Extend the Capabilities of Einstein 3A (E3A) with xTract

xTract is an IT security software program created to enhance the Einstein3Accelerated (E3A) service, making it easier to analyze, find the exact location of the problem and remaining traces of security impacts to networks. xTract helps your agency verify if there are one or more compromises on your network(s), enabling you to directly protect your unique assets.

With xTract’s trending and correlation information, your team can manage your response, policy and resource needs over time, integrating and utilizing xTract as a key component of your Information Assurance Strategy.

Ready for E3A?

Once you subscribe to E3A, based on the size of your Agency, you will receive potentially thousands of incident email notices every hour.

Manage Einstein 3A with xTract

xTract enhances E3A by consolidating multiple notices (risks) into specific incidents (problems), helping analysts to quickly pinpoint the source of the incident behind your firewall. Incidents can then be prioritized into actionable information for threat removal and neutralization.
Quantitative Data for Your Long Term Information Assurance Strategy

Today’s risks are not your only concern. In addition to identifying specific numbers of incidents and locations of successful breaches, xTract provides Security Managers with dashboards, reports and trending data for intrusion attempts. Resultant data can be used to help develop and implement appropriate policies aligned with each agency’s risk posture. Your Security Managers can use these metrics for reporting, review effectiveness of existing security postures, design improvements along with appropriate resource allocation; strengthening your security position for future attacks.

For more information on xTract, visit xla.com/xtract

Case Study: xTract at Work

xTract is currently deployed in the E3A active environment, helping to manage and prioritize email notices into actionable information.

May and June 2015

In this two month period alone, xTract automatically processed and correlated thousands of daily E3A notices. This would be equivalent manual effort by a Security Analyst of ~ 600-800 hours, a direct saving of $40-$50k/month ($480-$600k/year) to our Government customer.

› The Government is seeing a significant increase in the number of daily E3A notices, potentially dramatically, making automation a near necessity.

› xTract’s multi-faceted automation and correlation capabilities are one of its key features. In existing environments, the xTract correlation engine has combined notices into distinct incidents at an average rate of 86%, thereby significantly reducing the level of effort to research and locate the sources of problems.

› xTract was successfully tested for scalability for larger agency applicability, where it successfully processed ~ 16,000 daily E3A notices (320K/month). In such an environment, xTract can automatically process the equivalent of 53,000 Security Analyst labor hours per month, with a potential monthly savings of over five million dollars to the Government.

› Using xTract’s data to pinpoint and enable agencies to successfully neutralize malware, we are working with our customers to developing applicable and effective policies to reduce future probability of similar occurrences.

› xTract complements the Office of the Director of National Intelligence Insider Threat Program (ITP).