Threat Intelligence and Threat Hunting

• Application Security Monitoring
  No image available
  ◦ Detecting Kubernetes scanning activity
  ◦ Monitoring Kubernetes sensitive object access
  ◦ Protecting a Salesforce cloud deployment

• Cloud Security Monitoring
  No image available
  ◦ Analyzing AWS service action errors

• Data Loss Monitoring
  No image available
  ◦ Finding large web uploads
  ◦ Monitoring a network for DNS exfiltration
  ◦ Monitoring use of Git repositories

• Endpoint Security Monitoring
  No image available
  ◦ Detecting print spooler attacks
  ◦ Detecting recurring malware on a host
  ◦ Detecting techniques in the Orangeworm attack group
  ◦ Detecting the Baron Samedit sudo attack
  ◦ Finding interactive logins from service accounts
  ◦ Monitoring command line interface actions

• Fraud Analytics and Detection
  No image available
  ◦ Detecting ATM fraud
  ◦ Detecting wire transfer fraud
Insider Threat and Account Compromise

- Conducting an Azure new user census
- Detecting lateral movement with Active Directory data
- Detecting masquerading
- Detecting unusual GCP service account usage
- Finding Windows audit log tampering
- Identifying new Windows local admin accounts
- Monitoring for signs of Windows privilege escalation attack
- Monitoring Kubernetes sensitive role activities
- Recognizing improper use of system administration tools

Network Security Monitoring

- Detecting network and port scanning
- Detecting TOR traffic
- Detecting UDP service amplification abuse
- Monitoring employee network traffic
- Monitoring for network traffic volume outliers
- Terminating W3WP spawned processes

Web Activity Security Monitoring

- Deleting web shells automatically
- Detecting unencrypted web communications