exabeam

SOLUTION BRIEF

CBEST 2.0

THE CBEST 2.0 SECURITY ASSESSMENT FRAMEWORK IS DESIGNED TO ASSIST ORGANIZATIONS AS THEY ASSESS AND IMPROVE THEIR CYBERSECURITY READINESS.

CBEST is now widely considered as a world-leading framework for intelligence-led penetration testing of systemically critical organisations. Since the tests are designed to simulate actual attacks, a key component of CBEST testing is effective detection of attacks and accurate reporting of how the attack unfolded.

CBEST tests are conducted by CREST accredited penetration testing providers. The tests mimic real behaviours of threat actors as assessed by both UK government and commercial threat intelligence providers.

CBEST testing outcomes do not result in a straightforward pass or fail scenario - supervised remediation timeframes can be expected to take between six to twelve months, or longer in some cases, depending on the nature of the remediation plan.

CBEST 2.0 OVERVIEW

The CBEST assessment takes around six months to complete, and the process consists of four phases of work:

- **The Initiation Phase** - during which the CBEST assessment is formally launched, the scope is established and threat intelligence / penetration testing service providers are procured;
- **The Threat Intelligence Phase** - during which the core threat intelligence deliverables are produced, threat scenarios are developed into a draft penetration test plan, threat intelligence capability is assessed and control is handed over to the penetration testing service provider;
- **The Penetration Testing Phase** - during which an intelligence-led penetration test against the target systems and services that underpin each critical function in scope is planned, executed and reviewed and detection and response capabilities are assessed;

- **The Closure Phase** - during which the Bank of England Sector Cyber Team produces its intelligence, detection and response report, the firm / financial market infrastructure's remediation plan is finalised, the threat intelligence / penetration testing service providers are debriefed, and the regulator(s) supervises the execution of the remediation plan

