasures as prescribed by organization or agency security policy
- Case management that allows analysts to see threats and take proactive measures to mitigate emerging threats
- Reporting and Executive Dashboard Tool to provide insight into Incident Response effectiveness