Detection Strategy for Financial Theft, Detection Strategy DET0495

Archived: 2026-04-05 16:39:22 UTC

AN1361

Monitor for anomalous access to financial applications, browser-based banking sessions, or enterprise ERP systems from Windows endpoints. Detect mass emailing of payment instructions, sudden rule changes in Outlook for financial staff, or use of clipboard data exfiltration tied to cryptocurrency wallet addresses.

Log Sources

Mutable Elements

Field	Description
FinanceAppList	Baseline of finance-related executables or ERP processes to monitor closely.
HighRiskAccounts	Accounts belonging to finance, treasury, or executives that should be monitored with higher sensitivity.

AN1362

Monitor server and endpoint logs for unusual outbound network connections to cryptocurrency nodes, unauthorized scripts accessing financial systems, or automation targeting payment file formats. Detect curl/wget activity aimed at exfiltrating transaction data or credentials from financial apps.

Log Sources

Mutable Elements

Field	Description
KnownFinanceIPs	Whitelisted IPs for finance-related traffic to reduce noise.

AN1363

Monitor unified logs for access to payment applications, browser plug-ins, or Apple Pay services from non-standard processes. Detect anomalous use of Automator scripts or keychain extraction targeting financial account credentials.

Log Sources

Mutable Elements

Field	Description
MonitoredApps	Financial or payment applications to explicitly monitor for unauthorized use.

AN1364

Monitor SaaS financial systems (e.g., QuickBooks, Workday, SAP S/4HANA cloud) for unauthorized access, rule changes, or mass export of financial data. Detect anomalous transfers initiated via SaaS APIs or new MFA-disabled logins targeting finance apps.

Log Sources

Data Component	Name	Channel
Application Log Content (DC0038)	saas:finance	Transaction/Transfer: Unusual or large transactions initiated outside business hours or by unusual accounts

Mutable Elements

Field	Description
TransactionThreshold	Customizable monetary threshold above which financial transactions should be flagged.

AN1365

Monitor email and document management systems for fraudulent invoices, impersonation of vendors, or BEC-style payment redirections. Detect abnormal editing of invoice templates, or emails containing known fraud language combined with attachment delivery.

Log Sources

Data Component	Name	Channel
Application Log Content (DC0038)	m365:unified	MailSend: Outlook messages with suspicious subject/body terms (e.g., urgent payment, wire transfer) targeting finance teams
File Modification (DC0061)	m365:office	Anomalous editing of invoice or payment document templates

Mutable Elements

Field	Description
FraudTerms	Adjustable keyword list for email and document fraud detection.

Source: https://attack.mitre.org/detectionstrategies/DET0495#AN1363