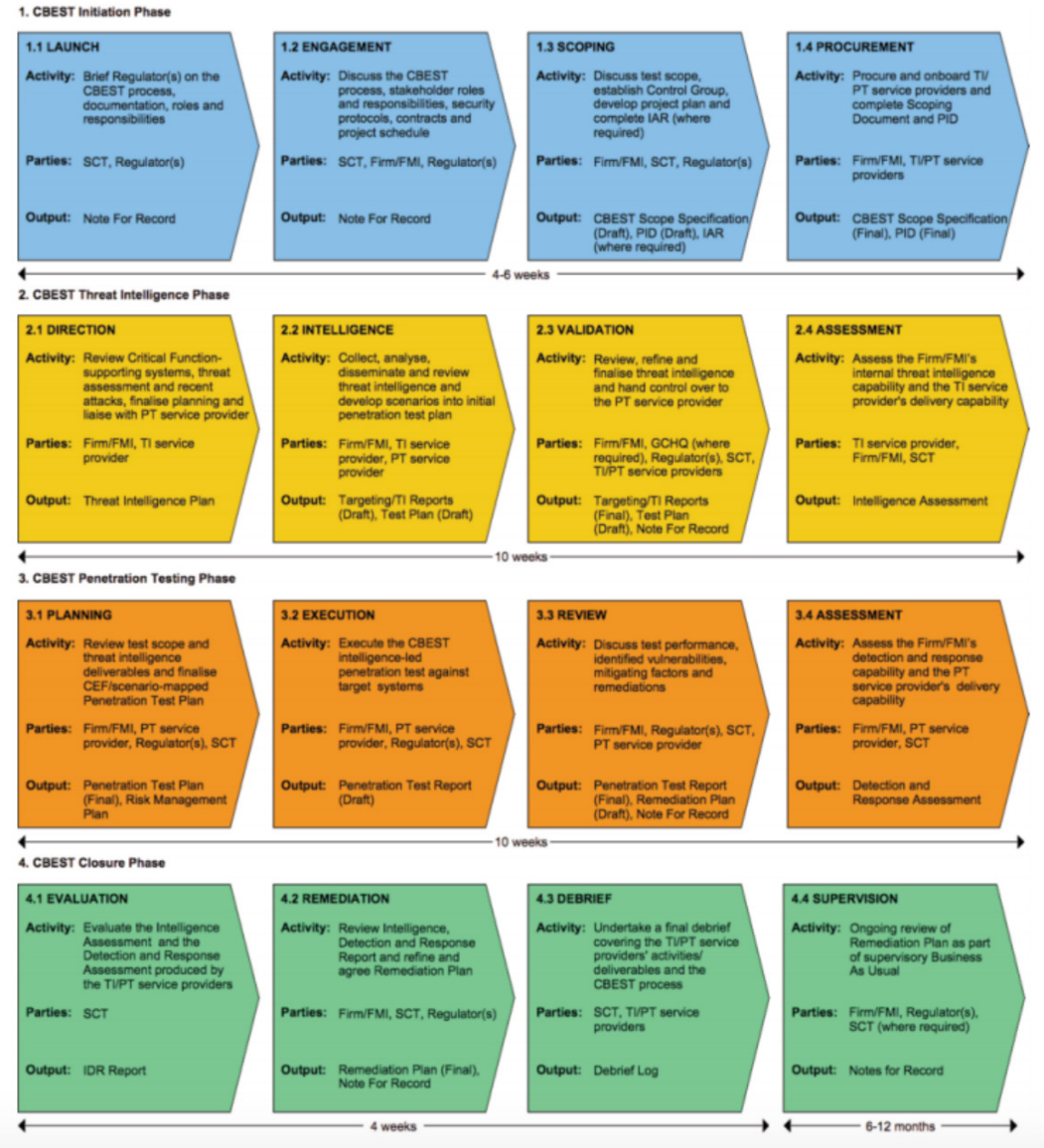

FIGURE 1: CBEST ASSESSMENT PROCESS MODEL (SOURCE: CBEST IMPLEMENTATION GUIDE)

HOW EXABEAM HELPS ORGANIZATIONS UNDERTAKING CBEST ASSESSMENTS

The rigorous, intelligence driven nature of CBEST assessments means traditional security defenses are significantly unlikely to prevent the advanced attacker behaviors used to exploit, infiltrate, and move laterally through an organization's infrastructure.

Exabeam's Security Management Platform (SMP) helps organizations quickly detect and rapidly react to advanced threat techniques, and provides accurate read-outs of attack techniques, timing, and identities involved.

During the execution subsection of the penetration test phase, Exabeam can help security teams identify testers' simulated attack behaviours. Exabeam detects lateral movement such as first-time access by user accounts as well as system or machine accounts. Exabeam also detects credential switches and privilege escalations including the creation of new user or admin accounts, which are typically used to access confidential information. As a result, Exabeam can sound the alarm very early in a CBEST test.

- Lateral movement can be notoriously difficult to detect, since attackers not only switch machines and IP addresses, but also use different credentials for different systems. Using traditional SIEM technology, the pieces are not self-evidently connected to the same attacker, making full context difficult. Exabeam Smart Timelines(™) automatically tie these seemingly unrelated activities together into a coherent picture, enabling effective detection of penetration testing (and actual) activities.
- Deeper movement into confidential systems often requires access that is uncommon for a user or that user's peers. Exabeam detects first-time access to confidential systems and can raise risk and visibility levels before actual exfiltration occurs.
- As data is copied to staging servers, Exabeam detects first-time copies or unusual amounts of data/file copy volume, and integrates verdicts from sensitive data fingerprinting (i.e. DLP) systems. Build-up of data on staging servers is identified before actual egress occurs.

Prompt response reduces the time afforded to the tester to intensify and expand their attacks. Once malicious activities are detected, Exabeam provides actionable insights to help security teams to respond faster, better utilize their existing processes and tools, and drastically improve analyst efficiency.

- Key pieces of information are automatically gathered via out-of-the-box integrations with popular security and IT infrastructure.These can include URL, IP and file reputation data, sandbox results, threat intelligence, device information, running process lists and many more. Security events, along with these enrichments, are then organized in Smart Timelines to provide analysts with the chronology of an attack.
- Response playbooks allow analysts to programmatically perform investigation, containment, or mitigation. Analysts have a wealth of actions at their fingertips, including:
  - Invoking forensics tools
  - Blocking malicious hashes and IP addresses
  - Quarantining systems
  - Triggering 2FA responses
  - Disabling compromised accounts
- Automated workflows, based upon commonly used processes such as phishing and malware triage reduce manual tasks and remove the potential for human error.

exabeam

During the review and assessment subsections of the penetration testing phase, organizations can also use Exabeam to demonstrate detection and response capabilities to the penetration testing team.

ABOUT EXABEAM

Exabeam is the Smarter SIEM™ company. We help security operations and insider threat teams work smarter, allowing them to detect, investigate and respond to cyberattacks in 51 percent less time. Security organizations no longer have to live with missed distributed attacks and unknown threats, manual investigations and remediation, or excessive storage fees. With the modular Exabeam Security Management Platform, analysts can use behavioral analytics to detect attacks, automate investigation and incident response, and reduce storage costs. Exabeam Smart Timelines, sequences of user and device behavior created using machine learning, further reduce the time and specialization required to detect attacker tactics, techniques and procedures. For more information, visit https://www.exabeam.com.

TO LEARN MORE ABOUT HOW EXABEAM CAN HELP YOU, VISIT EXABEAM.COM TODAY.