ExtraHop

SecOps Face Off:

Automated Investigation vs. Manual Meltdown

See how Reveal(x) automates security workflows for faster detection, investigation, and remediation.

Reveal(x)

UNPRECEDENTED VISIBILITY. DEFINITIVE INSIGHTS. IMMEDIATE ANSWERS.

Multi-Tool Workflow

ALERT OVERLOAD. MANUAL INVESTIGATION. ENDLESS GUESSWORK.

Failed Login Attempts

Several failed logins by a client on a sensitive database. Potential brute force login attempt.

WIRE DATA | LOGS/AGENTS

POTENTIAL BRUTE FORCE ALERT

BRUTE FORCE DETECTED

Automatically detected. Forensic evidence, including all transaction details and packets between client and DB automatically gathered and correlated.

DHCP LOGS
Analyst receives alert identifying IP address of suspicious client and must query DHCP logs and CMDB for contextual information about the client.

LDAP LOGS
Analyst manually checks LDAP logs or other auth logs to understand the relationship between the client and DB in question.

DATABASE LOGS
Analyst manually gathers database logs, if available.

SIEM
Analyst manually checks SIEM for logs of the suspicious IP address accessing the DB, if available.

Successfully Logged In

Client successfully logs into sensitive DB.

Analyst is provided evidence of suspicious DB access and can proactively assess the situation and respond.

DATABASE LOGS
Analyst manually queries DB logs.

SIEM
Analyst manually queries logs from client via SIEM, if available.

ATTACK AVERTED

FURTHER INVESTIGATION OF THE INCIDENT CAN OCCUR WITHOUT FEAR OF DAMAGE.

DATA DOWNLOADED

Client attempts to initiate download of data from DB. Database responds in affirmative and commences delivering data.

Reveal(x) sees exactly which data the client is attempting to download by decoding the contents of the client request and DB responses, so analysts can determine instantly whether or not the action is malicious.

FLOW LOG PROVIDER
Analyst manually queries network flow logs, DB logs, and client logs, if available.

DATABASE LOGS
If no transaction-level detail or DB logs available, analyst must conjecture whether or not data was delivered, and what it might have been.

LOGS DELETED

Client instructs DB to delete audit table (logs).

Reveal(x) sees the client issue a DROP command against the audit table, which should never be done, proving incontrovertibly that this is a malicious action.

Analyst is no longer able to obtain forensic evidence from DB logs about exactly which data, and how much, was taken.

PCAP & WIRESHARK
Analyst consults packet-capture solution, and downloads multi-Gigabyte PCAP file to examine in Wireshark. The file takes several minutes to open, and much longer to manually comb through for evidence of malicious action by the client on the database.

FTP CONNECTION WITH EXTERNAL IP ADDRESS

Client initiates FTP session with strange IP address outside corporate IP space.

Reveal(x) sees client initiate FTP session with external client, and sees exactly which files are being transferred, providing further conclusive evidence and forensic detail about the malicious action.

ALERT
New alert is not correlated with earlier suspicious behavior from this client.

SIEM
Analyst manually queries logs for internal client, if available.

FLOW
Analyst manually queries flow data between client and External IP address, which indicates volume of data transferred, but doesn't have filenames or other forensic details.

WIRESHARK
Analyst downloads new PCAP of all transactions with the suspicious client and examines in Wireshark.

Reveal(x)

GRAND TOTALS

Multi-Tool Workflow

1 TOOL REQUIRED

1 MANUAL STEP

Upon first receiving the alert about the potential brute force attack, the analyst cut off access to the DB for the suspicious client, then drilled down to transaction details and packets using Reveal(x) to confirm that the DB access was malicious.

Attack averted.

7 TOOLS REQUIRED

9 MANUAL STEPS

Having spent several hours, or even days, manually investigating separate alerts about the same attack, the security analyst discovers that sensitive data has been exfiltrated, and initiates a painful forensic investigation and reporting process.

Forensic investigation and damage assessment begins.

CUSTOMER VALUE

95% IMPROVEMENT IN TIME TO DETECT

77% IMPROVEMENT IN TIME TO RESOLVE

59% REDUCTION IN STAFF TO RESOLVE

ExtraHop

EXTRAHOP.COM/REVEALX